



Guida per l'utente

AWS Servizio di migrazione del Database



AWS Servizio di migrazione del Database: Guida per l'utente

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 AWS Database Migration Service?	1
Attività di migrazione eseguite da AWS DMS	2
Come AWS DMS funziona	4
Visualizzazione di alto livello di AWS DMS	4
Componenti	6
Origini	13
Origini per la migrazione dei dati	13
Origini per DMS Fleet Advisor	16
Origini per la conversione dello schema DMS	17
Origini per migrazioni omogenee di dati DMS	17
Destinazioni	18
Destinazioni per la migrazione dei dati	18
Destinazioni per DMS Fleet Advisor	21
Destinazioni per la conversione dello schema DMS	21
Destinazioni per migrazioni omogenee di dati DMS	22
Nome della risorsa Amazon	22
Con altri AWS servizi	25
Support per AWS CloudFormation	25
Nozioni di base	27
Configurazione	27
Registrati per un Account AWS	27
Crea un utente con accesso amministrativo	28
Prerequisiti	29
Crea un VPC	30
Creazione di gruppi di parametri Amazon RDS	32
Creazione del database Amazon RDS di origine	33
Creazione del database Amazon RDS di destinazione	35
Creazione di un client Amazon EC2	35
Popolamento del database di origine	37
Migrazione dello schema	38
Replica	40
Fase 1: creazione di un'istanza di replica	41
Fase 2: specificazione degli endpoint di origine e di destinazione	43
Fase 3: creazione di un'attività e migrazione dei dati	44

Fase 4: test della replica	46
Fase 5: eliminazione delle risorse AWS DMS	48
Risorse aggiuntive	49
Individuazione dei database per la migrazione	51
Regioni AWS supportate	52
Nozioni di base	54
Configurazione	55
Creazione delle risorse necessarie	55
Creazione di utenti di database	64
Raccoglitori di dati	71
Autorizzazioni	72
Creazione di un raccoglitore di dati	72
Installazione di un raccoglitore di dati	75
Individuazione dei server del sistema operativo e di database	78
Gestione degli oggetti monitorati	82
Uso di SSL	84
Raccolta di dati	85
Risoluzione dei problemi	91
Inventario	93
Utilizzo dell'inventario dei database	94
Utilizzo dell'inventario degli schemi	95
Suggerimenti delle destinazioni	97
Istanze di destinazione	98
In che modo DMS Fleet Advisor determina le specifiche della destinazione?	98
Generazione di suggerimenti delle destinazioni	99
Dettagli dei suggerimenti	101
Esportazione dei suggerimenti delle destinazioni	103
Limitazioni della migrazione	104
Risoluzione dei problemi	123
Limitazioni	124
Conversione degli schemi di database	126
Supportato Regioni AWS	127
Funzionalità	128
Limitazioni	129
Nozioni di base	130
Prerequisiti	131

Fase 1: creazione di un profilo dell'istanza	136
Fase 2: configurazione dei fornitori di dati	137
Fase 3: creazione di un progetto di migrazione	138
Fase 4: creazione di un report di valutazione	138
Fase 5: conversione del codice sorgente	139
Fase 6: applicazione del codice convertito	140
Fase 7: pulizia e risoluzione dei problemi	140
Configurazione di una rete	141
Configurazione di un singolo VPC	142
Configurazione di più VPC	142
Utilizzo di AWS Direct Connect o di una VPN	143
Utilizzo di una connessione Internet	143
Utilizzo di un ambiente senza un gateway Internet	143
Creazione di fornitori di dati di origine	144
Utilizzo di SQL Server come origine	145
Utilizzo di Oracle come origine	146
Utilizzo di Oracle Data Warehouse come origine	147
Utilizzo di PostgreSQL come origine	150
Utilizzo di MySQL come origine	151
Creazione di fornitori di dati di destinazione	152
Utilizzo di MySQL come destinazione	152
Utilizzo di PostgreSQL come destinazione	154
Utilizzo di Amazon Redshift come destinazione	155
Gestione dei progetti di migrazione	156
Specificazione delle impostazioni del progetto di migrazione	156
Report di valutazione della migrazione del database	158
Creazione di un report di valutazione	158
Visualizzazione del report di valutazione	159
Salvataggio del report di valutazione	160
Conversione dello schema	162
Configurazione delle regole di trasformazione	163
Conversione dello schema di database	165
Specifica delle impostazioni di conversione dello schema	169
Aggiornamento degli schemi di database	175
Salvataggio e applicazione dello schema	176
Utilizzo dei pacchetti di estensione	178

Migrazioni di database omogenee	179
Supportato Regioni AWS	180
Funzionalità	181
Limitazioni	181
Panoramica	182
Configurazione	183
Creazione di risorse IAM	183
Configurazione di una rete	188
Creazione di fornitori di dati di origine	192
Utilizzo di MariaDB o MySQL come origine	192
Utilizzo di PostgreSQL come origine	196
Utilizzo di MongoDB o Amazon DocumentDB come sorgente	199
Creazione di fornitori di dati di destinazione	203
Utilizzo di MariaDB o MySQL come destinazione	203
Utilizzo di PostgreSQL come destinazione	205
Utilizzo di Amazon DocumentDB come destinazione	207
Migrazione di dati	207
Creazione di una migrazione dei dati	208
Regole di selezione	210
Gestione delle migrazioni dei dati	213
Monitoraggio delle migrazioni dei dati	214
Stati di migrazione	216
Migrazione dei dati da MySQL	217
Migrazione dei dati da PostgreSQL	219
Migrazione dei dati da MongoDB	221
Risoluzione dei problemi	222
Creazione di una migrazione dei dati	223
Avvio di una migrazione dei dati	223
Problemi di connessione	223
Le viste vengono migrate come tabelle in PostgreSQL	224
Utilizzo di progetti di migrazione	225
Creazione di un gruppo di sottoreti	226
Creazione di profili dell'istanza	226
Creazione di fornitori di dati	228
Creazione di progetti di migrazione	230
Gestione dei progetti di migrazione	232

Best practice	233
Pianificazione della migrazione di AWS Database Migration Service	233
Conversione dello schema	235
Revisione della documentazione di AWS DMS	235
Esecuzione di un proof of concept	235
Miglioramento delle prestazioni	236
Utilizzo del server dei nomi in locale	241
Utilizzo del risolutore Amazon Route 53 con AWS DMS	243
Migrazione di oggetti binari di grandi dimensioni (LOB)	243
Utilizzo della modalità LOB limitata	244
Prestazioni LOB migliorate	245
Miglioramento delle prestazioni per la migrazione di tabelle di grandi dimensioni usando il filtro di riga	248
La replica continua	249
Riduzione del carico del database di origine	249
Riduzione dei colli di bottiglia sul database di destinazione	250
Utilizzo della convalida dei dati	250
Monitoraggio dei parametri	251
Eventi	251
Utilizzo del log delle attività	252
Risoluzione dei problemi di replica con Time Travel	252
Modifica dell'utente e dello schema per una destinazione Oracle	252
Modifica di spazi di tabella per tabelle e indici di una destinazione Oracle	253
Aggiornamento di un'istanza di replica	254
Comprensione dei costi di migrazione	255
Lavorare con Serverless AWS DMS	256
Componenti di DMS serverless	257
Versioni del motore supportate	260
Creazione di una replica serverless	261
Modifica delle repliche serverless AWS DMS	263
Configurazione del calcolo	267
Comprendere la scalabilità automatica in modalità serverless AWS DMS	268
Monitoraggio delle repliche senza server AWS DMS	269
Throughput esteso a pieno carico	274
Limitazioni del serverless	275
Utilizzo delle istanze di replica	277

Scelta dei tipi di istanze di replica	282
Decisione della classe di istanza da utilizzare	287
Istanze a prestazioni espandibili in modalità illimitata	288
Dimensionamento di un'istanza di replica	289
Fattori da considerare	290
Problemi comuni	291
Best practice	292
Versioni del motore di replica	292
Aggiornamento della versione del motore mediante la console	293
Aggiornamento della versione del motore utilizzando il AWS CLI	293
Istanze di replica pubbliche e private	294
Indirizzi IP e tipi di rete	295
Configurazione di una rete per un'istanza di replica	296
Configurazioni di rete per la migrazione del database	297
Creazione di un gruppo di sottoreti di replica	306
Risoluzione degli endpoint di dominio con DNS	307
Impostazione di una chiave di crittografia	308
Creazione di un'istanza di replica	308
Modifica di un'istanza di replica	314
riavvio di un'istanza di replica.	320
Eliminazione di un'istanza di replica.	323
Finestra di manutenzione DMS	325
Effetto della manutenzione sulle attività di migrazione esistenti	325
Modifica dell'impostazione della finestra di manutenzione	326
Endpoints	328
Creazione di endpoint di origine e destinazione	328
Origini per la migrazione dei dati	333
Utilizzo di Oracle come origine	334
Utilizzo di SQL Server come origine	405
Utilizzo di un database SQL di Azure come origine	436
Utilizzo dell'istanza gestita da Azure SQL come origine	436
Utilizzo di Azure Database per PostgreSQL come origine	437
Utilizzo di Azure Database per MySQL come origine	438
Utilizzo di OCI MySQL Heatwave come origine	439
Utilizzo di Google Cloud per MySQL come origine	440
Utilizzo di Google Cloud per PostgreSQL come origine	440

Utilizzo di PostgreSQL come origine	442
Utilizzo di MySQL come origine	482
Utilizzo di SAP ASE come origine	495
Utilizzo di MongoDB come origine	504
Utilizzo di Amazon DocumentDB come origine	523
Utilizzo di Amazon S3 come origine	540
Utilizzo di IBM Db2 LUW come origine	555
Utilizzo di IBM Db2 for z/OS come origine	562
Destinazioni per la migrazione dei dati	603
Utilizzo di Oracle come destinazione	604
Utilizzo di SQL Server come destinazione	615
Utilizzo di PostgreSQL come destinazione	621
Utilizzo di MySQL come destinazione	634
Utilizzo di Amazon Redshift come destinazione	643
Utilizzo di SAP ASE come destinazione	669
Utilizzo di Amazon S3 come destinazione	672
Utilizzo di Amazon DynamoDB come destinazione	723
Utilizzo dei flussi di dati Amazon Kinesis come destinazione	745
Utilizzo di Apache Kafka come destinazione	764
Utilizzo di OpenSearch come destinazione	792
Utilizzo di Amazon DocumentDB come destinazione	798
Utilizzo di Amazon Neptune come destinazione	812
Utilizzo di Redis come destinazione	829
Uso di Babelfish come destinazione	836
Utilizzo di Amazon Timestream come destinazione	844
Utilizzo di Db2 come destinazione	856
Endpoint VPC per la migrazione dei dati	857
Chi è interessato dalla migrazione a AWS DMS 3.4.7 e versioni successive?	858
Chi non è interessato dalla migrazione a AWS DMS 3.4.7 e versioni successive?	858
Preparazione di una migrazione a AWS DMS 3.4.7 e versioni successive	859
Istruzioni DDL supportate	860
Attività	862
Creazione di un'attività	866
Impostazioni delle attività	876
Impostazione del supporto LOB	931
Creazione di più attività	933

Attività di replica continua	933
Replica a partire da un punto di inizio CDC	935
Esecuzione della replica bidirezionale	940
Modifica di un'attività	945
Spostamento di un'attività	945
Ricaricamento delle tabelle durante un'attività	946
AWS Management Console	947
Mappatura delle tabelle	948
Specifica della selezione delle tabelle e delle regole di trasformazione dalla console	949
Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON	953
Operazioni e regole di selezione	955
Caratteri jolly nella mappatura delle tabelle	962
Operazioni e regole di trasformazione	963
Utilizzo delle espressioni delle regole di trasformazione per definire il contenuto delle colonne	987
Regole e operazioni delle impostazioni di tabella e raccolta	1002
Utilizzo di filtri di origine	1036
Applicazione di filtri	1037
Applicazione di filtri in base a ora e data	1043
Abilitazione e utilizzo delle valutazioni preliminari alla migrazione	1044
Prerequisiti	1045
Specifica, avvio e visualizzazione delle esecuzioni della valutazione	1048
Valutazioni individuali	1052
Avvio e visualizzazione delle valutazioni dei tipi di dati	1086
La valutazione dei problemi viene eseguita	1090
Specifica dei dati supplementari	1091
Monitoraggio delle attività	1092
Stato dell'attività	1094
Stato delle tabelle durante le attività	1097
Monitoraggio delle attività di replica usando Amazon CloudWatch	1098
Parametri di AWS Database Migration Service	1100
Parametri dell'istanza di replica	1103
Parametri dell'attività di replica	1106
Visualizzazione e gestione dei log AWS DMS	1109
Registrazione delle chiamate API AWS DMS con AWS CloudTrail	1111
Informazioni su AWS DMS in CloudTrail	1111

Comprensione delle voci dei file di log di AWS DMS	1112
Registrazione di log di contesto	1116
Tipi di oggetto	1116
Esempi di log	1118
Limitazioni	1119
Utilizzo degli eventi EventBridge	1120
Utilizzo delle regole di eventi di Amazon EventBridge per AWS DMS	1121
Categorie di eventi AWS DMS e messaggi di evento	1122
Messaggi dell'evento ReplicationInstance	1122
Messaggi dell'evento ReplicationTask	1127
Messaggi dell'evento Replication	1129
Utilizzo degli eventi Amazon SNS	1131
Spostamento delle sottoscrizioni a eventi su Amazon EventBridge	1131
Utilizzo degli eventi e delle notifiche Amazon SNS	1132
Categorie di eventi e messaggi di evento AWS DMS per le notifiche SNS	1134
Sottoscrizione alla notifica di eventi AWS DMS tramite SNS	1137
Utilizzo di AWS Management Console	1138
Convalida della policy di accesso dell'argomento SNS	1141
Convalida dei dati	1143
Statistiche delle attività di replica	1144
Statistiche dell'attività di replica con Amazon CloudWatch	1147
Nuova convalida delle tabelle durante un'attività	1148
AWS Management Console	1148
Utilizzo dell'editor JSON per modificare le regole di convalida	1148
Attività di sola convalida	1149
Sola convalida pieno carico	1150
Sola convalida CDC	1150
Casi d'uso di sola convalida	1151
Risoluzione dei problemi	1151
Prestazioni di convalida di Redshift	1153
Limitazioni	1154
Convalida S3	1155
Prerequisiti	1156
Autorizzazioni	1157
Limitazioni	1158
Attività di sola convalida	1159

Assegnazione di tag alle risorse	1161
API	1163
Sicurezza	1165
Protezione dei dati	1168
Crittografia dei dati	1168
Riservatezza del traffico Internet	1169
Protezione dei dati in DMS Fleet Advisor	1170
Identity and Access Management	1171
Destinatari	1171
Autenticazione con identità	1172
Gestione dell'accesso con policy	1175
Come AWS Database Migration Service funziona con IAM	1178
Esempi di policy basate su identità	1185
Esempi di policy basate su risorse	1193
Utilizzo dei segreti per accedere alle risorse	1198
Utilizzo di ruoli collegati ai servizi	1208
Risoluzione dei problemi	1215
Autorizzazioni IAM richieste	1218
Ruoli IAM per CLI e API	1223
Prevenzione del confused deputy tra servizi	1229
AWS politiche gestite	1232
Convalida della conformità	1241
Resilienza	1243
Sicurezza dell'infrastruttura	1244
Controllo granulare degli accessi	1247
Utilizzo dei nomi delle risorse per il controllo dell'accesso	1247
Utilizzo dei tag per controllare l'accesso	1250
Impostazione di una chiave di crittografia	1258
Sicurezza di rete	1261
Uso di SSL	1263
Limiti per l'utilizzo di SSL con AWS DMS	1265
Gestione dei certificati	1265
Abilitazione di SSL per un endpoint compatibile con MySQL, PostgreSQL o SQL Server ...	1266
Modifica della password del database	1269
Limiti	1270
Quote di risorse per AWS Database Migration Service	1270

Informazioni sulla limitazione (della larghezza di banda della rete) delle richieste API	1272
Risoluzione dei problemi e supporto diagnostico	1273
Attività di migrazione eseguite lentamente	1274
La barra di stato dell'attività non si sposta	1275
L'attività è stata completata ma non è stato migrato nulla	1275
Indici secondari e chiavi esterne mancanti	1275
AWS DMS non crea registri CloudWatch	1276
Problemi con la connessione ad Amazon RDS	1276
Messaggio di errore: Incorrect thread connection string: incorrect thread value 0 (Stringa di connessione del thread errata: valore 0 del thread errato)	1277
Problemi di rete	1277
Blocco del CDC dopo il pieno carico	1278
Errori di violazione delle chiavi primarie al riavvio di un'attività	1278
Il caricamento iniziale dello schema ha esito negativo	1278
Esito negativo delle attività con errore sconosciuto	1279
L'attività riavvia il caricamento delle tabelle dall'inizio	1279
Il numero di tabelle per attività causa problemi	1279
Attività non riuscite durante la creazione della chiave primaria in una colonna LOB	1279
Record duplicati nella tabella di destinazione senza chiave primaria	1280
Endpoint di origine nell'intervallo IP riservato	1280
Timestamp confusi nelle query di Amazon Athena	1280
Risoluzione dei problemi con Oracle	1281
Estrazione dei dati dalle viste	1281
Migrazione di LOB da Oracle 12c	1281
Passaggio tra Oracle LogMiner e Binary Reader	1282
Errore: Oracle CDC stopped 122301 Oracle CDC maximum retry counter exceeded (CDC Oracle arrestato 122301 Numero di nuovi tentativi di CDC Oracle superato).	1282
Aggiunta automatica di log supplementare a un endpoint di origine Oracle	1283
Le modifiche ai LOB non vengono acquisite	1283
Errore: ORA-12899: valore eccessivo per colonna <i>nome-colonna</i>	1284
Il tipo di dati NUMBER viene interpretato in modo errato	1284
Record mancanti durante il pieno carico	1284
Errore della tabella	1285
Errore: impossibile recuperare gli ID di destinazione di log redo archiviati da Oracle	1285
Valutazione delle prestazioni di lettura dei log redo o di archiviazione di Oracle	1285
Risoluzione dei problemi relativi a MySQL	1287

L'attività CDC ha esito negativo per l'endpoint dell'istanza database di Amazon RDS perché la registrazione binaria è disabilitata	1288
Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività	1288
Aggiunta di commit automatico a un endpoint compatibile con MySQL	1289
Disabilitazione delle chiavi esterne su un endpoint di destinazione compatibile con MySQL	1290
Caratteri sostituiti con punto interrogativo	1290
Voci di log "Evento errato"	1290
Change Data Capture con MySQL 5.5	1291
Aumento del periodo di conservazione dei log binari per istanze database di Amazon RDS	1291
Messaggio di log: Some changes from the source database had no impact when applied to the target database (Alcune modifiche dal database di origine non hanno avuto alcun impatto quando applicate al database di destinazione).	1291
Errore: Identifier too long (Identificatore troppo lungo)	1291
Errore: Unsupported Character Set Causes Field Data Conversion to Fail (Il set di caratteri non supportato causa l'esito negativo della conversione dei dati di campo)	1292
Errore: Codepage 1252 to UTF8 [120112] A field data conversion failed (Tabella codici 1252 su UTF8 [120112] Esito negativo di una conversione dei dati di campo)	1292
Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati	1293
Risoluzione dei problemi relativi a PostgreSQL	1295
I tipi di dati JSON sono troncati	1296
Le colonne di un tipo di dati definito dall'utente non vengono migrate correttamente	1297
Errore: No schema has been selected to create in (Nessuno schema selezionato per la creazione)	1297
Le operazioni di eliminazione e aggiornamento su una tabella non vengono replicate mediante CDC	1297
Le istruzioni Truncate non vengono propagate	1297
Come evitare che PostgreSQL acquisisca DDL	1297
Selezione dello schema in cui vengono creati gli oggetti di database per l'acquisizione di DDL	1298
Tabelle Oracle mancanti dopo la migrazione a PostgreSQL	1298
ReplicationSlotDiskUsage aumenta e restart_Isn smette di andare avanti durante transazioni lunghe, come i carichi di lavoro ETL	1298
Un'attività che utilizza la vista come origine non dispone di righe copiate	1299

Risoluzione dei problemi relativi a Microsoft SQL Server	1299
Errori durante l'acquisizione di modifiche per il database SQL Server	1299
Colonne di identità mancanti	1300
Errore: SQL Server non supporta le pubblicazioni	1300
Le modifiche non vengono visualizzate nella destinazione	1300
Tabella non uniforme mappata tra le partizioni	1301
Risoluzione dei problemi relativi ad Amazon Redshift	1301
Caricamento in un cluster Amazon Redshift in una regione AWS diversa rispetto a quella dell'istanza di replica	1302
Errore: Relation "awsdms_apply_exceptions" already exists (Relazione "awsdms_apply_exceptions" già esistente)	1302
Errori con tabelle il cui nome inizia con "awsdms_changes"	1302
Visualizzazione di tabelle nei cluster con nomi simili a dms.awsdms_changes000000000XXXX	1302
Autorizzazioni necessarie per l'utilizzo di Amazon Redshift	1303
Risoluzione dei problemi relativi ad Amazon Aurora MySQL	1303
Errore: CHARACTER SET UTF8 fields terminated by ',' enclosed by "" lines terminated by '\n' (Campi SET DI CARATTERI UTF8 terminati da ',' racchiusi tra "" righe terminate da '\n')	1303
Risoluzione dei problemi relativi a SAP ASE	1304
Errore: le colonne LOB hanno valori NULL quando l'origine ha un indice univoco composto con valori NULL	1304
Risoluzione dei problemi relativi a IBM Db2	1304
Errore: la funzione Riprendi dal timestamp non è un'attività supportata	1304
Risoluzione dei problemi di latenza	1305
Tipi di latenza CDC	1305
Cause comuni della latenza CDC	1306
Risoluzione dei problemi di latenza	1310
Utilizzo degli script di supporto per la diagnostica	1325
Script di supporto Oracle	1327
Script di supporto SQL Server	1330
Script di supporto compatibili con MySQL	1355
Script di supporto PostgreSQL	1357
Utilizzo dell'AMI di supporto diagnostico	1360
Avvia una nuova AWS DMS istanza diagnostica Amazon EC2	1361
Creazione di un ruolo IAM	1361

Esecuzione dei test diagnostici	1362
Fasi successive	1366
ID AMI per regione	1367
Riferimento	1368
Tipi di dati AWS DMS	1368
Note di rilascio	1371
AWS DMS Note di rilascio 3.5.3	1372
AWS DMS Note di rilascio 3.5.2	1375
AWS DMS note di rilascio 3.5.1	1377
AWS DMS Note sulla versione 3.5.0 Beta	1390
AWS DMS Note di rilascio 3.4.7	1396
AWS DMS Note di rilascio 3.4.6	1406
AWS DMS note di rilascio 3.4.5	1412
AWS DMS note di rilascio 3.4.4	1416
AWS DMS note di rilascio 3.4.3	1418
AWS DMS note di rilascio 3.4.2	1421
AWS DMS note di rilascio 3.4.1	1423
AWS DMS Note di rilascio 3.4.0	1424
AWS DMS note di rilascio 3.3.4	1425
AWS DMS note di rilascio 3.3.3	1426
Cronologia dei documenti	1428
Glossario AWS	1433
.....	mcdxxxiv

Cos'è AWS Database Migration Service?

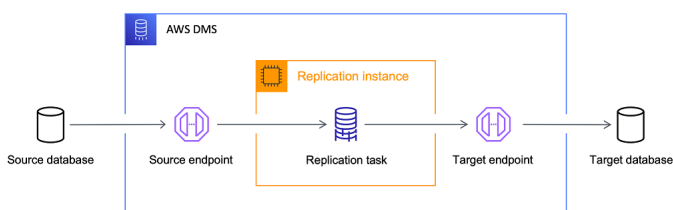
AWS Database Migration Service (AWS DMS) è un servizio cloud che consente di migrare database relazionali, data warehouse, database NoSQL e altri tipi di datastore. Puoi utilizzare AWS DMS per migrare i tuoi dati nel Cloud AWS o tra combinazioni di configurazioni cloud e on-premise.

Con AWS DMS, puoi individuare i datastore di origine, convertire gli schemi di origine e migrare i dati.

- Per individuare l'infrastruttura dei dati di origine, puoi utilizzare DMS Fleet Advisor. Questo servizio raccoglie i dati dal database on-premise e dai server di analisi e crea un inventario di server, database e schemi che puoi migrare al cloud AWS.
- Per eseguire la migrazione a un altro motore di database, puoi utilizzare la conversione dello schema DMS. Questo servizio valuta e converte automaticamente gli schemi di origine in un nuovo motore di destinazione. In alternativa, è possibile scaricare AWS Schema Conversion Tool (AWS SCT) sul PC locale per convertire gli schemi di origine.
- Dopo aver convertito gli schemi di origine e applicato il codice convertito al database di destinazione, puoi utilizzare AWS DMS per migrare i dati. Puoi eseguire migrazioni in un'unica fase o replicare le modifiche in corso per mantenere sincronizzate le origini e le destinazioni. AWS DMS fa parte del Cloud AWS, pertanto puoi ottenere la convenienza, la sicurezza, la flessibilità e i tempi rapidi di commercializzazione offerti dai servizi AWS.

Fondamentalmente, AWS DMS è un server nel Cloud AWS che esegue il software di replica. Puoi creare una connessione di origine e di destinazione per comunicare ad AWS DMS il percorso di estrazione e quello di caricamento dei dati. Quindi, puoi pianificare un'attività in esecuzione su questo server per spostare i dati. AWS DMS crea le tabelle e le chiavi primarie associate se non esistono sulla destinazione. Puoi creare le tabelle di destinazione manualmente, se preferisci. In alternativa, puoi utilizzare AWS Schema Conversion Tool (AWS SCT) per creare alcuni o tutti i trigger, le viste, gli indici, le tabelle di destinazione e così via.

Il diagramma seguente illustra il processo di replica AWS DMS.



Riferimenti

- Regioni AWS che supportano AWS DMS: per informazioni sulle regioni AWS che supportano AWS DMS, consulta [Utilizzo di un'istanza di AWS DMS replica](#).
- Costi di migrazione dei database: per informazioni sui costi di migrazione dei database, consulta la [pagina dei prezzi di AWS Database Migration Service](#).
- Funzionalità e vantaggi di AWS DMS: per informazioni su funzionalità e vantaggi di AWS DMS, consulta [Caratteristiche di AWS Database Migration Service](#).
- Opzioni di database disponibili: per ulteriori informazioni sulle varie opzioni di database disponibili su Amazon Web Services, consulta [Choosing the right database for your organization](#).

Attività di migrazione eseguite da AWS DMS

AWS DMS esegue automaticamente molte delle difficili e noiose attività presenti in un progetto di migrazione:

- In una soluzione tradizionale, è necessario eseguire l'analisi delle capacità, procedere all'acquisto di hardware e software, installare e gestire i sistemi ed eseguire il test e il debug dell'installazione. AWS DMS gestisce automaticamente l'implementazione, la gestione e il monitoraggio di tutto l'hardware e il software necessari per la migrazione. La migrazione può essere operativa pochi minuti dopo l'avvio del processo di configurazione di AWS DMS.
- Con AWS DMS, è possibile aumentare (o diminuire) le risorse di migrazione a seconda delle esigenze del carico di lavoro effettivo. Ad esempio, se stabilisci di aver bisogno di storage aggiuntivo, puoi facilmente incrementare lo storage allocato e riavviare la migrazione, di solito in pochi minuti.
- AWS DMS impiega un modello basato sul consumo. I prezzi delle risorse di AWS DMS sono calcolati in base all'uso effettivo e pertanto si differenziano dai tradizionali modelli di licenza con costi di acquisto iniziali e spese di manutenzione continue.
- AWS DMS gestisce automaticamente tutta l'infrastruttura che supporta il server di migrazione, inclusi hardware e software, applicazione di patch software e segnalazione degli errori.
- AWS DMS offre il failover automatico. Se il server di replica primario non viene eseguito per qualsiasi motivo, viene eseguito automaticamente un server di replica di backup con interruzione del servizio minima o assente.
- AWS DMS Fleet Advisor effettua automaticamente l'inventario dell'infrastruttura di dati. Crea i report che ti consentono di identificare i candidati alla migrazione e a pianificare la migrazione.

- La conversione dello schema AWS DMS valuta automaticamente la complessità della migrazione per il fornitore di dati di origine. Converte inoltre gli schemi del database e gli oggetti di codice in un formato compatibile con il database di destinazione e quindi applica il codice convertito.
- AWS DMS ti consente di passare a un motore di database moderno e forse più conveniente di quello attualmente in esecuzione. Ad esempio, AWS DMS può aiutarti a sfruttare i servizi di database gestiti forniti da Amazon Relational Database Service (Amazon RDS) o Amazon Aurora. Oppure ti consente di passare al servizio di data warehouse gestito fornito da Amazon Redshift, alle piattaforme NoSQL come Amazon DynamoDB o a piattaforme di archiviazione a costi contenuti, come Amazon Simple Storage Service (Amazon S3). Al contrario, se desideri eseguire la migrazione dalla vecchia infrastruttura, ma continuare a utilizzare lo stesso motore di database, AWS DMS supporta anche questo processo.
- AWS DMS supporta quasi tutti i motori del DBMS più diffusi al momento come endpoint di origine. Per ulteriori informazioni, consulta [Origini per la migrazione dei dati](#).
- AWS DMS offre un'ampia copertura dei motori di destinazione disponibili. Per ulteriori informazioni, consulta [Destinazioni per la migrazione dei dati](#).
- Puoi eseguire la migrazione da qualsiasi origine dati supportata a qualsiasi destinazione dati supportata. AWS DMS supporta migrazioni dei dati completamente eterogenee tra i motori supportati.
- AWS DMS garantisce la migrazione dei dati sicura. La crittografia dei dati inattivi avviene con AWS Key Management Service (AWS KMS). Durante la migrazione, puoi utilizzare SSL (Secure Socket Layer) per crittografare i dati in transito dall'origine alla destinazione.

Come funziona AWS Database Migration Service

AWS Database Migration Service (AWS DMS) è un servizio Web che puoi utilizzare per migrare i dati da un data store di origine a un data store di destinazione. Questi due data store vengono chiamati endpoint. È possibile eseguire la migrazione tra endpoint di origine e di destinazione che utilizzano lo stesso motore di database, ad esempio da un database Oracle a un database Oracle. È possibile eseguire la migrazione anche tra endpoint di origine e di destinazione che utilizzano diversi motori di database, ad esempio da un database Oracle a un database PostgreSQL. L'unico requisito da utilizzare AWS DMS è che uno degli endpoint deve essere collegato a un AWS servizio. Non è possibile eseguire AWS DMS la migrazione da un database locale a un altro database locale.

Per informazioni sui costi di migrazione di database, consulta la [pagina dei prezzi di AWS Database Migration Service](#).

Utilizza i seguenti argomenti per comprendere meglio. AWS DMS

Argomenti

- [Visualizzazione di alto livello di AWS DMS](#)
- [Componenti di AWS DMS](#)
- [Fonti per AWS DMS](#)
- [Obiettivi per AWS DMS](#)
- [Creazione di un Amazon Resource Name \(ARN\) per AWS DMS](#)
- [Utilizzo AWS DMS con altri servizi AWS](#)

Visualizzazione di alto livello di AWS DMS

Per eseguire una migrazione del database, AWS DMS si connette al data store di origine, legge i dati di origine e li formatta per l'utilizzo da parte del data store di destinazione. Successivamente, carica i dati nel data store di destinazione. La maggior parte di questo processo avviene nella memoria, anche se transazioni di grandi dimensioni potrebbero richiedere buffering su disco. Anche le transazioni e i file di log memorizzati nella cache vengono scritti su disco.

A un livello elevato, durante l'utilizzo, AWS DMS procedi come segue:

- Individua i database presenti nel tuo ambiente di rete che sono buoni candidati per la migrazione.

- Converti automaticamente gli schemi del database di origine e la maggior parte degli oggetti di codice del database in un formato compatibile con il database di destinazione.
- Creazione di un server di replica.
- Creazione di endpoint di origine e di destinazione che hanno informazioni di connessione sui datastore.
- Creazione di una o più attività di migrazione per migrare i dati tra i datastore di origine e di destinazione.

Un'attività può essere composta da tre fasi principali:

- Migrazione dei dati esistenti (pieno carico)
- L'applicazione delle modifiche memorizzate nella cache
- Replica continua (acquisizione dei dati di modifica)

Durante una migrazione a pieno carico, in cui i dati esistenti dall'origine vengono spostati nella destinazione, AWS DMS carica i dati dalle tabelle del data store di origine alle tabelle del data store di destinazione. Mentre il caricamento completo è in corso, tutte le modifiche apportate alle tabelle in fase di caricamento vengono memorizzate nella cache del server di replica; queste sono le modifiche memorizzate nella cache. È importante notare che AWS DMS non acquisisce le modifiche per una determinata tabella finché non viene avviato il caricamento completo di quella tabella. In altre parole, il punto di inizio dell'acquisizione delle modifiche è diverso per ogni singola tabella.

Quando il caricamento completo di una determinata tabella è completo, inizia AWS DMS immediatamente ad applicare le modifiche memorizzate nella cache per quella tabella. Una volta caricata la tabella e applicate le modifiche memorizzate nella cache, AWS DMS inizia a raccogliere le modifiche come transazioni per la fase di replica in corso. Se una transazione include tabelle non ancora completamente caricate, le modifiche vengono archiviate localmente nell'istanza di replica. Dopo aver AWS DMS applicato tutte le modifiche memorizzate nella cache a tutte le tabelle, le tabelle sono coerenti dal punto di vista transazionale. A questo punto, AWS DMS passa alla fase di replica in corso, applicando le modifiche come transazioni.

All'inizio della fase di replica continua, un backlog di transazioni provoca generalmente un ritardo tra i database di origine e di destinazione. La migrazione raggiunge infine uno stato stabile dopo aver superato questo backlog di transazioni. A questo punto, è possibile chiudere le applicazioni, consentire l'applicazione di eventuali transazioni rimanenti alla destinazione e rilanciare le applicazioni, rivolte ora al database di destinazione.

AWS DMS crea gli oggetti dello schema di destinazione necessari per eseguire una migrazione dei dati. È possibile AWS DMS utilizzarlo per adottare un approccio minimalista e creare solo gli oggetti necessari per migrare in modo efficiente i dati. Utilizzando questo approccio, vengono AWS DMS create tabelle, chiavi primarie e, in alcuni casi, indici univoci, ma non vengono creati altri oggetti che non siano necessari per la migrazione efficiente dei dati dall'origine.

In alternativa, è possibile utilizzare DMS Schema Conversion within AWS DMS per convertire automaticamente gli schemi del database di origine e la maggior parte degli oggetti di codice del database in un formato compatibile con il database di destinazione. Questa conversione include tabelle, viste, stored procedure, funzioni, tipi di dati, sinonimi e così via. Tutti gli oggetti che la conversione dello schema DMS non è in grado di convertire automaticamente sono contrassegnati in modo chiaro. Per completare la migrazione, puoi convertire questi oggetti manualmente.

Componenti di AWS DMS

Questa sezione descrive i componenti interni AWS DMS e il modo in cui funzionano insieme per eseguire la migrazione dei dati. Capire i componenti sottostanti di AWS DMS aiuta a migrare i dati in modo più efficiente e a ottenere informazioni migliori durante l'analisi o la risoluzione dei problemi.

Una AWS DMS migrazione è composta da cinque componenti: individuazione dei database da migrare, conversione automatica dello schema, un'istanza di replica, endpoint di origine e destinazione e un'attività di replica. È possibile creare una AWS DMS migrazione creando l'istanza di replica, gli endpoint e le attività necessari in un. Regione AWS

Individuazione dei database

DMS Fleet Advisor raccoglie i dati da più ambienti di database per fornire approfondimenti sull'infrastruttura dei dati. DMS Fleet Advisor raccoglie i dati dal database on-premise e dai server di analisi da una o più postazioni centrali senza la necessità di installarlo su ogni computer. Attualmente, DMS Fleet Advisor supporta i server di database Microsoft SQL Server, MySQL, Oracle e PostgreSQL.

Sulla base dei dati rilevati dalla rete, DMS Fleet Advisor crea un inventario che è possibile esaminare per determinare quali server di database e oggetti monitorare. Una volta raccolti i dettagli su questi server, database e schemi, è possibile analizzare la fattibilità delle migrazioni di database previste.

Migrazione di schema e codice

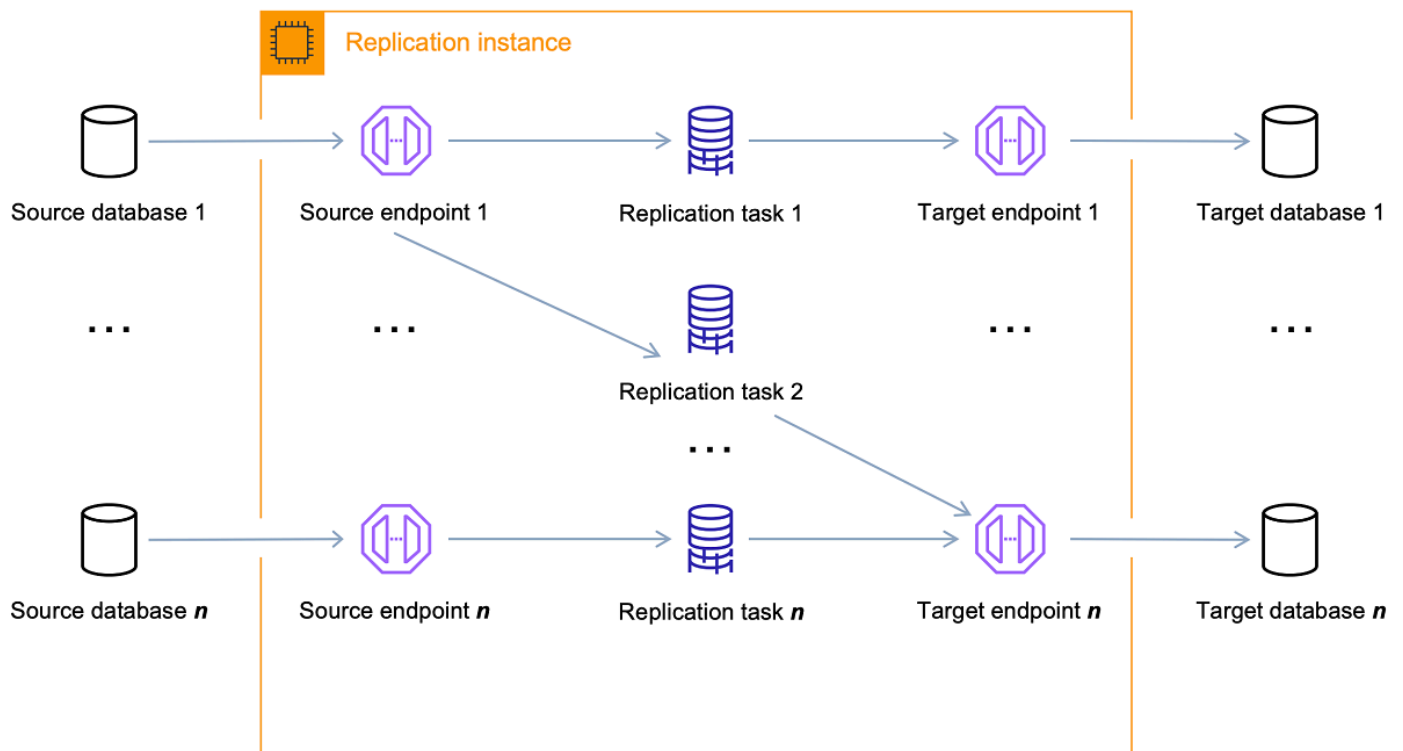
La conversione dello schema DMS AWS DMS rende più prevedibili le migrazioni di database tra diversi tipi di database. È possibile utilizzare la conversione dello schema DMS per valutare la complessità della migrazione per il fornitore di dati di origine e per convertire schemi di database e oggetti di codice. Puoi quindi applicare il codice convertito al database di destinazione.

Ad alto livello, la conversione dello schema DMS funziona con i seguenti tre componenti: profili dell'istanza, fornitore di dati e progetti di migrazione. Un profilo dell'istanza specifica le impostazioni di rete e di sicurezza. Un fornitore di dati archivia le credenziali di connessione al database. Un progetto di migrazione contiene fornitori di dati, un profilo di istanza e regole di migrazione. AWS DMS utilizza fornitori di dati e un profilo di istanza per progettare un processo che converte gli schemi di database e gli oggetti di codice.

Istanza di replica

Ad alto livello, un'istanza di AWS DMS replica è semplicemente un'istanza gestita di Amazon Elastic Compute Cloud (Amazon EC2) che ospita una o più attività di replica.

La figura seguente mostra un esempio di istanza di replica che esegue diverse attività di replica associate.



Una singola istanza di replica può ospitare una o più attività di replica, a seconda delle caratteristiche della migrazione e della capacità del server di replica. AWS DMS fornisce una varietà di istanze di replica in modo da poter scegliere la configurazione ottimale per il proprio caso d'uso. Per ulteriori informazioni sulle varie classi di istanze di replica, consulta [Scelta dell'istanza di replica AWS DMS giusta per la migrazione](#).

AWS DMS crea l'istanza di replica su un'istanza Amazon EC2. Alcune delle classi di istanze più piccole sono sufficienti per testare il servizio o per migrazioni di piccole dimensioni. Se la migrazione coinvolge un numero elevato di tabelle oppure se desideri eseguire diverse attività di replica simultanee, è opportuno valutare l'utilizzo di una delle istanze di dimensioni maggiori. Ti consigliamo questo approccio poiché AWS DMS può consumare una notevole quantità di memoria e di CPU.

In base alla classe di istanza Amazon EC2 selezionata, l'istanza di replica dispone di 50 GB o 100 GB di archiviazione di dati. Tale quantità è in genere sufficiente per la maggior parte dei clienti. Tuttavia, se la migrazione include transazioni di grandi dimensioni o un volume elevato di modifiche dei dati, è possibile aumentare l'allocazione di storage di base. Il Change Data Capture (CDC) può determinare la scrittura dei dati sul disco, a seconda della velocità a cui la destinazione è in grado di scrivere le modifiche. Poiché i file di log vengono scritti anche sul disco, l'aumento del livello di gravità della registrazione comporta anche un maggiore consumo di spazio di storage.

AWS DMS può fornire elevata disponibilità e supporto per il failover utilizzando una distribuzione Multi-AZ. In un'implementazione Multi-AZ, effettua AWS DMS automaticamente il provisioning e mantiene una replica in standby dell'istanza di replica in una zona di disponibilità diversa. L'istanza di replica primaria viene replicata in modo sincrono nella replica di standby. Se l'istanza di replica primaria incorre in un guasto o non risponde, l'istanza di standby riprende tutte le attività in esecuzione con un'interruzione minima. Poiché l'istanza primaria replica costantemente il suo stato sull'istanza di standby, un'implementazione Multi-AZ riscontra una certa riduzione delle prestazioni.

Per informazioni più dettagliate sull'istanza di AWS DMS replica, vedere [Utilizzo di un'istanza di AWS DMS replica](#)

Anziché creare e gestire un'istanza di replica, puoi consentire il provisioning automatico della replica utilizzando Serverless. AWS DMS Per ulteriori informazioni, consulta [Lavorare con AWS DMS Serverless](#).

Endpoint

AWS DMS utilizza un endpoint per accedere al data store di origine o di destinazione. Le informazioni di connessione specifiche sono diverse, a seconda del datastore, ma in generale è possibile specificare le informazioni riportate di seguito al momento della creazione di un endpoint.

- Tipo di endpoint: origine o destinazione.
- Tipo di motore: tipo di motore di database, ad esempio Oracle o PostgreSQL.
- Nome server: nome del server o indirizzo IP AWS DMS raggiungibile.
- Porta: numero di porta utilizzato per le connessioni al server di database.
- Crittografia: modalità SSL (Secure Sockets Layer), se SSL è utilizzato per crittografare la connessione.
- Credenziali: nome utente e password per un account con i diritti di accesso richiesti.

Quando si crea un endpoint utilizzando la AWS DMS console, la console richiede di testare la connessione dell'endpoint. Il test deve avere esito positivo prima di utilizzare l'endpoint in un'attività. AWS DMS Come per le informazioni di connessione, i criteri di test specifici sono diversi per tipi di motori diversi. In generale, AWS DMS verifica che il database esista per il nome e la porta di un dato server e che le credenziali fornite possano essere utilizzate per la connessione al database con i privilegi necessari per eseguire una migrazione. Se il test di connessione ha esito positivo, AWS DMS scarica e archivia le informazioni sullo schema da utilizzare successivamente durante la configurazione dell'attività. Le informazioni sullo schema possono includere le definizioni di tabella, le definizioni delle chiavi primarie e le definizioni delle chiavi univoche, ad esempio.

Più attività di replica possono utilizzare un singolo endpoint. Ad esempio, si possono avere due applicazioni logicamente distinte in hosting sullo stesso database di origine, da migrare separatamente. In questo caso, è possibile creare due attività di replica, una per ogni set di tabelle dell'applicazione. È possibile utilizzare lo stesso AWS DMS endpoint in entrambe le attività.

È possibile personalizzare il comportamento di un endpoint utilizzando le impostazioni degli endpoint. Le impostazioni degli endpoint possono controllare vari comportamenti come il dettaglio della registrazione, le dimensioni dei file e altri parametri. Per ogni tipo di motore di datastore sono disponibili diverse impostazioni degli endpoint. Puoi trovare le impostazioni degli endpoint specifiche per ogni datastore nella sezione di origine o di destinazione di quel datastore. Per un elenco di datastore di origine e di destinazione supportati, consulta [Fonti per AWS DMS](#) e [Obiettivi per AWS DMS](#).

Per informazioni più dettagliate sugli AWS DMS endpoint, consulta. [Utilizzo degli endpoint AWS DMS](#)

Attività di replica

Si utilizza un'attività di AWS DMS replica per spostare un set di dati dall'endpoint di origine all'endpoint di destinazione. La creazione di un'attività di replica è l'ultima fase da intraprendere prima di avviare una migrazione.

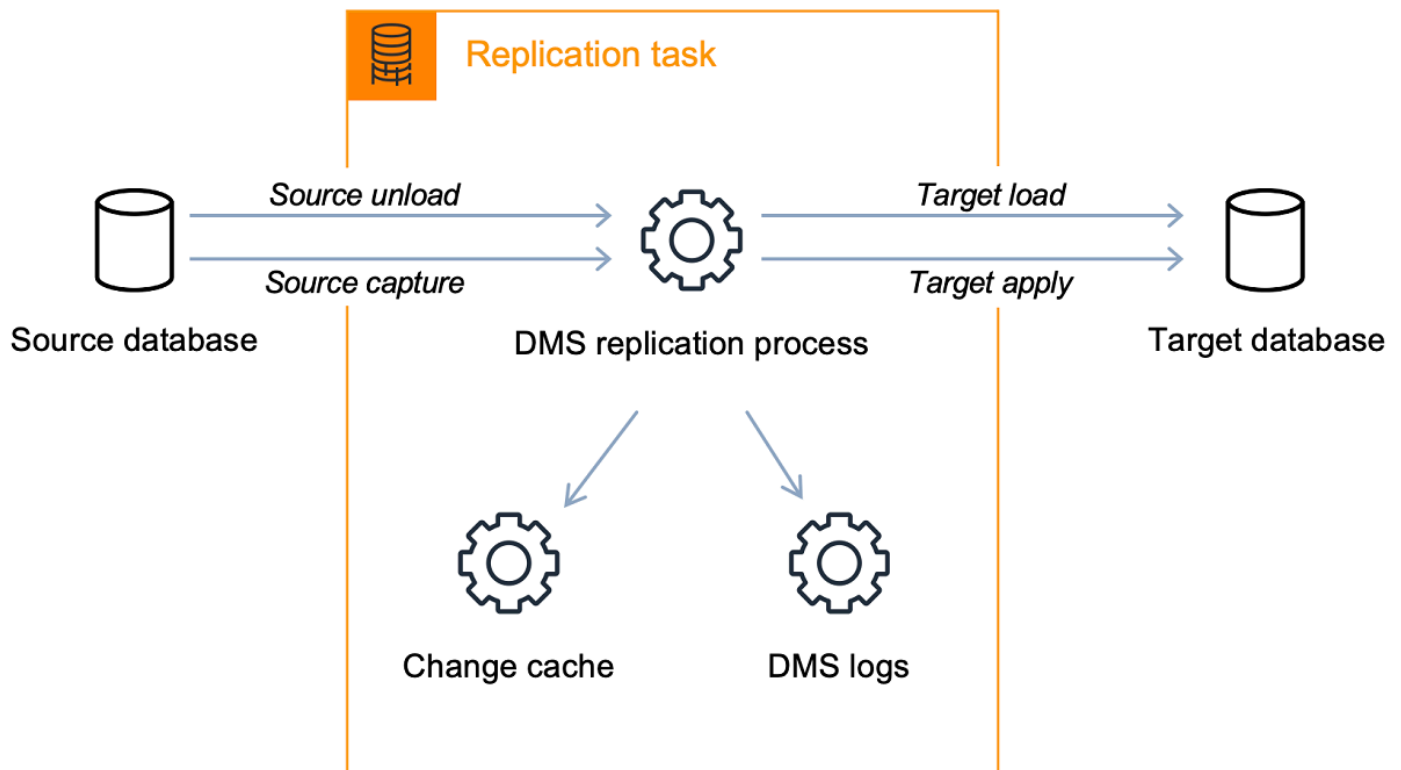
Quando si crea un'attività di replica, è necessario specificare le seguenti impostazioni delle attività:

- Istanza di replica: l'istanza che ospita ed esegue l'attività
- Source endpoint (Endpoint di origine)
- Target endpoint (Endpoint di destinazione)
- Opzioni del tipo di migrazione, elencate di seguito. Per una spiegazione completa delle opzioni di tipo di migrazione, consulta [Creazione di un'attività](#).
 - Pieno carico (migrazione dei dati esistenti): se puoi permetterti un'interruzione abbastanza lunga per copiare i dati esistenti, questa è l'opzione ideale. Questa opzione esegue semplicemente la migrazione dei dati dal database di origine al database di destinazione, creando tabelle quando necessario.
 - Pieno carico e CDC (migrazione dei dati esistenti e replica delle modifiche in corso): questa opzione esegue un pieno carico dei dati durante l'acquisizione delle modifiche sull'origine. Dopo la conclusione del caricamento completo, le modifiche acquisite vengono applicate alla destinazione. L'applicazione delle modifiche raggiunge infine uno stato stabile. A questo punto, è possibile chiudere le applicazioni, lasciare che le modifiche rimanenti raggiungano la destinazione e riavviare quindi le applicazioni che puntano alla destinazione.
 - sola CDC (replica solo le modifiche ai dati): in alcune situazioni, potrebbe essere più efficiente copiare i dati esistenti utilizzando un metodo diverso da AWS DMS. Ad esempio, in una migrazione omogenea, l'utilizzo di strumenti di importazione/esportazione nativi potrebbe essere più efficiente per il caricamento dei dati in blocco. In questa situazione, è possibile replicare le modifiche AWS DMS a partire dall'avvio del caricamento in blocco per portare e mantenere sincronizzati i database di origine e di destinazione.
- Opzioni di modalità di preparazione tabella di destinazione, elencate di seguito. Per una spiegazione completa delle modalità della tabella di destinazione, consulta [Creazione di un'attività](#).

- Non eseguire alcuna operazione: AWS DMS si presuppone che le tabelle di destinazione siano precreate sulla destinazione.
- Elimina le tabelle di destinazione: AWS DMS elimina e ricrea le tabelle di destinazione.
- Tronca: se hai creato tabelle sulla destinazione, AWS DMS le tronca prima dell'inizio della migrazione. Se non esistono tabelle e si seleziona questa opzione, AWS DMS crea le tabelle mancanti.
- Opzioni di modalità LOB, elencate di seguito. Per una spiegazione completa delle modalità LOB, consulta [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#).
 - Non includere le colonne LOB: le colonne LOB vengono escluse dalla migrazione.
 - Modalità LOB completa: migra LOB completi indipendentemente dalle dimensioni. AWS DMS migra i LOB a tratti in blocchi controllati dal parametro Max LOB Size. Questa modalità è più lenta rispetto alla modalità LOB limitata.
 - Modalità LOB limitata: tronca i LOB in base al valore del parametro Dimensione LOB massima. Questa modalità è più veloce rispetto alla modalità LOB completa.
- Mappature delle tabelle: indica le tabelle da migrare e il modo in cui vengono migrate. Per ulteriori informazioni, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#).
- Trasformazioni di dati, elencate di seguito. Per ulteriori informazioni sulle trasformazioni dei dati, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).
 - Modifica di nomi di schemi, di tabelle e di colonne.
 - Modifica di nomi di spazio tabelle (per gli endpoint Oracle di destinazione).
 - Definizione di chiavi primarie e indici univoci sulla destinazione.
- Convalida dei dati
- CloudWatch Registrazione su Amazon

Puoi utilizzare l'attività per migrare i dati dall'endpoint di origine all'endpoint di destinazione e l'elaborazione dell'attività viene eseguita sull'istanza di replica. Puoi specificare le tabelle e gli schemi da migrare e qualsiasi elaborazione particolare, ad esempio i requisiti di registrazione, i dati della tabella di controllo e la gestione degli errori.

Concettualmente, un'attività di AWS DMS replica svolge due funzioni distinte, come illustrato nel diagramma seguente.



Il processo di caricamento completo è semplice da comprendere. I dati vengono estratti dall'origine attraverso un metodo di estrazione in blocco e caricati direttamente nella destinazione. È possibile specificare il numero di tabelle da estrarre e caricare in parallelo sulla AWS DMS console in Impostazioni avanzate.

Per ulteriori informazioni sulle AWS DMS attività, vedere [Utilizzo delle attività di AWS DMS](#).

Replica continua o Change Data Capture (CDC)

È inoltre possibile utilizzare un' AWS DMS attività per acquisire le modifiche in corso all'archivio dati di origine durante la migrazione dei dati verso una destinazione. Il processo di acquisizione delle modifiche AWS DMS utilizzato per replicare le modifiche in corso da un endpoint di origine raccoglie le modifiche ai log del database utilizzando l'API nativa del motore di database.

Nel processo CDC, l'attività di replica è stata concepita per lo streaming delle modifiche dall'origine alla destinazione, utilizzando buffer in memoria per mantenere i dati in transito. Se i buffer in memoria si esauriscono per qualsiasi motivo, l'attività di replica distribuisce le modifiche in sospeso nella cache delle modifiche sul disco. Ciò potrebbe verificarsi, ad esempio, se le modifiche AWS DMS vengono acquisite dall'origine più rapidamente di quanto possano essere applicate alla destinazione. In questo caso, si osserva che la latenza di destinazione dell'attività supera la latenza di origine dell'attività.

Puoi verificarlo accedendo alla tua attività sulla AWS DMS console e aprendo la scheda Task Monitoring. I LatencySource grafici CDC LatencyTarget e CDC sono mostrati nella parte inferiore della pagina. Se disponi di un'attività che mostra latenza di destinazione, è probabile che sia necessaria un'ottimizzazione sull'endpoint di destinazione per aumentare la velocità dell'applicazione.

L'attività di replica, inoltre, utilizza lo storage per i log di attività come descritto in precedenza. Lo spazio su disco preconfigurato con l'istanza di replica è in genere sufficiente per la registrazione e per le modifiche distribuite. Se hai bisogno di ulteriore spazio su disco, ad esempio quando utilizzi il debug dettagliato per analizzare un problema di migrazione, è possibile modificare l'istanza di replica per allocare più spazio.

Fonti per AWS DMS

È possibile utilizzare diversi archivi di dati di origine in diverse AWS DMS funzionalità. Le seguenti sezioni contengono gli elenchi degli archivi di dati di origine supportati per ogni AWS DMS funzionalità.

Argomenti

- [Endpoint di origine per la migrazione dei dati](#)
- [Database di origine per DMS Fleet Advisor](#)
- [Provider di dati di origine per la conversione dello schema DMS](#)
- [Provider di dati di origine per migrazioni omogenee di dati DMS](#)


Endpoint di origine per la migrazione dei dati

Puoi utilizzare i seguenti datastore come endpoint di origine per la migrazione dei dati tramite AWS DMS.

Database locali e di istanze EC2


- Oracle 10.2 e versioni successive (per le versioni 10.x), 11g e fino a 12.2, 18c e 19c per le edizioni Enterprise, Standard, Standard One e Standard Two.
- Microsoft SQL Server versioni 2005, 2008, 2008R2, 2012, 2014, 2016, 2017, 2019 e 2022.
 - Le edizioni Enterprise, Standard, Workgroup, Developer e Web supportano la replica a pieno carico.

- Le edizioni Enterprise, Standard (versione 2016 e successive) e Developer supportano la replica CDC (continua) oltre al caricamento completo.
- L'edizione Express non è supportata.
- MySQL versioni 5.5, 5.6, 5.7 e 8.0.

 Note


Il supporto per MySQL 8.0 come sorgente è disponibile AWS DMS nelle versioni 3.4.0 e successive, tranne quando il payload della transazione è compresso. Il supporto per Google Cloud for MySQL 8.0 come sorgente è disponibile AWS DMS nelle versioni 3.4.6 e successive.

- MariaDB (supportato come origine dati compatibile con MySQL) 10.0 (solo versioni 10.0.24 e successive), 10.2, 10.3, 10.4, 10.5 e 10.6.

 Note


Il supporto per MariaDB come sorgente è disponibile in AWS DMS tutte le versioni in cui è supportato MySQL.

- PostgreSQL versione 9.4 e successive (per le versioni 9.x), 10.x, 11.x, 12.x, 13.x 14.x, 15.x e 16.x.

 Note

AWS DMS supporta solo PostgreSQL versione 15.x nelle versioni 3.5.1 e successive. AWS DMS supporta solo la versione 16.x di PostgreSQL nelle versioni 3.5.3 e successive.

- MongoDB versioni 3.x, 4.0, 4.2, 4.4, 5.0 e 6.0

 Note

AWS DMS le versioni 3.5.0 e successive non supportano le versioni di MongoDB precedenti alla 3.6.

- SAP Adaptive Server Enterprise (ASE) 12.5, 15, 15.5, 15.7, 16 e versioni successive.
- IBM Db2 per le versioni Linux, UNIX e Windows (Db2 LUW):
 - Versione 9.7, tutti i Fix Pack


- Versione 10.1, tutti i Fix Pack
- Versione 10.5, tutti i Fix Pack eccetto Fix Pack 5
- Versione 11.1, tutti i Fix Pack
- Versione 11.5, Mods (0-8) con solo Fix Pack Zero
- IBM Db2 per z/OS versione 12

Servizi di database gestiti da terze parti:

- Database SQL di Microsoft Azure
- Microsoft Azure PostgreSQL Flexible Server versioni 11.2, 12.15, 13.11, 14.8 e 15.3.
- Microsoft Azure MySQL Flexible Server versioni 5.7 e 8.
- Google Cloud per MySQL versioni 5.6, 5.7 e 8.0.
- Google Cloud per PostgreSQL versioni 9.6, 10, 11, 12, 13, 14 e 15.
- OCI MySQL Heatwave versione 8.0.34.


Database di istanza Amazon RDS e Amazon Simple Storage Service (Amazon S3)

- Oracle versioni 11g (11.2.0.4 e versioni successive) e fino a 12.2, 18c e 19c per le edizioni Enterprise, Standard, Standard One e Standard Two
- Microsoft SQL Server versioni 2012, 2014, 2016, 2017, 2019 e 2022 per le edizioni Enterprise, Standard, Workgroup e Developer.

 Note


AWS DMS non supporta SQL Server Express. L'edizione Web è supportata solo per la replica di pieno carico.

- MySQL versioni 5.5, 5.6, 5.7 e 8.0.

 Note


Il supporto per MySQL 8.0 come sorgente è disponibile AWS DMS nelle versioni 3.4.0 e successive, tranne quando il payload della transazione è compresso.

- MariaDB (supportato come origine dati compatibile con MySQL) versioni da 10.0.24 a 10.0.28, 10.2, 10.3, 10.4, 10.5 e 10.6.

 Note

Il supporto per MariaDB come sorgente è disponibile in AWS DMS tutte le versioni in cui è supportato MySQL.

- PostgreSQL versione 10.x, 11.x, 12.x, 13.x, 14.x, 15.x e 16.x.

 Note

AWS DMS supporta solo PostgreSQL versione 15.x nelle versioni 3.5.1 e successive. AWS DMS supporta solo la versione 16.x di PostgreSQL nelle versioni 3.5.3 e successive.

- Amazon Aurora con compatibilità MySQL (supportato come origine dati compatibile con MySQL).
- Amazon Aurora con compatibilità PostgreSQL (supportato come origine dati compatibile con PostgreSQL).
- Amazon S3
- Amazon DocumentDB (con compatibilità con MongoDB) versioni 3.6, 4.0 e 5.0.
- Amazon RDS per IBM Db2 LUW.

[Per informazioni sull'utilizzo di una fonte specifica, consulta Lavorare con gli endpoint. AWS DMS](#)

Per informazioni sugli endpoint di destinazione supportati, consulta [Endpoint di destinazione per la migrazione dei dati](#).

Database di origine per DMS Fleet Advisor

DMS Fleet Advisor supporta i seguenti database di origine.

- Microsoft SQL Server versione 2012 e fino alla 2019
- MySQL versione 5.6 fino alla 8
- Oracle versione 11g release 2 e fino a 12c, 19c e 21c
- PostgreSQL versione 9.6 e fino alla 13

Per informazioni sull'utilizzo di un'origine specifica, consulta [Creazione di utenti di database per AWS DMS Fleet Advisor](#).

Per l'elenco dei database utilizzati da DMS Fleet Advisor per generare raccomandazioni di destinazione, consulta [Destinazioni per DMS Fleet Advisor](#).

Provider di dati di origine per la conversione dello schema DMS

La conversione dello schema DMS supporta i seguenti fornitori di dati come origini per i progetti di migrazione.

- Microsoft SQL Server versioni 2008 R2, 2012, 2014, 2016, 2017 e 2019.
- Oracle versione 10.2 e successive, 11g e fino alla 12.2, 18c e 19c e Oracle Data Warehouse.
- PostgreSQL versione 9.2 e successive
- MySQL versione 5.5 e successive

Il fornitore di dati di origine può essere un motore autogestito in esecuzione on-premise o su un'istanza Amazon Elastic Compute Cloud (Amazon EC2).

Per informazioni sull'utilizzo di un'origine specifica, consulta [Creazione di fornitori di dati di origine per la conversione dello schema DMS](#).

Per informazioni sui database di destinazione supportati, consulta [Provider di dati di destinazione per la conversione dello schema DMS](#).

Il AWS Schema Conversion Tool (AWS SCT) supporta più database di origine e di destinazione rispetto a DMS Schema Conversion. Per informazioni sui database che AWS SCT supportano, vedete [What is the AWS Schema Conversion Tool](#).

Provider di dati di origine per migrazioni omogenee di dati DMS

Puoi utilizzare i seguenti fornitori di dati come origini per le migrazioni omogenee di dati.

- MySQL versione 5.7 e successive.
- MariaDB versione 10.2 e successive.
- PostgreSQL versione 10.4 fino alla 14.x.
- MongoDB versione 4.x, 5.x, 6.0
- Amazon DocumentDB versione 3.6, 4.0, 5.0

Il fornitore di dati di origine può essere un motore autogestito in esecuzione on-premise o su un'istanza Amazon EC2. Inoltre, puoi utilizzare un'istanza database Amazon RDS come fornitore di dati di origine.

Per informazioni sull'utilizzo di un'origine specifica, consulta [Creazione di fornitori di dati di origine per migrazioni di dati omogenee in AWS DMS](#).

Per informazioni sui database di destinazione supportati, consulta [Provider di dati di destinazione per migrazioni omogenee di dati DMS](#).

Obiettivi per AWS DMS

È possibile utilizzare diversi archivi di dati di destinazione AWS DMS con funzionalità diverse. Le seguenti sezioni contengono gli elenchi degli archivi di dati di destinazione supportati per ciascuna AWS DMS funzionalità.

Argomenti

- [Endpoint di destinazione per la migrazione dei dati](#)
- [Database di destinazione per DMS Fleet Advisor](#)
- [Provider di dati di destinazione per la conversione dello schema DMS](#)
- [Provider di dati di destinazione per migrazioni omogenee di dati DMS](#)

Endpoint di destinazione per la migrazione dei dati

Puoi utilizzare i seguenti datastore come endpoint di destinazione per la migrazione dei dati tramite AWS DMS.


Database locali e di istanze Amazon EC2

- Oracle versioni 10g, 11g, 12c, 18c e 19c per le edizioni Enterprise, Standard, Standard One e Standard Two.
- Microsoft SQL Server versioni 2005, 2008, 2008R2, 2012, 2014, 2016, 2017, 2019 e 2022 per le edizioni Enterprise, Standard, Workgroup e Developer.

Note


AWS DMS non supporta le edizioni SQL Server Web ed Express.

- MySQL versioni 5.5, 5.6, 5.7 e 8.0.
- MariaDB (supportato come destinazione dati compatibile con MySQL) versioni da 10.0.24 a 10.0.28, 10.2, 10.3, 10.4, 10.5 e 10.6.

 Note

Il supporto per MariaDB come destinazione è disponibile in AWS DMS tutte le versioni in cui è supportato MySQL.

- PostgreSQL versione 9.4 e successive (per le versioni 9.x), 10.x, 11.x, 12.x, 13.x, 14.x, 15.x e 16.x.


 Note

AWS DMS supporta PostgreSQL 15.x solo nelle versioni 3.5.1 e successive. AWS DMS supporta solo la versione 16.x di PostgreSQL nelle versioni 3.5.3 e successive.

- SAP Adaptive Server Enterprise (ASE) 15, 15.5, 15.7, 16 e versioni successive.
- Redis versioni 6.x.

Database di istanze Amazon RDS, Amazon Redshift, Amazon Redshift Serverless, Amazon DynamoDB, Amazon S3, Amazon Service, Amazon for Redis, Amazon Kinesis OpenSearch Data Streams, ElastiCache Amazon DocumentDB, Amazon Neptune e Apache Kafka

- Oracle versioni 11g (versione 11.2.0.3.v1 e successive), 12c, 18c e 19c per le edizioni Enterprise, Standard, Standard One e Standard Two.
- Microsoft SQL Server versioni 2012, 2014, 2016, 2017, 2019 e 2022 per le edizioni Enterprise, Standard, Workgroup e Developer.

 Note

AWS DMS non supporta le edizioni SQL Server Web ed Express.

- MySQL versioni 5.5, 5.6, 5.7 e 8.0.
- MariaDB (supportato come destinazione dati compatibile con MySQL) versioni da 10.0.24 a 10.0.28, 10.2, 10.3, 10.4, 10.5 e 10.6.

Note

Il supporto per MariaDB come destinazione è disponibile in AWS DMS tutte le versioni in cui è supportato MySQL.

- PostgreSQL versione 10.x, 11.x, 12.x, 13.x, 14.x, 15.x e 16.x.

Note

AWS DMS supporta PostgreSQL 15.x solo nelle versioni 3.5.1 e successive. AWS DMS supporta PostgreSQL 16.x solo nelle versioni 3.5.3 e successive.

- IBM Db2 LUW versioni 11.1 e 11.5
- Amazon Aurora edizione compatibile con MySQL
- Amazon Aurora PostgreSQL-Compatible Edition
- Amazon Aurora serverless v2
- Amazon Redshift
- Amazon Redshift Serverless
- Amazon S3
- Amazon DynamoDB
- OpenSearch Servizio Amazon
- Amazon ElastiCache per Redis
- Flusso di dati Amazon Kinesis
- Amazon DocumentDB (compatibile con MongoDB)
- Amazon Neptune
- [Apache Kafka. Streaming gestito da Amazon per Apache Kafka \(Amazon MSK\) e Apache Kafka autogestito](#)
- Babelfish (versione 3.2.0 e successive) per Aurora PostgreSQL (versioni 15.3/14.8 e successive)

Per informazioni su come lavorare con un obiettivo specifico, consulta [Lavorare con gli AWS DMS endpoints](#).

Per informazioni sugli endpoint di origine supportati, consulta [Endpoint di origine per la migrazione dei dati](#).

Database di destinazione per DMS Fleet Advisor

DMS Fleet Advisor genera raccomandazioni sulle destinazioni utilizzando la versione più recente dei seguenti database di destinazione.

- Amazon Aurora MySQL
- Amazon Aurora PostgreSQL
- Amazon RDS per MySQL
- Amazon RDS per Oracle
- Amazon RDS per PostgreSQL
- Amazon RDS per SQL Server

Per informazioni sulle raccomandazioni sulle destinazioni in DMS Fleet Advisor, consulta [Utilizzo della funzionalità dei suggerimenti delle destinazioni di AWS DMS Fleet Advisor](#).

Per informazioni sui database di origine supportati, consulta [Database di origine per DMS Fleet Advisor](#).

Provider di dati di destinazione per la conversione dello schema DMS

La conversione dello schema DMS supporta i seguenti fornitori di dati come destinazioni per i progetti di migrazione.

- Amazon Aurora MySQL 8.0.23
- Amazon Aurora PostgreSQL 14.5
- Amazon RDS per MySQL 8.0.23
- Amazon RDS per PostgreSQL 14.x
- Amazon Redshift

Per informazioni sull'utilizzo di una destinazione specifica, consulta [Creazione di fornitori di dati di destinazione per la conversione dello schema DMS](#).

Per informazioni sui database di origine supportati, consulta [Provider di dati di origine per la conversione dello schema DMS](#).

Provider di dati di destinazione per migrazioni omogenee di dati DMS

Puoi utilizzare i seguenti fornitori di dati come destinazioni per le migrazioni omogenee di dati.

- Amazon Aurora MySQL 5.7 e versioni successive
- Amazon Aurora PostgreSQL versione 10.4 fino alla 14.x
- Amazon Aurora serverless v2
- Amazon RDS per MySQL 5.7 e versioni successive
- Amazon RDS per MariaDB 10.2 e versioni successive
- Amazon RDS per PostgreSQL versione 10.4 fino alla 14.x
- Amazon DocumentDB versione 4.0, 5.0 e cluster Elastic DocumentDB

Per informazioni sull'utilizzo di una destinazione specifica, consulta [Creazione di fornitori di dati target per migrazioni di dati omogenee in AWS DMS](#).

Per informazioni sui database di origine supportati, consulta [Provider di dati di origine per migrazioni omogenee di dati DMS](#).

Creazione di un Amazon Resource Name (ARN) per AWS DMS

Se utilizzi l' AWS DMS API AWS CLI o per automatizzare la migrazione del database, allora lavori con Amazon Resource Name (ARNs). Ogni risorsa creata in Amazon Web Services è identificata da un ARN, che è un identificatore univoco. Se utilizzi l' AWS DMS API AWS CLI o per configurare la migrazione del database, fornisci l'ARN della risorsa con cui desideri lavorare.

Un ARN per una AWS DMS risorsa utilizza la seguente sintassi:

```
arn:aws:dms:region:account number:resourcetype:resourcename
```

In questa sintassi, si applica quanto segue:

- *region* è l'ID del Regione AWS luogo in cui è stata creata la AWS DMS risorsa, ad esempio. us-west-2

La tabella seguente mostra Regione AWS i nomi e i valori da utilizzare per la creazione di un ARN.

Regione	Nome
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacifico (Seoul)	ap-northeast-2
Regione Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Singapore)	ap-southeast-1
Asia Pacifico (Sydney)	ap-southeast-2
Canada (Centrale)	ca-central-1
Cina (Pechino)	cn-north-1
Regione Cina (Ningxia)	cn-northwest-1
Regione Europa (Stoccolma)	eu-north-1
Regione Europa (Milano)	eu-south-1
UE (Francoforte)	eu-central-1
Europa (Irlanda)	eu-west-1
UE (Londra)	eu-west-2
Regione UE (Parigi)	eu-west-3
Sud America (San Paolo)	sa-east-1
Stati Uniti orientali (Virginia settentrionale)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
Regione Stati Uniti occidentali (California settentrionale)	us-west-1
Stati Uniti occidentali (Oregon)	us-west-2

- *account number* è il numero dell'account senza trattini. Per trovare il numero del tuo account, accedi al tuo AWS account all'indirizzo <http://aws.amazon.com>, scegli Il mio account/console, quindi scegli Il mio account.
- *resourcetype* è il tipo di risorsa. AWS DMS

La tabella seguente mostra i tipi di risorse da utilizzare per la creazione di un ARN per una AWS DMS particolare risorsa.

AWS DMS tipo di risorsa	Formato ARN
Istanza di replica	<code>arn:aws:dms: <i>region</i>: <i>account</i>:rep: <i>resourcename</i></code>
Endpoint	<code>arn:aws:dms: <i>region</i>:<i>account</i>:endpoint: <i>resourcename</i></code>
Attività di replica	<code>arn:aws:dms: <i>region</i>:<i>account</i>:task:<i>resourcename</i></code>
Subnet group (Gruppo di sottoreti)	<code>arn:aws:dms: <i>region</i>:<i>account</i>:subgrp:<i>resourcename</i></code>

- *resourcename* è il nome della risorsa assegnato alla AWS DMS risorsa. Questa è una stringa generata in modo arbitrario.

La tabella seguente mostra esempi di ARN per AWS DMS le risorse. In questo caso, si presume di disporre dell'account AWS 123456789012 creato nella regione Stati Uniti orientali (Virginia settentrionale) con un nome di risorsa.

Tipo di risorsa	ARN di esempio
Istanza di replica	<code>arn:aws:dms:us-east-1:123456789012:rep:QLXQZ64MH7CXF4QCQMGRVYVXAI</code>
Endpoint	<code>arn:aws:dms:us-east-1:123456789012:endpoint:D3HMZ2IGUCGFF3NTAXUGF6S5A</code>
Attività di replica	<code>arn:aws:dms:us-east-1:123456789012:task:2PVREMNPGYJCVU2IBPTOYTIV4</code>

Tipo di risorsa	ARN di esempio
Subnet group (Gruppo di sottoreti)	arn:aws:dms:us-east-1:123456789012:subgrp:test-tag-grp

Utilizzo AWS DMS con altri servizi AWS

È possibile utilizzare AWS DMS con diversi altri AWS servizi:

- È possibile utilizzare un'istanza di Amazon EC2 o l'istanza database di Amazon RDS come destinazione per una migrazione dei dati.
- È possibile utilizzare il AWS Schema Conversion Tool (AWS SCT) per convertire lo schema di origine e il codice SQL in uno schema di destinazione e codice SQL equivalenti.
- È possibile utilizzare Amazon S3 come sito di storage per i dati o utilizzarlo come fase intermedia durante la migrazione di grandi quantità di dati.
- È possibile AWS CloudFormation utilizzarlo per configurare le AWS risorse per la gestione o l'implementazione dell'infrastruttura. Ad esempio, è possibile effettuare il provisioning di AWS DMS risorse come istanze di replica, attività, certificati ed endpoint. È possibile creare un modello che descrive tutte le AWS risorse desiderate e fornisce e configura tali AWS CloudFormation risorse al posto dell'utente.

AWS DMS supporto per AWS CloudFormation

È possibile fornire AWS DMS risorse utilizzando AWS CloudFormation. AWS CloudFormation è un servizio che consente di modellare e configurare AWS le risorse per la gestione o l'implementazione dell'infrastruttura. Ad esempio, è possibile fornire AWS DMS risorse come istanze di replica, attività, certificati ed endpoint. È necessario creare un modello che descrive tutte le AWS risorse desiderate e fornisce e configura tali AWS CloudFormation risorse al posto dell'utente.

Gli sviluppatori o gli amministratore di sistema possono creare e gestire raccolte di queste risorse e utilizzarle poi per le attività di migrazione ripetitive o per la distribuzione delle risorse nell'organizzazione. Per ulteriori informazioni in merito AWS CloudFormation, consulta [AWS CloudFormation i concetti](#) nella Guida per l'AWS CloudFormation utente.

AWS DMS supporta la creazione delle seguenti AWS DMS risorse utilizzando AWS CloudFormation:

- [AWS::DMS::Certificate](#)
- [AWS::DMS::Endpoint](#)
- [AWS::DMS::EventSubscription](#)
- [AWS::DMS::ReplicationInstance](#)
- [AWS::DMS::ReplicationSubnetGruppo](#)
- [AWS::DMS::ReplicationTask](#)

Nozioni di base su AWS Database Migration Service

Nel seguente tutorial sono presenti informazioni su come migrare un database tramite AWS Database Migration Service (AWS DMS).

Per eseguire la migrazione di un database, procedi come indicato di seguito:

1. Configura l'account AWS seguendo la procedura descritta in [Configurazione per AWS Database Migration Service](#).
2. Crea i database di esempio e un client Amazon EC2 per popolare il database di origine e testare la replica. Inoltre, crea un cloud privato virtuale (VPC) basato sul servizio Amazon Virtual Private Cloud (Amazon VPC) per contenere le risorse del tutorial. Per creare queste risorse, segui i passaggi indicati in [Prerequisiti per AWS Database Migration Service](#).
3. Popola il database di origine utilizzando uno [script di creazione di database di esempio](#).
4. Utilizza la conversione dello schema DMS o AWS Schema Conversion Tool (AWS SCT) per convertire lo schema dal database di origine al database di destinazione. Per utilizzare la conversione dello schema DMS, segui i passaggi indicati in [Nozioni di base sulla conversione dello schema DMS](#). Per convertire lo schema con AWS SCT, segui i passaggi indicati in [Migrazione dello schema](#).
5. Crea un'istanza di replica che esegua tutti i processi per la migrazione. Per eseguire questa operazione e le attività seguenti, segui i passaggi indicati in [Replica](#).
6. Specifica gli endpoint del database di origine e di destinazione. Per informazioni sulla creazione di endpoint, consulta [Creazione di endpoint di origine e destinazione](#).
7. Crea un'attività per definire le tabelle e i processi di replica da utilizzare, quindi avvia la replica. Per ulteriori informazioni sulla creazione di una attività di migrazione del database, consulta [Creazione di un'attività](#).
8. Verifica che la replica funzioni eseguendo query sul database di destinazione.

Configurazione per AWS Database Migration Service

Registrati per un Account AWS

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 procedura consigliata in materia di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire [attività che richiedono l'accesso da parte dell'utente root](#).

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo <https://aws.amazon.com/> e selezionando Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [AWS Management Console](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Signing in as the root user](#) della Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

Per istruzioni, consulta [Abilitare un dispositivo MFA virtuale per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

Per istruzioni, consulta [Abilitazione di AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta [Configurare l'accesso utente con le impostazioni predefinite IAM Identity Center directory](#) nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta [AWS Accedere al portale di accesso](#) nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

Per istruzioni, consulta [Creare un set di autorizzazioni](#) nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente.AWS IAM Identity Center

Prerequisiti per AWS Database Migration Service

In questa sezione, puoi apprendere le attività prerequisite per AWS DMS, come la configurazione dei database di origine e di destinazione. Come parte di queste attività, configuri anche un cloud privato virtuale (VPC) basato sul servizio Amazon VPC per contenere le tue risorse. Inoltre, configuri un'istanza Amazon EC2 da utilizzare per popolare il database di origine e verificare la replica sul database di destinazione.

Note

Il popolamento del database di origine richiede fino a 45 minuti.

In questo tutorial, crei un database MariaDB come origine e un database PostgreSQL come destinazione. Nello scenario si utilizzano motori di database a basso costo di uso comune per dimostrare la replica. L'utilizzo di diversi motori di database dimostra le AWS DMS funzionalità per la migrazione dei dati tra piattaforme eterogenee.

Le risorse di questo tutorial utilizzano la regione Stati Uniti occidentali (Oregon). Se desideri utilizzare una AWS regione diversa, specifica invece la regione prescelta ovunque appaia la regione degli Stati Uniti occidentali (Oregon).

Note

Per semplicità, i database che crei per questo tutorial non utilizzano la crittografia o altre funzionalità di sicurezza avanzate. È necessario invece usare le funzionalità di sicurezza per proteggere i database di produzione. Per ulteriori informazioni, consulta [Sicurezza in Amazon RDS](#).

Per i passaggi relativi ai prerequisiti, consulta i seguenti argomenti.

Argomenti

- [Crea un VPC](#)
- [Creazione di gruppi di parametri Amazon RDS](#)
- [Creazione del database Amazon RDS di origine](#)
- [Creazione del database Amazon RDS di destinazione](#)
- [Creazione di un client Amazon EC2](#)
- [Popolamento del database di origine](#)

Crea un VPC

In questa sezione, crei un VPC per contenere le tue AWS risorse. L'uso di un VPC è una best practice per l'utilizzo AWS delle risorse, in modo che i database, le istanze Amazon EC2, i gruppi di sicurezza e così via siano organizzati e sicuri in modo logico.

L'utilizzo di un VPC per le risorse del tutorial garantisce inoltre l'eliminazione di tutte le risorse impiegate al termine del tutorial. Prima di poter eliminare il VPC devi eliminare tutte le risorse che contiene.

Per creare un VPC da utilizzare con AWS DMS

1. [Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.](https://console.aws.amazon.com/vpc/)
2. Nel riquadro di navigazione, scegli Pannello di controllo VPC, quindi seleziona Crea VPC.
3. Nella pagina Crea VPC scegli le opzioni seguenti:
 - Risorse da creare: VPC e altro
 - Generazione automatica del tag del nome: scegli Generazione automatica e inserisci **DMSVPC**.
 - Blocco IPv4: **10.0.1.0/24**
 - Blocco CIDR IPv6: Nessun blocco CIDR IPv6
 - Tenancy: predefinito
 - Numero delle zone di disponibilità: 2
 - Numero di sottoreti pubbliche: 2
 - Numero di sottoreti private: 2
 - Gateway NAT (\$): nessuno
 - Endpoint VPC: nessuno

Seleziona Crea VPC.

4. Nel pannello di navigazione, scegli I tuoi VPC. Annota l'ID VPC di DMSVPC.
5. Nel riquadro di navigazione, scegli Gruppi di sicurezza.
6. Scegli il gruppo denominato default con l'ID VPC che corrisponde all'ID che hai annotato per DMSVPC.
7. Seleziona la scheda Regole in entrata, quindi scegli Modifica le regole in entrata.
8. Scegli Aggiungi regola. Aggiungi una regola di tipo MySQL/Aurora e scegli Ovunque-IPv4 per Fonte.
9. Scegli nuovamente Aggiungi regola. Aggiungi una regola di tipo PostgreSQL e scegli Ovunque-IPv4 per Fonte.
10. Scegliere Salva regole.

Creazione di gruppi di parametri Amazon RDS

Per specificare le impostazioni per i database di origine e di destinazione AWS DMS, utilizza i gruppi di parametri di Amazon RDS. Per consentire la replica iniziale e continua tra i database, assicurati di configurare quanto segue:

- Il log binario del database di origine, in modo che AWS DMS possa determinare quali aggiornamenti incrementali deve essere replicato.
- Il ruolo di replica del database di destinazione, in modo che AWS DMS ignori i vincoli di chiave esterna durante il trasferimento iniziale dei dati. Con questa impostazione, è AWS DMS possibile migrare i dati in modo errato.

Per creare gruppi di parametri da utilizzare con AWS DMS

1. Apri la console di Amazon RDS all'indirizzo <https://console.aws.amazon.com/rds/>.
2. Nel riquadro di navigazione scegli Gruppi di parametri.
3. Nella pagina Gruppi di parametri scegli Crea gruppo di parametri.
4. Nella pagina Crea gruppo di parametri immetti le seguenti impostazioni:
 - Famiglia del gruppi di parametri: mariadb10.6
 - Group name (Nome gruppo: **dms-mariadb-parameters**)
 - Descrizione: **Group for specifying binary log settings for replication**

Scegli Crea.

5. Nella pagina Gruppi di parametri scegli dms-mariadb-parameters e nella pagina dms-mariadb-parameters seleziona Modifica.
6. Imposta i seguenti parametri sui valori specificati:
 - binlog_checksum: NONE
 - binlog_format: ROW

Seleziona Salvataggio delle modifiche.

7. Nella pagina Gruppi di parametri scegli di nuovo Crea gruppo di parametri.
8. Nella pagina Crea gruppo di parametri immetti le seguenti impostazioni:

- Famiglia del gruppo di parametri: postgres13
- Group name (Nome gruppo: **dms-postgresql-parameters**)
- Descrizione: **Group for specifying role setting for replication**

Scegli Crea.

9. Nella pagina Gruppi di parametri scegli dms-postgresql-parameters.
10. Nella pagina dms-postgresql-parameters scegli Modifica e imposta session_replication_role parameter su replica. Tieni presente che il parametro session_replication_role non si trova nella prima pagina dei parametri. Utilizza i controlli di impaginazione o il campo di ricerca per trovare il parametro.
11. Seleziona Salvataggio delle modifiche.

Creazione del database Amazon RDS di origine

Utilizza la procedura seguente per creare il database Amazon RDS di origine.

Per creare il database Amazon RDS per MariaDB di origine

1. Apri la console di Amazon RDS all'indirizzo <https://console.aws.amazon.com/rds/>.
2. Nella pagina Dashboard scegli Crea database nella sezione Database. Non scegliere Crea database nella sezione Prova la nuova opzione di implementazione Amazon RDS Multi-AZ per MySQL e PostgreSQL all'inizio della pagina.
3. Nella pagina Crea database imposta le seguenti opzioni:
 - Scegli un metodo di creazione del database: seleziona Creazione Standard.
 - Opzioni motore: per Tipo di motore scegli MariaDB. Per Versione lascia selezionato MariaDB 10.6.14.
 - Modelli: scegli Sviluppo/Test.
 - Impostazioni:
 - Identificatore di istanza database: immetti **dms-mariadb**.
 - Nella sezione Impostazioni delle credenziali immetti i seguenti valori:
 - Nome utente master: lascia **admin**.
 - Lascia deselezionata l'opzione Gestisci le credenziali principali in AWS Secrets Manager.

- Genera automaticamente una password: lascia l'opzione deselezionata.
- Password master: immetti **changeit**.
- Conferma la password: inserisci di nuovo **changeit**.
- Configurazione dell'istanza:
 - Classe di istanza database: lascia selezionata l'opzione Classi standard.
 - Per classe di istanza database scegli db.m5.large.
- Archiviazione:
 - Deseleziona la casella Abilita il dimensionamento automatico dello storage.
 - Lascia inalterate le impostazioni rimanenti.
- Disponibilità e durabilità: lascia selezionata l'opzione Non creare un'istanza di standby.
- Connettività:
 - Risorsa di calcolo: lascia Non connettere una risorsa di calcolo EC2.
 - Tipo di rete: lascia IPv4 selezionato.
 - Cloud privato virtuale: DMSVPC-vpc
 - Accesso pubblico: Yes. È necessario abilitare l'accesso pubblico per utilizzare AWS Schema Conversion Tool.
 - Zona di disponibilità: us-west-2a
 - Lascia inalterate le impostazioni rimanenti.
- Autenticazione database: lascia selezionata l'opzione Autenticazione password.
- In Monitoraggio deseleziona la casella Attiva Performance Insights. Espandi la sezione Configurazione aggiuntiva e deseleziona la casella Abilita monitoraggio avanzato.
- Espandi Configurazione aggiuntiva.
 - In Opzioni database immetti **dms_sample** per Nome database iniziale.
 - In Gruppo di parametri database scegli dms-mariadb-parameters.
 - Per Gruppo di opzioni lascia selezionato default:mariadb-10-6.
 - In Backup, eseguire le seguenti operazioni:
 - Lascia selezionata l'opzione Abilita backup automatici. Il database di origine deve avere i backup automatici abilitati per supportare la replica continua.
 - Per Periodo di conservazione dei backup seleziona 1 giorno.
- Per Finestra di backup lascia selezionata l'opzione Nessuna preferenza.
 - Deseleziona la casella Copia tag in snapshot.

- Lascia deselezionata l'opzione Abilita la replica in un'altra regione AWS .
- In Crittografia deseleziona la casella Abilita crittografia.
- Lascia inalterata la sezione Esportazioni log.
- In Manutenzione deseleziona la casella Abilita aggiornamento automatico versione secondaria e lascia l'impostazione Finestra di manutenzione su Nessuna preferenza.
- Lascia deselezionata l'opzione Abilita protezione da eliminazione.

4. Scegliere Crea database.

Creazione del database Amazon RDS di destinazione

Ripeti la procedura precedente per creare il database Amazon RDS di destinazione, con le seguenti modifiche.

Per creare il database RDS per PostgreSQL di destinazione

1. Ripeti le fasi 1 e 2 della procedura precedente.
2. Nella pagina Crea database imposta le stesse opzioni, ad eccezione di queste:
 - a. In Opzioni motore, seleziona PostgreSQL.
 - b. Per Versione scegli PostgreSQL 13.7-R1.
 - c. Per l'identificatore dell'istanza DB, inserisci **dms-postgresql**.
 - d. Per Nome utente master lascia **postgres** selezionato.
 - e. Per Gruppo di parametri database scegli dms-postgresql-parameters.
 - f. Deseleziona Abilita backup automatici.
3. Scegliere Crea database.

Creazione di un client Amazon EC2

In questa sezione viene descritto come creare un client Amazon EC2. Utilizzi questo client per popolare il database di origine con dati da replicare. Il client viene utilizzato anche per verificare la replica eseguendo le query sul database di destinazione.


L'utilizzo di un client Amazon EC2 per accedere ai database offre i seguenti vantaggi rispetto all'accesso ai database tramite Internet:

- Puoi limitare l'accesso ai database ai client che si trovano nello stesso VPC.
- Abbiamo verificato che gli strumenti utilizzati in questo tutorial funzionano e sono facili da installare su Amazon Linux 2023, che quindi consigliamo per questo tutorial.
- Le operazioni sui dati tra i componenti di un VPC generalmente offrono prestazioni migliori rispetto a quelle su Internet.

Per creare e configurare un client Amazon EC2 per popolare il database di origine

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nella pagina Dashboard scegli Avvia istanza.
3. Nella pagina Avvia un'istanza immetti i seguenti valori:
 - a. Nella sezione Nome e tag immetti **DMSClient** per Nome.
 - b. Nella sezione Immagini dell'applicazione e del sistema operativo (Amazon Machine Image) lascia le impostazioni inalterate.
 - c. Nella sezione Tipo di istanza scegli t2.xlarge.
 - d. Nella sezione Coppia di chiavi (registrazione) scegli Crea una nuova coppia di chiavi.
 - e. Nella pagina Crea coppia di chiavi immetti i seguenti valori:
 - Key pair name (Nome della coppia di chiavi): **DMSKeyPair**
 - Tipo di coppia di chiavi: lascia RSA.
 - Formato del file della chiave privata: scegli pem per OpenSSH su MacOS o Linux oppure ppk per PuTTY su Windows.

Salva il file della chiave quando richiesto.

 Note

Puoi anche utilizzare una coppia di chiavi Amazon EC2 esistente anziché crearne una nuova.

- f. Nella sezione Impostazioni di rete scegli Modifica. Scegliere le seguenti impostazioni:
 - VPC obbligatorio: scegli il VPC con l'ID che hai registrato per DMSVPC-vpc.
 - Sottorete: seleziona la prima sottorete pubblica.

- Assegna automaticamente IP pubblico: scegli Abilita.

Lascia inalterate le altre impostazioni e scegli Avvia istanza.

Popolamento del database di origine

In questa sezione sono descritti gli endpoint per i database di origine e di destinazione per un uso successivo e gli strumenti per popolare il database di origine:

- Git, per scaricare lo script che popola il database sorgente.
- Client MariaDB, per eseguire lo script.

Recupero degli endpoint

Trova e annota gli endpoint delle tue istanze DB RDS for MariaDB e RDS for PostgreSQL per un uso successivo.

Per individuare gli endpoint dell'istanza database

1. Accedi AWS Management Console e apri la console Amazon RDS all'[indirizzo https://console.aws.amazon.com/rds/](https://console.aws.amazon.com/rds/).
2. Nel riquadro di navigazione scegli Database.
3. Scegli il database dms-mariadb e annota il valore Endpoint del database.
4. Ripeti le fasi precedenti per il database dms-postgresql.

Popolamento del database di origine

Successivamente, connessi all'istanza del client, installa il software necessario, scarica script di database di AWS esempio da Git ed esegui gli script per popolare il database di origine.

Per popolare il database di origine

1. Connettiti all'istanza client utilizzando il nome host e la chiave pubblica salvati nelle fasi precedenti.

Per ulteriori informazioni sulla connessione a un'istanza Amazon EC2, consulta [Accedere alle istanze](#) nella Amazon EC2 User Guide.

Note

Se utilizzi PuTTY, abilita i keepalive TCP nella pagina delle impostazioni Connessione in modo che la connessione non generi un timeout a causa dell'inattività.

2. Installa Git, MariaDB e PostgreSQL. Verifica l'installazione se necessario.

```
$ sudo yum install git
$ sudo dnf install mariadb105
$ sudo dnf install postgresql15
```

3. Esegui il comando seguente per scaricare gli script di creazione del database da GitHub

```
git clone https://github.com/aws-samples/aws-database-migration-samples.git
```

4. Passare alla directory `aws-database-migration-samples/mysql/sampledb/v1/`.
5. Esegui il comando seguente. Fornisci l'endpoint per l'istanza RDS di origine che hai annotato in precedenza, ad esempio `dms-mariadb.cdv5fbeyiy4e.us-east-1.rds.amazonaws.com`.

```
mysql -h dms-mariadb.abcdefghij01.us-east-1.rds.amazonaws.com -P 3306 -u admin -p
dms_sample < ~/aws-database-migration-samples/mysql/sampledb/v1/install-rds.sql
```

6. Consenti l'esecuzione dello script di creazione del database. Lo script impiega fino a 45 minuti per creare lo schema e popolare i dati. È possibile ignorare in sicurezza gli errori e gli avvisi visualizzati dallo script.

Migrazione dello schema di origine nel database di destinazione mediante AWS SCT

In questa sezione, si utilizza AWS Schema Conversion Tool per migrare lo schema di origine nel database di destinazione. In alternativa, puoi usare la conversione dello schema DMS per convertire gli schemi del database di origine. Per ulteriori informazioni, consulta [Nozioni di base sulla conversione dello schema DMS](#).

Per migrare lo schema di origine nel database di destinazione mediante AWS SCT

1. Installazione di AWS Schema Conversion Tool. Per ulteriori informazioni, consulta [Installing, verifying, and updating the AWS SCT](#) nella Guida per l'utente di AWS Schema Conversion Tool.

Quando scarichi i driver JDBC per MySQL e PostgreSQL, annota dove li salvi, nel caso in cui lo strumento richieda la loro posizione.

2. Aprire AWS Schema Conversion Tool. Scegli File, quindi seleziona Nuovo progetto.
3. Nella finestra Nuovo progetto imposta i seguenti valori:
 - Imposta Nome progetto su **DMSProject**.
 - Mantieni Posizione così com'è per archiviare il progetto AWS SCT nella cartella predefinita.

Scegli OK.

4. Scegli Aggiungi origine per aggiungere un database MySQL di origine al progetto, quindi seleziona MySQL e Successivo.
5. Nella pagina Aggiungi origine, imposta i seguenti valori:
 - Nome connessione: **source**
 - Nome del server: inserisci l'endpoint per il database MySQL che hai annotato in precedenza.
 - Porta del server: **3306**
 - Nome utente: **admin**
 - Password: **changeit**
6. Scegli Aggiungi destinazione per aggiungere un database Amazon RDS per PostgreSQL di destinazione al progetto, quindi seleziona Amazon RDS per PostgreSQL. Seleziona Successivo.
7. Nella pagina Aggiungi destinazione, imposta i seguenti valori:
 - Nome connessione: **target**
 - Nome del server: inserisci l'endpoint per il database PostgreSQL che hai annotato in precedenza.
 - Porta del server: **5432**
 - Database: immetti il nome del database PostgreSQL.
 - Nome utente: **postgres**
 - Password: **changeit**
8. Nel riquadro a sinistra scegli dms_sample in Schema. Nel riquadro a destra, scegli il database Amazon RDS per PostgreSQL di destinazione. Scegli Crea mappatura. Puoi aggiungere più regole di mappatura a un singolo progetto AWS SCT. Per ulteriori informazioni sulle regole di mappatura, consulta [Creating mapping rules](#).

- Scegli Visualizzazione principale.
- Nel riquadro a sinistra scegli `dms_sample` in Schema. Apri il menu contestuale (pulsante destro del mouse) e scegli Converti lo schema. Confermare l'operazione.

Una volta che lo strumento termina la conversione, lo schema `dms_sample` viene visualizzato nel riquadro destro.

- Nel riquadro destro, in Schemi, apri il menu contestuale (pulsante destro del mouse) per `dms_sample` e scegli Applica al database. Confermare l'operazione.

Verifica che la migrazione dello schema sia stata completata. Esegui questa procedura.

Per verificare la migrazione dello schema

- Esegui la connessione al client Amazon EC2.
- Avvia il client utilizzando il seguente comando. Specifica l'endpoint del database PostgreSQL e fornisci la password del database quando richiesto.

```
psql \  
  --host=dms-postgresql.abcdefg12345.us-west-2.rds.amazonaws.com \  
  --port=5432 \  
  --username=postgres \  
  --password \  
  --dbname=dms_sample
```

- Esegui una query su una delle tabelle (vuote) per verificare che AWS SCT abbia applicato lo schema correttamente.

```
dms_sample=> SELECT * from dms_sample.player;  
 id | sport_team_id | last_name | first_name | full_name  
----+-----+-----+-----+-----  
(0 rows)
```

Impostazione della replica per AWS Database Migration Service

In questo argomento si configura la replica tra il database di origine e quello di destinazione.

Fase 1: creazione di un'istanza di replica mediante la console AWS DMS

Per iniziare a usare AWS DMS, crea un'istanza di replica.

Un'istanza di replica esegue l'effettiva migrazione dei dati tra gli endpoint di origine e di destinazione. L'istanza necessita di una potenza di storage e di elaborazione sufficiente per eseguire le attività di migrazione dei dati dal database di origine a quello di destinazione. La dimensione di questa istanza di replica dipende dalla quantità di dati da migrare e dalle attività che l'istanza deve eseguire. Per ulteriori informazioni sulle istanze di replica, consulta [Utilizzo di un'istanza di AWS DMS replica](#).

DMS > Replication instances > Create replication instance

Create replication instance

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

Descriptive Amazon Resource Name (ARN) - optional
A friendly name to override the default DMS ARN. You cannot modify it after creation.

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](#) 

dms.t2.medium
2 vCPUs 4 GiB Memory ▼

Include previous-generation instance classes

Per creare un'istanza di replica mediante la console

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.
2. Nel riquadro di navigazione scegli Istanze di replica e seleziona Crea istanza di replica.
3. Nella pagina Crea istanza di replica specifica la configurazione dell'istanza di replica:
 - a. In Nome, inserisci **DMS-instance**.
 - b. Per Descrizione inserisci una breve descrizione (facoltativa) dell'istanza di replica.
 - c. Per Classe di istanza lascia selezionato dms.t3.medium.

L'istanza necessita della potenza di storage, rete ed elaborazione sufficiente per la migrazione. Per ulteriori informazioni su come scegliere una classe di istanza, consulta [Scelta dell'istanza di replica AWS DMS giusta per la migrazione](#).

- d. Per Versione del motore mantieni il valore predefinito.
- e. Per Multi AZ scegli Carico di lavoro di sviluppo o test (AZ singola).
- f. Per Spazio di archiviazione allocato (GiB) accetta il valore predefinito di 50 GiB.

In AWS DMS, lo spazio di storage viene utilizzato principalmente dai file di log e dalle transazioni memorizzate nella cache. Per le transazioni memorizzate nella cache, lo spazio di storage viene utilizzato solo quando le transazioni memorizzate nella cache devono essere scritte su disco. Pertanto, AWS DMS non utilizza una quantità significativa di spazio di storage.

- g. Per Tipo di rete scegli IPv4.
 - h. Per VPC scegli DMSVPC.
 - i. Per Gruppo di sottoreti di replica lascia selezionato il gruppo di sottoreti di replica corrente.
 - j. Deseleziona Accessibile pubblicamente.
4. Scegli la scheda Configurazione di rete e sicurezza avanzata per definire i valori per le impostazioni di rete e crittografia, se necessario:
 - a. Per Zona di disponibilità scegli us-west-2a.
 - b. Per Gruppi di sicurezza VPC scegli il gruppo di sicurezza Predefinito se non è già presente.
 - c. Per AWS KMS key lascia selezionato (Impostazione predefinita) aws/dms.

5. Non modificare le impostazioni nella scheda Manutenzione. 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.
6. Seleziona Crea.

AWS DMS crea un'istanza di replica per eseguire la migrazione.

Fase 2: specificazione degli endpoint di origine e di destinazione

Durante la creazione dell'istanza di replica, puoi specificare gli endpoint del datastore di origine e di destinazione per i database Amazon RDS creati in precedenza. Ogni endpoint viene creato separatamente.

The screenshot shows the AWS DMS console interface for creating an endpoint. At the top, there is a breadcrumb trail: 'DMS > Endpoints > Create endpoint'. The main heading is 'Create endpoint'. Below this, there is a section titled 'Endpoint type' with an 'Info' link. Two options are presented: 'Source endpoint' (selected with a radio button) and 'Target endpoint' (unselected). The 'Source endpoint' option includes a description: 'A source endpoint allows AWS DMS to read data from a database (on-premises or in the cloud), or from other data source such as Amazon S3.' The 'Target endpoint' option includes a description: 'A target endpoint allows AWS DMS to write data to a database, or to other data source.' Below these options is a checkbox labeled 'Select RDS DB instance'. The next section is 'Endpoint configuration'. It starts with 'Endpoint identifier' and an 'Info' link, followed by the instruction 'A label for the endpoint to help you identify it.' A text input field contains the value 'ProdEndpoint'. Below this is the field for 'Descriptive Amazon Resource Name (ARN) - optional', with a note: 'A friendly name to override the default DMS ARN. You cannot modify it after creation.'

Per specificare gli endpoint del database di origine e di destinazione mediante la console AWS DMS

1. Nel riquadro di navigazione della console IAM, scegli Endpoint quindi seleziona Crea endpoint.
2. Nella pagina Crea endpoint scegli il tipo di endpoint di origine. Per la casella Seleziona un'istanza database RDS scegli l'istanza dms-mariadb.
3. Nella sezione Configurazione dell'endpoint inserisci **dms-mysql-source** per Identificativo endpoint.
4. Per Motore di origine lascia selezionato MySQL.
5. Per Accede al database di endpoint scegli Fornisci le informazioni di accesso manualmente. Verifica che i valori di Porta, Modalità Secure Socket Layer (SSL), Nome utente e Password siano corretti.
6. Scegli la scheda Testa la connessione dell'endpoint (facoltativo). Per VPC scegli DMSVPC.
7. Per Istanza di replica lascia selezionata l'opzione dms-instance.
8. Scegli Esegui test.

Dopo aver scelto Esegui test, AWS DMS crea l'endpoint con i dettagli che hai fornito ed esegue la connessione. Se la connessione non riesce, modifica la definizione dell'endpoint e prova nuovamente a connetterti. Puoi anche eliminare l'endpoint manualmente.

9. Dopo aver superato con successo il test, scegli Crea endpoint.
10. Specifica l'endpoint del database di destinazione usando la console AWS DMS. Per farlo, ripeti i passaggi precedenti, con le seguenti impostazioni:
 - Tipo di endpoint: Endpoint di destinazione
 - Istanza RDS: dms-postgresql
 - Identificativo endpoint: **dms-postgresql-target**
 - Motore di destinazione: lascia **PostgreSQL**.

Una volta specificate tutte le informazioni per gli endpoint, AWS DMS crea gli endpoint di origine e di destinazione da utilizzare durante la migrazione del database.

Fase 3: creazione di un'attività e migrazione dei dati

In questa fase, si crea un'attività per la migrazione dei dati tra i database creati.

DMS > Database migration tasks > Create database migration task

Create database migration task

Task configuration

Task identifier

Replication instance

Source database endpoint

Target database endpoint

Migration type [Info](#)

Per creare un'attività di migrazione e avviare la migrazione del database

1. Nel riquadro di navigazione della console scegli Attività di migrazione database e seleziona Crea attività. Viene visualizzata la pagina Crea attività di migrazione del database.
2. Nella sezione Configurazione dell'attività specificar le seguenti opzioni:
 - Identificativo di attività: immetti **dms-task**.
 - Istanza di replica: scegli la tua istanza di replica (dms-instance-vpc-**<vpc id>**).
 - Endpoint del database di origine: scegli dms-mysql-source.
 - Endpoint del database di destinazione: scegli dms-postgresql-target.
 - Tipo di migrazione: scegli Migrazione dei dati esistenti e replica delle modifiche in corso.

3. Scegli la scheda Impostazioni delle attività. Configura le seguenti impostazioni:
 - Modalità di preparazione della tabella di destinazione: Nessuna azione
 - Interrompi l'attività dopo il completamento del pieno carico: non interrompere
4. Scegli la scheda Mappature delle tabelle ed espandi Regole di selezione. Scegli Aggiungi nuova regola di selezione. Configura le seguenti impostazioni:
 - Schema: Inserisci uno schema
 - Nome dello schema: **dms_sample**
5. Scegli la scheda Configurazione di avvio dell'attività di migrazione, quindi seleziona Automaticamente al momento della creazione.
6. Scegli Create task (Crea attività).

AWS DMS quindi crea l'attività di migrazione e la avvia. La replica iniziale del database richiede circa 10 minuti. Assicurati di eseguire la prossima fase del tutorial prima che AWS DMS completi la migrazione dei dati.

Fase 4: test della replica

In questa sezione inserisci i dati nel database di origine durante e dopo la replica iniziale ed esegui una query sul database di destinazione per i dati inseriti.

Per testare la replica

1. Assicurati che l'attività di migrazione del database mostri lo stato In esecuzione e che la replica iniziale del database, avviata nella fase precedente, non sia stata completata.
2. Esegui la connessione al client Amazon EC2 e avvia il client MySQL con il comando seguente. Fornisci l'endpoint del database MySQL.

```
mysql -h dms-mysql.abcdefg12345.us-west-2.rds.amazonaws.com -P 3306 -u admin -pchangeit dms_sample
```

3. Esegui il comando seguente per inserire un record nel database di origine.

```
MySQL [dms_sample]> insert person (full_name, last_name, first_name) VALUES ('Test User1', 'User1', 'Test');  
Query OK, 1 row affected (0.00 sec)
```

4. Esci dal client MySQL.

```
MySQL [dms_sample]> exit
Bye
```

5. Prima del completamento della replica, esegui una query sul database di destinazione per il nuovo record.

Dall'istanza Amazon EC2, connettiti al database di destinazione con il seguente comando, fornendo l'endpoint del database di destinazione.

```
psql \  
  --host=dms-postgresql.abcdefg12345.us-west-2.rds.amazonaws.com \  
  --port=5432 \  
  --username=postgres \  
  --password \  
  --dbname=dms_sample
```

Fornisci la password (**changeit**) quando richiesto.

6. Prima del completamento della replica, esegui una query sul database di destinazione per il nuovo record.

```
dms_sample=> select * from dms_sample.person where first_name = 'Test';
 id | full_name | last_name | first_name
-----+-----+-----+-----
(0 rows)
```

7. Mentre l'attività di migrazione del database è in esecuzione, è possibile monitorarne l'avanzamento in tempo reale:

- Dal riquadro di navigazione della console DMS scegli Attività di migrazione del database.
- Scegli dms-task.
- Scegli Statistiche della tabella.

Per ulteriori informazioni sul monitoraggio, consulta [Monitoraggio delle attività AWS DMS](#).

8. Al termine della replica, esegui nuovamente la query sul database di destinazione per il nuovo record. AWS DMS migra il nuovo record al termine della replica iniziale.

```
dms_sample=> select * from dms_sample.person where first_name = 'Test';
```

```

  id      | full_name | last_name | first_name
-----+-----+-----+-----
  7077784 | Test User1 | User1     | Test
(1 row)

```

9. Esci dal client psql.

```
dms_sample=> quit
```

10. Ripeti la fase 1 per connetterti nuovamente al database di origine.

11. Inserisci un altro record nella tabella person.

```

MySQL [dms_sample]> insert person (full_name, last_name, first_name) VALUES ('Test
  User2', 'User2', 'Test');
Query OK, 1 row affected (0.00 sec)

```

12. Ripeti le fasi 3 e 4 per disconnetterti dal database di origine e connetterti al database di destinazione.

13. Esegui nuovamente la query sul database di destinazione per i dati replicati.

```

dms_sample=> select * from dms_sample.person where first_name = 'Test';
  id      | full_name | last_name | first_name
-----+-----+-----+-----
  7077784 | Test User1 | User1     | Test
  7077785 | Test User2 | User2     | Test
(2 rows)

```

Fase 5: eliminazione delle risorse AWS DMS

Dopo aver completato il tutorial introduttivo, puoi eliminare le risorse che hai creato. È possibile utilizzare il comando AWS per rimuoverle. Assicurati di eliminare le attività di migrazione prima di eliminare l'istanza di replica e gli endpoint.

Per eliminare un'attività di migrazione mediante la console

1. Dal riquadro di navigazione della console AWS DMS scegli Attività di migrazione del database.
2. Scegli dms-task.
3. Scegliere Operazioni, Elimina.

Per eliminare un'istanza di replica mediante la console

1. Dal riquadro di navigazione della console AWS DMS scegli Istanze di replica.
2. Scegli DMS-instance.
3. Scegliere Operazioni, Elimina.

AWS DMS elimina l'istanza di replica e la rimuove dalla pagina Istanze di replica.

Per rimuovere gli endpoint mediante la console

1. Dal riquadro di navigazione della console AWS DMS scegli Endpoint.
2. Seleziona dms-mysql-source.
3. Scegliere Operazioni, Elimina.

Dopo aver eliminato le risorse AWS DMS, assicurati di eliminare anche le seguenti risorse. Per informazioni sull'eliminazione di risorse in altri servizi, consulta la documentazione di ciascun servizio.

- I database RDS.
- I gruppi di parametri del database RDS.
- I gruppi di sottoreti RDS.
- Tutti i file di log Amazon CloudWatch creati insieme ai database e all'istanza di replica.
- I gruppi di sicurezza creati per il client Amazon VPC e Amazon EC2. Assicurati di rimuovere l'opzione Predefinito della regola in entrata per i gruppi di sicurezza launch-wizard-1, operazione necessaria per poterli eliminare.
- Il client Amazon EC2.
- Il VPC Amazon.
- La coppia di chiavi Amazon EC2 per il client Amazon EC2.

Risorse aggiuntive per l'utilizzo di AWS Database Migration Service

Più avanti in questa guida, sono disponibili le informazioni su come usare AWS DMS per migrare i dati da e verso i database commerciali e open source più comuni.

Ti consigliamo inoltre di consultare le seguenti risorse durante la preparazione e l'esecuzione di un progetto di migrazione del database:

- [AWS DMS Step-by-Step Migration Guide](#): questa guida fornisce le procedure dettagliate per il processo di migrazione dei dati ad AWS.
- [AWS DMS API Reference](#): questo riferimento descrive nel dettaglio tutte le operazioni delle API per AWS Database Migration Service.
- [AWS CLI for AWS DMS](#): questo riferimento fornisce informazioni sull'utilizzo di AWS Command Line Interface (AWS CLI) con AWS DMS.

Individuazione e valutazione dei database per la migrazione con AWS DMS Fleet Advisor

Puoi utilizzare DMS Fleet Advisor per raccogliere metadati e parametri delle prestazioni da più ambienti di database. Questi parametri raccolti forniscono informazioni dettagliate sulla tua infrastruttura di dati. [DMS Fleet Advisor](#) raccoglie metadati e parametri dal database on-premise e dai server di analisi da una o più postazioni centrali senza la necessità di installarlo su ogni computer. Attualmente, DMS Fleet Advisor supporta il rilevamento e la raccolta di metriche per i server di database Microsoft SQL Server, MySQL, Oracle e PostgreSQL.

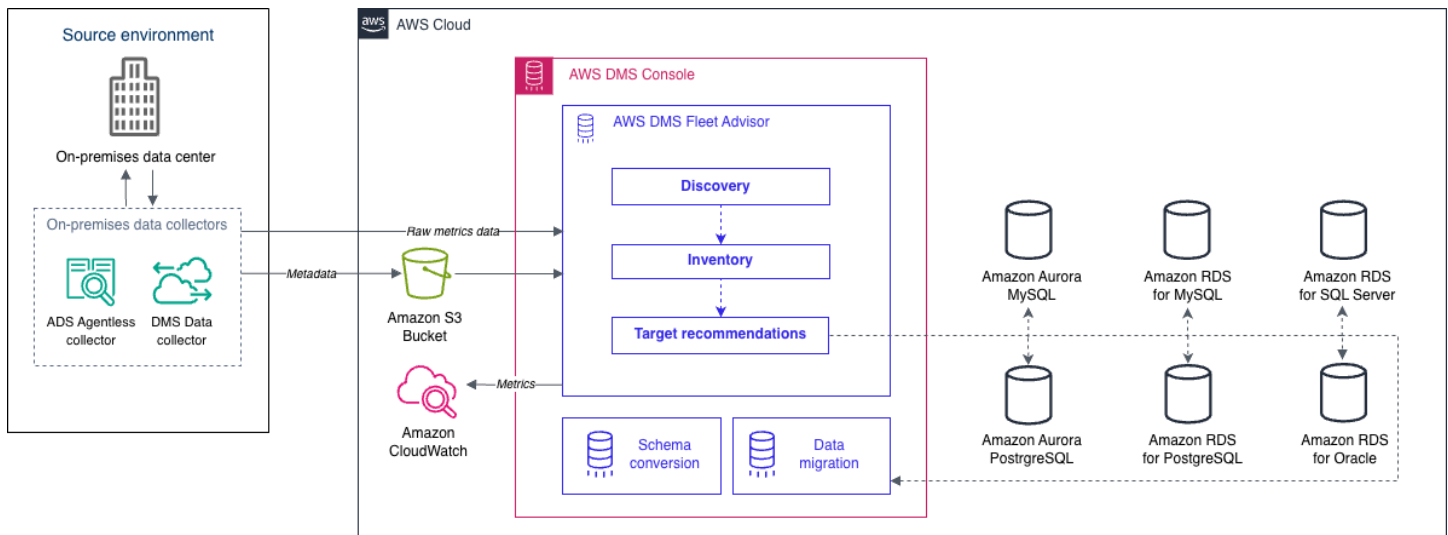
In base ai dati rilevati della rete, è possibile creare un inventario per definire l'elenco dei server di database per la raccolta di dati. Una volta che AWS DMS completa la raccolta di informazioni su server, database e schemi, è possibile analizzare la fattibilità delle migrazioni di database previste.

Per i database presenti nell'inventario che intendi migrare nel Cloud AWS, DMS Fleet Advisor genera raccomandazioni sulle destinazioni correttamente dimensionate. Per generare raccomandazioni sulle destinazioni, DMS Fleet Advisor prende in considerazione i parametri della raccolta dati e le impostazioni preferite. Dopo che DMS Fleet Advisor ha generato le raccomandazioni, è possibile visualizzare informazioni dettagliate per ogni configurazione del database di destinazione. I tecnici e gli amministratori dei database dell'organizzazione possono utilizzare le raccomandazioni sulle destinazioni di DMS Fleet Advisor per pianificare la migrazione dei database on-premise ad AWS. È possibile esplorare le diverse opzioni di migrazione disponibili ed esportare questi consigli in file per ottimizzare ulteriormente i costi. AWS Pricing Calculator

Per l'elenco dei database di origine supportati, consulta [Origini per DMS Fleet Advisor](#).

Per l'elenco dei database utilizzati da DMS Fleet Advisor per generare raccomandazioni di destinazione, consulta [Destinazioni per DMS Fleet Advisor](#). DMS Fleet Advisor genera consigli simili a like, ad esempio, dal database Oracle di origine al database Oracle di destinazione. DMS Fleet Advisor genera anche raccomandazioni eterogenee, come la migrazione dal database Oracle o Microsoft SQL Server di origine al database RDS for PostgreSQL o Aurora PostgreSQL di destinazione.

Il diagramma seguente illustra il processo di raccomandazione di AWS DMS Fleet Advisor.



Consulta gli argomenti che seguono per capire meglio come utilizzare AWS DMS Fleet Advisor.

Argomenti

- [Regioni AWS supportate](#)
- [Nozioni di base su DMS Fleet Advisor](#)
- [Configurazione di AWS DMS Fleet Advisor](#)
- [Individuazione dei database per la migrazione utilizzando i raccoglitori di dati](#)
- [Utilizzo degli inventari per l'analisi in AWS DMS Fleet Advisor](#)
- [Utilizzo della funzionalità dei suggerimenti delle destinazioni di AWS DMS Fleet Advisor](#)
- [Limitazioni di DMS Fleet Advisor](#)

Regioni AWS supportate

È possibile utilizzare DMS Fleet Advisor nelle seguenti Regioni AWS.

Nome della regione	Regione
US East (N. Virginia)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
Stati Uniti occidentali (California settentrionale)	us-west-1

Nome della regione	Regione
US West (Oregon)	us-west-2
Asia Pacifico (Hong Kong)	ap-east-1
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Mumbai)	ap-south-1
Asia Pacifico (Singapore)	ap-southeast-1
Asia Pacifico (Sydney)	ap-southeast-2
Asia Pacifico (Giacarta)	ap-southeast-3
Canada (Central)	ca-central-1
Europa (Francoforte)	eu-central-1
Europa (Stoccolma)	eu-north-1
Europa (Irlanda)	eu-west-1
Europa (London)	eu-west-2
Europa (Paris)	eu-west-3
Europa (Milano)	eu-south-3
Canada (Central)	ca-central-1
Sud America (São Paulo)	sa-east-1
Medio Oriente (Bahrein)	me-south-1
Africa (Cape Town)	af-south-1

Nozioni di base su DMS Fleet Advisor

Puoi utilizzare DMS Fleet Advisor per individuare i database on-premise di origine per la migrazione nel Cloud AWS. Quindi, puoi determinare la destinazione di migrazione corretta nel Cloud AWS per ciascuno dei tuoi database on-premise. Utilizza il seguente flusso di lavoro per creare un inventario dei database di origine e generare i suggerimenti delle destinazioni.

1. Crea un bucket Amazon S3, le policy IAM, i ruoli e gli utenti. Per ulteriori informazioni, consulta [Creazione delle risorse necessarie](#).
2. Crea gli utenti del database con le autorizzazioni minime richieste per il raccoglitore di dati DMS. Per ulteriori informazioni, consulta [Creazione di utenti di database](#).
3. Crea e scarica un raccoglitore di dati. Per ulteriori informazioni, consulta [Creazione di un raccoglitore di dati](#).
4. Installa il raccoglitore di dati nel tuo ambiente locale. Quindi, configuralo per assicurarti che possa inviare i dati raccolti a DMS Fleet Advisor. Per ulteriori informazioni, consulta [Installazione di un raccoglitore di dati](#).
5. Individua il sistema operativo e i server di database nel tuo ambiente di dati. Per ulteriori informazioni, consulta [Individuazione dei server del sistema operativo e di database](#).
6. Raccogli i metadati del database e le metriche di utilizzo delle risorse. Per ulteriori informazioni, consulta [Raccolta di dati](#).
7. Analizza i database e gli schemi di origine. DMS Fleet Advisor esegue la valutazione su larga scala dei database per identificare schemi simili. Per ulteriori informazioni, consulta [Utilizzo degli inventari per l'analisi in AWS DMS Fleet Advisor](#).
8. Genera, visualizza e salva una copia locale dei suggerimenti delle destinazioni per i tuoi database di origine. Per ulteriori informazioni, consulta [Suggerimenti delle destinazioni](#).

Dopo aver determinato la destinazione di migrazione per ogni database di origine, puoi utilizzare la conversione dello schema DMS per convertire gli schemi del database in una nuova piattaforma. Puoi quindi utilizzare AWS DMS per migrare i dati. Per ulteriori informazioni, consulta [Conversione degli schemi di database utilizzando la conversione dello schema DMS](#) e [Cos'è AWS Database Migration Service?](#)

[Questo video](#) presenta l'interfaccia utente della conversione dello schema DMS per familiarizzare con i componenti principali di questo servizio.

Configurazione di AWS DMS Fleet Advisor

Per configurare AWS DMS Fleet Advisor, completa le seguenti attività preliminari.

Argomenti

- [Creazione delle risorse AWS necessarie per AWS DMS Fleet Advisor](#)
- [Creazione di utenti di database per AWS DMS Fleet Advisor](#)

Creazione delle risorse AWS necessarie per AWS DMS Fleet Advisor

DMS Fleet Advisor necessita di una serie di risorse AWS nell'account per inoltrare e importare le informazioni sull'inventario e aggiornare lo stato del raccoglitore di dati DMS.

Prima di raccogliere dati e creare inventari di database e schemi per la prima volta, è necessario completare i seguenti prerequisiti.

Per configurare il bucket Amazon S3 e le risorse IAM, procedi in uno dei modi seguenti:

- [Configura le risorse Amazon S3 e IAM utilizzando AWS CloudFormation](#) (consigliato).
- [Configurazione delle risorse Amazon S3 e IAM nella AWS Management Console](#)

Configura le risorse Amazon S3 e IAM utilizzando AWS CloudFormation

Uno CloudFormation stack è una raccolta di risorse di AWS che è possibile gestire come un'unità singola. Per semplificare la creazione delle risorse necessarie per DMS Fleet Advisor, puoi utilizzare i file AWS CloudFormation modello per creare CloudFormation pile. Per ulteriori informazioni, consulta [Creazione di uno stack sulla console AWS CloudFormation](#) nella Guida per l'utente di AWS CloudFormation.

Note

Questa sezione si riferisce esclusivamente all'utilizzo del raccoglitore autonomo DMS Fleet Advisor. Per informazioni sull'utilizzo di un singolo raccoglitore on-premise per la raccolta di informazioni su database e server, consulta [Application Discovery Service Agentless Collector](#) nella [Guida per l'utente di AWS Application Discovery Service](#).

Risorse Amazon S3 e IAM create da CloudFormation

Quando utilizzi i CloudFormation modelli, creano stack che includono le seguenti risorse: Account AWS

- Un bucket Amazon S3 denominato `dms-fleetadvisor-data-accountId-region`
- Un utente IAM denominato `FleetAdvisorCollectorUser-region`
- Un ruolo di servizio IAM denominato `FleetAdvisorS3Role-region`
- Una policy di accesso denominata `FleetAdvisorS3Role-region-Policy`
- Una policy di accesso denominata `FleetAdvisorCollectorUser-region-Policy`
- Un ruolo collegato al servizio IAM denominato `AWSServiceRoleForDMSFleetAdvisor`

Segui i passaggi elencati di seguito per configurare le tue risorse con CloudFormation.

- [Passaggio 1: scarica i file CloudFormation modello](#)
- [Fase 2: configurare Amazon S3 e IAM utilizzando CloudFormation](#)

Passaggio 1: scarica i file CloudFormation modello

Un CloudFormation modello è una dichiarazione delle AWS risorse che compongono uno stack. Il modello viene archiviato come un file JSON.

Per scaricare i file CloudFormation modello

1. Apri il menu contestuale (fai clic con il tasto destro del mouse) per uno dei seguenti collegamenti, quindi scegli Salva collegamento come:
 - Se prevedi di utilizzare DMS Fleet Advisor, scegli [dms-fleetadvisor-iam-slr-s3.zip](#). [Se hai già creato la reflex per DMS Fleet Advisor, scegli 3.zip dms-fleetadvisor-iam-s](#)
 - [Se intendi utilizzare l'AWSApplication Discovery Service \(ADS\) Agentless Collector e non hai creato la relativa reflex, scegli -slr-s3.zip. dms-fleetadvisor-ads-iam](#) [Se hai già creato la reflex per DMS Fleet Advisor con ADS, scegli -s3.zip. dms-fleetadvisor-ads-iam](#)
2. Salvare il file sul computer.

Fase 2: configurare Amazon S3 e IAM utilizzando CloudFormation

Quando utilizzi il CloudFormation modello per IAM, crea le risorse Amazon S3 e IAM elencate in precedenza.

Per configurare Amazon S3 e IAM utilizzando CloudFormation

1. Apri la CloudFormation console all'indirizzo <https://console.aws.amazon.com/cloudformation>.
2. Avvia la procedura guidata Crea stack selezionando Crea stack e Con nuove risorse nell'elenco a discesa.
3. Nella pagina Create stack (Crea stack), esegui le operazioni seguenti:
 - a. In Prepare template (Prepara modello) scegli Template is ready (Il modello è pronto).
 - b. Come Template source (Origine modello), scegliere Upload a template file (Carica un file di modello).
 - c. Per Scegli file, vai a, quindi scegli dms-fleetadvisor-iam-slr-S3.json, -S3.json. dms-fleetadvisor-iam dms-fleetadvisor-ads-iamdms-fleetadvisor-ads-iam, -slr-s3.zip o -s3.zip.
 - d. Seleziona Avanti.
4. Nella pagina Specify stack details (Specifica dettagli), procedere come segue:
 - a. Per Nome stack immetti **dms-fleetadvisor-iam-slr-s3**, **dms-fleetadvisor-iam-s3**, **dms-fleetadvisor-ads-iam-slr-s3** o **dms-fleetadvisor-ads-iam-s3**.
 - b. Seleziona Avanti.
5. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
6. Nella pagina Review dms-fleetadvisor-iam-slr -s3, Review dms-fleetadvisor-iam-s 3, Review dms-fleetadvisor-ads-iam -slr-s3 o Review -s3, effettuate le seguenti operazioni dms-fleetadvisor-ads-iam:
 - a. Seleziona la casella di spunta I acknowledge that AWS CloudFormation might create IAM resources with custom names (Sono consapevole che AWS CloudFormation potrebbe creare risorse IAM con nomi personalizzati).
 - b. Seleziona Invia.

CloudFormation crea il bucket S3 e i ruoli e l'utente IAM richiesti da DMS Fleet Advisor. Nel pannello di sinistra, quando dms-fleetadvisor-iam-slr-s3, 3, dms-fleetadvisor-ads-iam -slr-s3 o

dms-fleetadvisor-iam-sdms-fleetadvisor-ads-iam-s3 mostra CREATE_COMPLETE, procedi al passaggio successivo.

7. Nel pannello di sinistra, scegli -s3, -slr-s3 o -s3. dms-fleetadvisor-iam-slr dms-fleetadvisor-iam-s dms-fleetadvisor-ads-iam dms-fleetadvisor-ads-iam Nel riquadro di destra esegui queste operazioni:

- a. Scegli Informazioni stack. **Il tuo stack ha un ID nel formato**
`arn:aws:cloudformation: region: account-no:stack/ -s3/ identifier,`
`arn:aws:cloudformation: region: account-no:stack/ 3/ identifier,`
`arn:aws:cloudformation: region: account-no:stack/ -slr-s3/ dms-`
`fleetadvisor-iam-slr identifier, o`
`arn:aws:cloudformation: region: account-no:account-no/ s3/ identifier o`
`arn:aws:cloudformation: region: account-no:account-no/s3/`
`identifierdms-fleetadvisor-iam-s: identificatore stack/ -s3/ dms-`
`fleetadvisor-ads-iam dms-fleetadvisor-ads-iam .`
- b. Scegliere Resources (Risorse). Verrà visualizzato un codice analogo al seguente:
 - Un bucket Amazon S3 denominato dms-fleetadvisor-data-*accountId-region*
 - Un ruolo di servizio denominato FleetAdvisorS3Role-*region*
 - Un utente IAM denominato FleetAdvisorCollectorUser-*region*
 - Un ruolo collegato al servizio IAM AWSServiceRoleForDMSFleetAdvisor (se hai scaricato dms-fleet-advisor-iam-slr-s3.zip o dms-fleet-advisor-ads-iam-slr-s3.zip)
 - Una policy di accesso denominata FleetAdvisorS3Role-*region*-Policy
 - Una policy di accesso denominata FleetAdvisorCollectorUser-*region*-Policy

Configurazione delle risorse Amazon S3 e IAM nella AWS Management Console

Creazione di un bucket Amazon S3

Crea un bucket Amazon S3 in cui è possibile archiviare i metadati dell'inventario. Ti consigliamo di preconfigurare il bucket S3 prima di utilizzare DMS Fleet Advisor. AWS DMS archivia i metadati dell'inventario di DMS Fleet Advisor in questo bucket S3.

Per ulteriori informazioni sulla creazione di un bucket Amazon S3, consulta [Fase 1: creare il primo bucket S3](#) nella Guida per l'utente di Amazon S3.

 Note

DMS Fleet Advisor supporta solo bucket crittografati SSE-S3.

Per creare un bucket Amazon S3 per archiviare le informazioni dell'ambiente dati locale

1. Accedi alla AWS Management Console e apri la console di Amazon S3 all'indirizzo <https://console.aws.amazon.com/s3/>.
2. Scegliere Create bucket (Crea bucket).
3. Nella pagina Crea bucket inserisci un nome univoco globale che includa il nome di accesso per il bucket, ad esempio fa-bucket-***yoursignin***.
4. Scegli la Regione AWS in cui desideri utilizzare DMS Fleet Advisor.
5. Mantieni le impostazioni rimanenti e scegli Crea bucket.

Creazione di risorse IAM

In questa sezione crei le risorse IAM per il raccogliatore di dati, l'utente IAM e DMS Fleet Advisor.

Argomenti

- [Creazione di risorse IAM per il raccogliatore di dati](#)
- [Creazione del ruolo collegato ai servizi DMS Fleet Advisor](#)

Creazione di risorse IAM per il raccogliatore di dati

Per assicurarti che il raccogliatore di dati funzioni correttamente e carichi i metadati raccolti nel bucket Amazon S3, crea le seguenti policy. Quindi, crea un utente IAM con le seguenti autorizzazioni minime. Per ulteriori informazioni sul raccogliatore di dati DMS, consulta [Individuazione dei database per la migrazione utilizzando i raccoglitori di dati](#).

Per creare una policy IAM per l'accesso di DMS Fleet Advisor e del raccogliatore dati ad Amazon S3

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Scegli Create Policy (Crea policy).

4. Nella pagina Crea policy seleziona la scheda JSON.
5. Incolla il seguente JSON nell'editor per sostituire il codice di esempio. Sostituisci *fa_bucket* con il nome del bucket Amazon S3 creato nella sezione precedente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject*",
        "s3:GetBucket*",
        "s3:List*",
        "s3:DeleteObject*",
        "s3:PutObject*"
      ],
      "Resource": [
        "arn:aws:s3:::fa_bucket",
        "arn:aws:s3:::fa_bucket/*"
      ]
    }
  ]
}
```

6. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
7. Per Nome* immetti **FleetAdvisorS3Policy**, quindi scegli Crea policy.

Per creare una policy IAM per l'accesso del raccogliatore di dati DMS a DMS Fleet Advisor

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Crea policy seleziona la scheda JSON.
5. Incolla il seguente codice JSON nell'editor per sostituire il codice di esempio.

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

```
{
  "Effect": "Allow",
  "Action": [
    "dms:DescribeFleetAdvisorCollectors",
    "dms:ModifyFleetAdvisorCollectorStatuses",
    "dms:UploadFileMetadataList"
  ],
  "Resource": "*"
}
```

6. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
7. Per Nome* immetti **DMSCollectorPolicy**, quindi scegli Crea policy.

Per creare un utente IAM con le autorizzazioni minime per utilizzare il raccogliore di dati DMS

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Utenti.
3. Scegli Aggiungi utenti.
4. Nella pagina Aggiungi utente immetti **FleetAdvisorCollectorUser** per Nome utente*. Scegli Chiave di accesso - Accesso programmatico per Seleziona il tipo di accesso AWS. Scegli Successivo: Autorizzazioni.
5. Nella sezione Imposta autorizzazioni scegli Collega direttamente le policy esistenti.
6. Usa il controllo di ricerca per trovare e scegliere le politiche DMS CollectorPolicy e FleetAdvisorS3Policy che hai creato in precedenza. Scegliere Successivo: Tag.
7. Nella pagina Tag, scegliere Successivo: esamina.
8. Nella pagina Review (Verifica) scegli Create user (Crea utente). Nella pagina successiva scegli Scarica .csv per salvare le nuove credenziali dell'utente. Utilizza queste credenziali con DMS Fleet Advisor per le autorizzazioni di accesso minime richieste.

Per creare un ruolo IAM per l'accesso di DMS Fleet Advisor e del raccogliore dati ad Amazon S3

1. Accedi alla AWS Management Console e apri la console di IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Ruoli.

3. Selezionare Create role (Crea ruolo).
4. Nella pagina Seleziona un'entità attendibile scegli Servizio AWS per Tipo di entità attendibile. Per Casi d'uso per altri servizi AWS scegli DMS.
5. Seleziona la casella di controllo DMS e scegli Successivo.
6. Nella pagina Aggiungi autorizzazioni, scegli S3Policy. FleetAdvisor Seleziona Avanti.
7. Nella pagina Nomina, verifica e crea immetti **FleetAdvisorS3Role** per Nome ruolo e scegli Crea ruolo.
8. Nella pagina Ruoli immetti **FleetAdvisorS3Role** per Nome ruolo. Scegli S3Role. FleetAdvisor
9. Nella pagina FleetAdvisorS3Role, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.
10. Nella pagina Modifica policy di attendibilità incolla il seguente codice JSON nell'editor, sostituendo il testo esistente.

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

La policy precedente concede l'autorizzazione `sts:AssumeRole` ai servizi utilizzati da AWS DMS per importare i dati raccolti dal bucket Amazon S3.

11. Scegli Aggiorna policy.

Creazione del ruolo collegato ai servizi DMS Fleet Advisor

DMS Fleet Advisor utilizza un ruolo collegato ai servizi per gestire le CloudWatch metriche di Amazon nel tuo Account AWS DMS Fleet Advisor utilizza questo ruolo collegato al servizio per pubblicare i parametri di performance del database raccolti per tuo conto. CloudWatch

Per creare il ruolo collegato ai servizi per DMS Fleet Advisor

1. Accedi alla AWS Management Console e apri la console di IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Ruoli. Quindi seleziona Create role (Crea ruolo).
3. Per Tipo di entità attendibile, scegli Servizio AWS.
4. Per Casi d'uso per altri servizi AWS scegli DMS Fleet Advisor.
5. Seleziona la casella di controllo DMS Fleet Advisor e scegli Successivo.
6. Nella pagina Add permissions (Aggiungi autorizzazioni), scegli Next (Successivo).
7. Nella pagina Nomina, rivedi e crea scegli Crea ruolo.

In alternativa, puoi creare questo ruolo collegato ai servizi dall'API AWS o dalla AWS CLI. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi per AWS DMS Fleet Advisor](#).

Dopo aver creato il ruolo collegato ai servizi per DMS Fleet Advisor, puoi visualizzare le metriche delle prestazioni per i tuoi database di origine nei suggerimenti delle destinazioni. Inoltre, puoi visualizzare queste metriche e nel tuo account. CloudWatch Per ulteriori informazioni, consulta [Suggerimenti delle destinazioni](#).

Per creare una policy IAM necessaria per il ruolo collegato ai servizi di DMS Fleet Advisor

Le autorizzazioni minime necessarie per creare il ruolo collegato al servizio sono specificate nella policy `DMSFleetAdvisorCreateServiceLinkedRolePolicy`. Crea questa policy IAM per il tuo account se non è possibile creare il ruolo collegato al servizio.

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Crea policy seleziona la scheda JSON.
5. Incolla il seguente codice JSON nell'editor per sostituire il codice di esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "arn:aws:iam::*:role/aws-service-role/dms-fleet-
advisor.amazonaws.com/AWSServiceRoleForDMSFleetAdvisor*",
      "Condition": {"StringLike": {"iam:AWSServiceName": "dms-fleet-
advisor.amazonaws.com"}}
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PutRolePolicy"
      ],
      "Resource": "arn:aws:iam::*:role/aws-service-role/dms-fleet-
advisor.amazonaws.com/AWSServiceRoleForDMSFleetAdvisor*"
    }
  ]
}
```

6. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
7. Per Nome* immetti **DMSFleetAdvisorCreateServiceLinkedRolePolicy**, quindi scegli Crea policy.

Ora è possibile utilizzare questa policy per creare il ruolo collegato ai servizi per DMS Fleet Advisor.

Creazione di utenti di database per AWS DMS Fleet Advisor

In questa sezione viene descritto come creare gli utenti per i database di origine con le autorizzazioni minime richieste per il raccogliitore di dati DMS.

Questa sezione contiene i seguenti argomenti:

- [Utilizzo di un utente di database con AWS DMS Fleet Advisor](#)
- [Creazione di un utente di database con MySQL](#)
- [Creazione di un utente di database con Oracle](#)
- [Creazione di un utente di database con PostgreSQL](#)

- [Creazione di un utente di database con Microsoft SQL Server](#)
- [Eliminazione degli utenti di database](#)

Utilizzo di un utente di database con AWS DMS Fleet Advisor

È possibile utilizzare un utente del database diverso da `root` con il raccogliatore di dati DMS. Specifica il nome utente e la password dopo aver aggiunto il database all'inventario, ma prima di eseguire il raccogliatore di dati. Per ulteriori informazioni sull'aggiunta dei database all'inventario, consulta [Gestione degli oggetti monitorati](#).

Quando hai terminato di utilizzare il raccogliatore di dati DMS, puoi eliminare gli utenti di database che hai creato. Per ulteriori informazioni, consulta [Eliminazione degli utenti di database](#).

Important

Negli esempi seguenti, sostituisci `{your_user_name}` con il nome dell'utente di database che hai creato per il database. Quindi, sostituisci `{your_password}` con una password sicura.

Creazione di un utente di database con MySQL

Per creare un utente di database in un database di origine MySQL, utilizza lo script seguente. Assicurati di conservare una versione dell'istruzione GRANT che dipenda dalla versione del database MySQL.

```
CREATE USER {your_user_name} identified BY '{your_password}';

GRANT PROCESS ON *.* TO {your_user_name};
GRANT REFERENCES ON *.* TO {your_user_name};
GRANT TRIGGER ON *.* TO {your_user_name};
GRANT EXECUTE ON *.* TO {your_user_name};

# For MySQL versions lower than 8.0, use the following statement.
GRANT SELECT, CREATE TEMPORARY TABLES ON `temp`.* TO {your_user_name};

# For MySQL versions 8.0 and higher, use the following statement.
GRANT SELECT, CREATE TEMPORARY TABLES ON `mysql`.* TO {your_user_name};

GRANT SELECT ON performance_schema.* TO {your_user_name};
```

```

SELECT
  IF(round(Value1 + Value2 / 100 + Value3 / 10000, 4) > 5.0129, 'GRANT EVENT ON *.*
  TO {your_user_name};', 'SELECT ''Events are not applicable'';) sql_statement
INTO @stringStatement
FROM (
  SELECT
    substring_index(ver, '.', 1) value1,
    substring_index(substring_index(ver, '.', 2), '.', - 1) value2,
    substring_index(ver, '.', - 1) value3
  FROM (
    SELECT
      IF((@@version regexp '^[^0-9\.]+' ) != 0, @@innodb_version, @@version) AS ver
    FROM dual
  ) vercase
) v;

PREPARE sqlStatement FROM @stringStatement;
SET @stringStatement := NULL;
EXECUTE sqlStatement;
DEALLOCATE PREPARE sqlStatement;

```

Creazione di un utente di database con Oracle

Per creare un utente di database in un database di origine Oracle, utilizza lo script seguente.

Per eseguire questo script SQL, connessi al database Oracle utilizzando i privilegi SYSDBA. Dopo aver eseguito lo script SQL, connessi al database utilizzando le credenziali dell'utente che hai creato con questo script. Usa le credenziali di questo utente anche per eseguire il raccogliatore di dati DMS.

Lo script seguente aggiunge il prefisso C## al nome dell'utente per i database container (CDB) multi-tenant Oracle.

```

CREATE USER {your_user_name} IDENTIFIED BY "{your_password}";
GRANT CREATE SESSION TO {your_user_name};
GRANT SELECT ANY DICTIONARY TO {your_user_name};
GRANT SELECT ON DBA_WM_SYS_PRIVS TO {your_user_name};
BEGIN
  DBMS_NETWORK_ACL_ADMIN.CREATE_ACL(
    acl => UPPER('{your_user_name}') || '_Connect_Access.xml',
    description => 'Connect Network',
    principal => UPPER('{your_user_name}'),
    is_grant => TRUE,

```

```

    privilege => 'resolve',
    start_date => NULL,
    end_date => NULL);

DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL(
    acl => UPPER('{your_user_name}') || '_Connect_Access.xml',
    host => '*',
    lower_port => NULL,
    upper_port => NULL);

END;
```

Creazione di un utente di database con PostgreSQL

Per creare un utente di database in un database di origine PostgreSQL, utilizza lo script seguente.

```

CREATE USER "{your_user_name}" WITH LOGIN PASSWORD '{your_password}';
GRANT pg_read_all_settings TO "{your_user_name}";

-- For PostgreSQL versions 10 and higher, add the following statement.
GRANT EXECUTE ON FUNCTION pg_ls_waldir() TO "{your_user_name}";
```

Creazione di un utente di database con Microsoft SQL Server

Per creare un utente di database in un database di origine Microsoft SQL Server, utilizza lo script seguente.

```

USE master
GO

IF NOT EXISTS (SELECT * FROM sys.sql_logins WHERE name = N'{your_user_name}')

    CREATE LOGIN [{your_user_name}] WITH PASSWORD=N'{your_password}',
    DEFAULT_DATABASE=[master], DEFAULT_LANGUAGE=[us_english], CHECK_EXPIRATION=OFF,
    CHECK_POLICY=OFF

GO

GRANT VIEW SERVER STATE TO [{your_user_name}]

GRANT VIEW ANY DEFINITION TO [{your_user_name}]

GRANT VIEW ANY DATABASE TO [{your_user_name}]
```

```

IF LEFT(CONVERT(SYSNAME,SERVERPROPERTY('ProductVersion')), CHARINDEX('.',
CONVERT(SYSNAME,SERVERPROPERTY('ProductVersion')), 0)-1) >= 12
EXECUTE('GRANT CONNECT ANY DATABASE TO [{your_user_name}]')

DECLARE @dbname VARCHAR(100)
DECLARE @statement NVARCHAR(max)

DECLARE db_cursor CURSOR
LOCAL FAST_FORWARD
FOR
    SELECT
        name
    FROM MASTER.sys.databases
    WHERE state = 0
        AND is_read_only = 0
        OPEN db_cursor
FETCH NEXT FROM db_cursor INTO @dbname
    WHILE @@FETCH_STATUS = 0
BEGIN

    SELECT @statement = 'USE '+ quotename(@dbname) +';'+ '
    IF NOT EXISTS (SELECT * FROM sys.syslogins WHERE name = ''{your_user_name}'') OR
    NOT EXISTS (SELECT * FROM sys.sysusers WHERE name = ''{your_user_name}'')
    CREATE USER [{your_user_name}] FOR LOGIN [{your_user_name}];

    EXECUTE sp_addrolemember N'db_datareader', [{your_user_name}]

    BEGIN TRY
        EXECUTE sp_executesql @statement
    END TRY
    BEGIN CATCH
        DECLARE @err NVARCHAR(255)

        SET @err = error_message()

        PRINT @dbname
        PRINT @err
    END CATCH

    FETCH NEXT FROM db_cursor INTO @dbname
END
CLOSE db_cursor
DEALLOCATE db_cursor

```

```
USE msdb
GO

GRANT EXECUTE ON dbo.agent_datetime TO [{your_user_name}]
```

Eliminazione degli utenti di database

Dopo aver completato tutte le attività di raccolta dati, puoi eliminare gli utenti di database che hai creato per il raccogliitore di dati DMS. È possibile utilizzare i seguenti script per eliminare gli utenti con le autorizzazioni minime dai database.

Per eliminare l'utente dal database MySQL, esegui lo script seguente.

```
DROP USER IF EXISTS "{your_user_name}";
```

Per eliminare l'utente dal database Oracle, esegui lo script seguente.

```
DECLARE
  -- Input parameters, please set correct value
  cnst$user_name CONSTANT VARCHAR2(255) DEFAULT '{your_user_name}';

  -- System variables, please, don't change
  var$is_exists INTEGER DEFAULT 0;
BEGIN
  SELECT COUNT(hal.acl) INTO var$is_exists
  FROM dba_host_acls hal
  WHERE hal.acl LIKE '%' || UPPER(cnst$user_name) || '_Connect_Access.xml';
  IF var$is_exists > 0 THEN
    DBMS_NETWORK_ACL_ADMIN.DROP_ACL(
      acl => UPPER(cnst$user_name) || '_Connect_Access.xml');
  END IF;
  SELECT COUNT(usr.username) INTO var$is_exists
  FROM all_users usr
  WHERE usr.username = UPPER(cnst$user_name);
  IF var$is_exists > 0 THEN
    EXECUTE IMMEDIATE 'DROP USER ' || cnst$user_name || ' CASCADE';
  END IF;
END;
```

Per eliminare l'utente dal database PostgreSQL, esegui lo script seguente.

```
DROP USER IF EXISTS "{your_user_name}";
```

Per eliminare l'utente dal database SQL Server, esegui lo script seguente.

```
USE msdb
GO

REVOKE EXECUTE ON dbo.agent_datetime TO [{your_user_name}]

USE master
GO

DECLARE @dbname VARCHAR(100)
DECLARE @statement NVARCHAR(max)

DECLARE db_cursor CURSOR
LOCAL FAST_FORWARD
FOR
SELECT
    name
FROM MASTER.sys.databases
WHERE state = 0
    AND is_read_only = 0
    OPEN db_cursor
FETCH NEXT FROM db_cursor INTO @dbname
    WHILE @@FETCH_STATUS = 0
BEGIN

SELECT @statement = 'USE ' + quotename(@dbname) + ';' + '
EXECUTE sp_droprolemember N'db_datareader', [{your_user_name}]

IF EXISTS (SELECT * FROM sys.syslogins WHERE name = '{your_user_name}')
    OR EXISTS (SELECT * FROM sys.sysusers WHERE name = '{your_user_name}')
    DROP USER [{your_user_name}];'

BEGIN TRY
EXECUTE sp_executesql @statement
END TRY
BEGIN CATCH
    DECLARE @err NVARCHAR(255)

    SET @err = error_message()

    PRINT @dbname
    PRINT @err
END CATCH
```

```
FETCH NEXT FROM db_cursor INTO @dbname
END
CLOSE db_cursor
DEALLOCATE db_cursor

GO

IF EXISTS (SELECT * FROM sys.sql_logins WHERE name = N'{your_user_name}')
DROP LOGIN [{your_user_name}] -- Use for SQL login

GO
```

Individuazione dei database per la migrazione utilizzando i raccoglitori di dati

Per scoprire la tua infrastruttura di dati di origine, puoi utilizzare [AWSApplication Discovery Service Agentless Collector](#) o gli agenti di raccolta di dati AWS DMS. ADS Agentless Collector è un'applicazione on-premise che raccoglie tramite metodi agentless le informazioni sull'ambiente on-premise, tra cui informazioni sul profilo del server (ad esempio, sistema operativo, numero di CPU, quantità di RAM), metadati del database e metriche di utilizzo. Agentless Collector si installa come macchina virtuale (VM) nell'ambiente VMware vCenter Server utilizzando un file Open Virtualization Archive (OVA). Un raccoglitore di AWS DMS dati è un'applicazione Windows che si installa nell'ambiente locale. Questa applicazione si connette all'ambiente dei dati e raccoglie metadati e metriche delle prestazioni dal database on-premise e dai server di analisi. Una volta raccolti i metadati del database e le metriche delle prestazioni tramite ADS Agentless Collector o un agente di raccolta dati DMS, DMS Fleet Advisor crea un inventario di server, database e schemi che è possibile migrare al Cloud AWS.

Il raccoglitore di dati DMS è un'applicazione Windows che utilizza librerie.NET, connettori e provider di dati per connettersi ai database di origine per l'individuazione e la raccolta dei dati.

Il raccoglitore di dati DMS funziona su Windows. Tuttavia, il raccoglitore di dati DMS può raccogliere dati da tutti i fornitori di database supportati indipendentemente dal server del sistema operativo su cui vengono eseguiti.

Il raccoglitore di dati DMS utilizza un protocollo RTPS protetto con crittografia TLS per stabilire una connessione sicura con DMS Fleet Advisor. Pertanto, per impostazione predefinita, i dati vengono crittografati durante il transito.

AWS DMS dispone del numero massimo di raccoglitori di dati che puoi creare per il tuo Account AWS. Per informazioni sulle quote di servizio di AWS DMS, consulta [Quote per AWS Database Migration Service](#).

Argomenti

- [Autorizzazioni per il raccoglitore di dati DMS](#)
- [Creazione di un raccoglitore di dati per AWS DMS Fleet Advisor](#)
- [Installazione e configurazione di un raccoglitore di dati](#)
- [Individuazione dei server del sistema operativo e di database da monitorare](#)
- [Gestione degli oggetti monitorati](#)
- [Utilizzo di SSL con AWS DMS Fleet Advisor](#)
- [Raccolta di dati per AWS DMS Fleet Advisor](#)
- [Risoluzione dei problemi relativi al raccoglitore di dati DMS](#)

Autorizzazioni per il raccoglitore di dati DMS

Gli utenti del database che crei per il raccoglitore di dati DMS devono disporre delle autorizzazioni di lettura. Tuttavia, in alcuni casi, l'utente del database richiede l'autorizzazione EXECUTE. Per ulteriori informazioni, consulta [Creazione di utenti di database per AWS DMS Fleet Advisor](#).

Il raccoglitore di dati DMS richiede autorizzazioni aggiuntive per eseguire gli script di individuazione.

- Per l'individuazione del sistema operativo, il raccoglitore di dati DMS necessita delle credenziali affinché il server di dominio possa eseguire le richieste utilizzando il protocollo LDAP.
- Per l'individuazione dei database in Linux, il raccoglitore di dati DMS necessita di credenziali con autorizzazioni sudo SSH. Inoltre, è necessario configurare i server Linux per consentire l'esecuzione di script SSH remoti.
- Per l'individuazione dei database in Windows, il raccoglitore di dati DMS necessita di credenziali con autorizzazioni per eseguire le query di Windows Management Instrumentation (WMI) e WMI Query Language (WQL) e leggere il registro. Inoltre, è necessario configurare i server Windows per consentire l'esecuzione remota di WMI, WQL e script PowerShell.

Creazione di un raccoglitore di dati per AWS DMS Fleet Advisor

Informazioni su come creare e scaricare un raccoglitore di dati DMS.

Prima di creare un raccogliatore di dati, utilizza la console IAM per creare un ruolo collegato ai servizi per DMS Fleet Advisor. Questo ruolo consente ai responsabili di pubblicare punti dati metrici su Amazon. CloudWatch DMS Fleet Advisor utilizza questo ruolo per visualizzare i grafici con le metriche del database. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi per AWS DMS Fleet Advisor](#).

Per creare e scaricare un raccogliatore di dati

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).



Scegli la regione in cui desideri utilizzare DMS Fleet Advisor.

2. Nel riquadro di navigazione, scegli Raccoglitori di dati in Scopri. Viene visualizzata la pagina Raccoglitori di dati.
3. Scegli Crea raccogliatore di dati. Viene visualizzata la pagina Crea raccogliatore di dati.

DMS > Discover: Data collectors > Create data collector

Create data collector Info

Create a data collector to identify servers, databases, and schemas on a network. After the data collector is created, you're prompted to register it by downloading and installing a local collector.

 You can create a maximum of 10 data collectors. [Learn more](#) 

General configuration

Name

Can have only Unicode letters, digits, white space, or one of the symbols in parentheses: `[_:/=+-@()]`. Maximum of 60 characters.

Description - optional

Provide a description of the data collector purpose, environment, or network to help you identify it in the future.

Can have only Unicode letters, digits, white space, or one of the symbols in parentheses: `[_:/=+-@()]`. Maximum of 255 characters.

Connectivity Info

Amazon S3 bucket


Choose or create an Amazon S3 bucket to store collected metadata. Ensure this bucket is the currently selected region.

[View](#) [Browse S3](#)

To create a bucket role, go to [S3](#) 

IAM role

Choose or create an IAM role that grants AWS DMS permissions to access the specified S3 bucket.

To create an IAM role, go to [IAM console](#) 

[Cancel](#)[Create data collector](#)

4. Per Nome nella sezione Configurazione generale, inserisci il nome del raccogliitore di dati.

5. Nella sezione Connettività scegli Sfoglia S3. Scegli il bucket Amazon S3 che hai preconfigurato dall'elenco visualizzato.

AWS DMS archivia i metadati dell'inventario DMS Fleet Advisor in questo bucket S3. Assicurati che il bucket Amazon S3 sia nella stessa Regione AWS in cui è attualmente in esecuzione AWS DMS Fleet Advisor.

Note

DMS Fleet Advisor supporta solo i bucket crittografati SSE-S3.

6. Nell'elenco dei ruoli IAM, scegli il ruolo IAM preconfigurato dall'elenco visualizzato. Questo ruolo fornisce ad AWS DMS le autorizzazioni di accesso al bucket Amazon S3 specificato.
7. Scegli Crea raccoglitore di dati. Viene visualizzata la pagina Raccoglitori di dati e il raccoglitore di dati creato è presente nell'elenco.

Quando crei il tuo primo raccoglitore di dati, AWS DMS configura un ambiente nel bucket Amazon S3 che formatta i dati e archivia gli attributi da utilizzare con DMS Fleet Advisor.

8. Scegli Scarica il raccoglitore locale nel banner informativo per scaricare il raccoglitore di dati appena creato. Viene visualizzato un messaggio che ti informa che il download è in corso. Una volta che il download è terminato, puoi accedere al file `AWS_DMS_Collector_Installer_ version_number .msi`.

Ora puoi installare il raccoglitore di dati DMS sul client. Per ulteriori informazioni, consulta [Installazione e configurazione di un raccoglitore di dati](#).

Installazione e configurazione di un raccoglitore di dati

Informazioni su come installare il raccoglitore di dati DMS, specificare le credenziali di inoltro dei dati e aggiungere un server LDAP al progetto.

La tabella seguente descrive i requisiti hardware e software per l'installazione di un raccoglitore di dati DMS.

Minimo	Consigliato
Processore: 2 core con punteggio di benchmark della CPU superiore a 8.000	Processore: 4 core con punteggio di benchmark della CPU superiore a 11.000

Minimo	Consigliato
RAM: 8 GB	RAM: 16 GB
Dimensioni del disco rigido: 256 GB	Dimensioni del disco rigido: 512 GB
Sistema operativo: Microsoft Windows Server 2012 o versioni successive	Sistema operativo: Windows Server 2016 o versioni successive

Per installare un raccogliitore di dati su un client della rete

1. Esegui il programma di installazione .MSI. Viene visualizzata la pagina Installazione guidata del raccogliitore AWS DMS Fleet Advisor.
2. Seleziona Avanti. Viene visualizzato il contratto di licenza per l'utente finale.
3. Leggi e accetta il contratto di licenza per l'utente finale.
4. Seleziona Avanti. Viene visualizzata la pagina Cartella di destinazione.
5. Scegli Successivo per installare il raccogliitore di dati nella directory predefinita.

In alternativa, scegli Cambia per inserire un'altra directory di installazione. Quindi scegli Successivo.

6. Nella pagina Collegamento desktop seleziona la casella per installare un'icona sul desktop.
7. Scegli Installa. Il raccogliitore dati viene installato nella directory scelta.
8. Nella pagina Installazione guidata del raccogliitore DMS completata scegli Avvia raccogliitore AWS DMS, quindi seleziona Fine.

Il raccogliitore di dati DMS utilizza librerie .NET, connettori e fornitori di dati per connettersi ai database di origine. Il programma di installazione del raccogliitore di dati DMS installa automaticamente questo software necessario per tutti i database supportati sul server.

Dopo aver installato il raccogliitore di dati, puoi eseguirlo da un browser immettendo **http://localhost:11000/** come indirizzo. Facoltativamente, dal menu Start di Microsoft Windows, scegli Raccogliitore AWS DMS nell'elenco dei programmi. Quando esegui il raccogliitore di dati DMS per la prima volta, ti viene richiesto di configurare le credenziali. Crea il nome utente e la password per accedere al raccogliitore di dati.

Nella home page del raccogliatore di dati DMS, puoi trovare le informazioni per preparare ed eseguire la raccolta dei metadati, incluse le seguenti condizioni di stato:

- Stato e integrità della raccolta di dati.
- Accessibilità al bucket Amazon S3 e ad AWS DMS per permettere al raccogliatore di inoltrare i dati ad AWS DMS.
- Connettività ai driver del database installati.
- Credenziali di un server LDAP per eseguire l'individuazione iniziale.

The screenshot displays the AWS DMS Collector interface. At the top, there's a navigation bar with the AWS logo and 'DMS Collector' text, and a 'Sign out' link. The main content area is titled 'Home' and contains three panels:

- Data collection:** Status: Running, Health: 100%.
- Data forwarding:** Name: new-data-collector, Access to Amazon S3: Yes, Access to AWS DMS: Yes, Last updated: 31-01-2023 11:43:30. A 'Configure forwarding' button is visible.
- Software check (4/4):** Microsoft SQL Server connector for .NET: Passed, MySQL connector for .NET: Passed, Oracle data provider for .NET: Passed, PostgreSQL connector for .NET: Passed.

Below these panels is the 'LDAP servers configuration' section, which includes a '+ Server' button and a table with the following data:

LDAP server host name ↓	User name	Connection status
<input type="checkbox"/> dc01.dbm.local	shareduser	Passed

Il raccogliatore di dati DMS utilizza una directory LDAP per raccogliere le informazioni sui computer e sui server di database della rete. Lightweight Directory Access Protocol (LDAP) è un protocollo applicativo standard aperto. Viene utilizzato per accedere e gestire i servizi distribuiti di informazioni sulle directory su una rete IP. Puoi aggiungere un server LDAP esistente al progetto per la raccolta di dati che puoi usare per individuare le informazioni sull'infrastruttura dei sistemi. Per farlo, scegli l'opzione +Server, quindi specifica un nome di dominio completo (FQDN) e le credenziali per il controller di dominio. Dopo aver aggiunto il server, convalida il controllo della connessione. Per le nozioni di base sul processo di individuazione, consulta [Individuazione dei server del sistema operativo e di database da monitorare](#).

Configurazione delle credenziali per l'inoltro dei dati

Dopo aver installato il raccogliitore di dati, assicurati che questa applicazione possa inviare i dati raccolti ad AWS DMS Fleet Advisor.

Per configurare le credenziali per l'inoltro dei dati in AWS DMS Fleet Advisor

1. Nella home page del raccogliitore di dati DMS scegli Configura l'inoltro nella sezione Inoltro dei dati. Viene visualizzata la finestra di dialogo Configura le credenziali per l'inoltro dei dati.
2. Scegli la Regione AWS in cui intendi utilizzare DMS Fleet Advisor.
3. Inserisci l'ID chiave di accesso AWS e la chiave di accesso segreta AWS ottenute in precedenza durante la creazione delle risorse IAM. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).
4. Scegli Sfoglia raccoglitori di dati.

Se non hai ancora creato un raccogliitore di dati nella regione specificata, crea un raccogliitore di dati prima di procedere. Per ulteriori informazioni, consulta [Creazione di un raccogliitore di dati](#).

5. Nella finestra Scegli raccogliitore di dati seleziona un raccogliitore di dati nell'elenco e fai clic su Scegli.
6. Nella finestra di dialogo Configura le credenziali per l'inoltro dei dati scegli Salva.

Nella home page di Raccogliitore DMS, verifica nella scheda Inoltro dei dati che gli stati Accesso ad Amazon S3 e Accesso ad AWS DMS siano impostati su Sì.

Se vedi che lo stato di Accesso ad Amazon S3 o Accesso ad AWS DMS è impostato su No, assicurati di aver creato le risorse IAM per accedere ad Amazon S3 e DMS Fleet Advisor. Dopo aver creato queste risorse IAM con tutte le autorizzazioni necessarie, configura nuovamente l'inoltro dei dati. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).

Individuazione dei server del sistema operativo e di database da monitorare

Puoi utilizzare il raccogliitore di dati DMS per individuare ed elencare tutti i server disponibili nella rete. L'individuazione di tutti i server di database disponibili nella rete è una procedura consigliata, ma non obbligatoria. Facoltativamente, puoi aggiungere o caricare manualmente l'elenco dei server per un'altra raccolta di dati. Per ulteriori informazioni sull'aggiunta manuale di un elenco di server, consulta [Gestione degli oggetti monitorati](#).

Ti consigliamo di individuare prima tutti i server del sistema operativo (OS) e poi i database sui server. Per scoprire i server del sistema operativo, è necessaria l'autorizzazione per eseguire script e comandi remoti PowerShell, Secure Shell (SSH) e Windows Management Instrumentation (WMI), oltre all'accesso al registro di Windows. Per individuare i server di database presenti nella rete e raccogliere i relativi metadati, sono necessarie le autorizzazioni di amministratore di sola lettura per una connessione remota al database. Assicurati di aver aggiunto un server LDAP prima di procedere con l'individuazione. Per ulteriori informazioni, consulta [Configurazione delle credenziali per l'inoltro dei dati](#).

Per iniziare a utilizzare il raccogliatore di dati DMS, completa le attività descritte di seguito:

- Individua tutti i server del sistema operativo presenti nella rete.
- Aggiungi i server del sistema operativo specifici come oggetti da monitorare.
- Verifica le connessioni dei server del sistema operativo monitorati.
- Individua i database Microsoft SQL Server, MySQL, Oracle e PostgreSQL in esecuzione sui server del sistema operativo.
- Aggiungi i server di database per la raccolta dei dati.
- Verifica le connessioni ai database monitorati.

Per individuare i server del sistema operativo da monitorare presenti nella rete

1. Nel riquadro di navigazione del raccogliatore di dati DMS scegli Individuazione. Per visualizzare il pannello di navigazione seleziona l'icona del menu nell'angolo in alto a sinistra della home page del raccogliatore di dati DMS.

Viene visualizzata la pagina Individuazione.

2. Assicurati che la scheda Server del sistema operativo sia selezionata, quindi scegli Esegui individuazione. Viene visualizzata la finestra di dialogo Parametri di individuazione.
3. Immetti i server LDAP che desideri utilizzare per eseguire la scansione della rete.
4. Scegli Esegui individuazione. La pagina mostra l'elenco di tutti i server del sistema operativo individuati all'interno della rete, indipendentemente dal fatto che stiano eseguendo un database.

Ti consigliamo di eseguire l'individuazione di tutti i server del sistema operativo prima di eseguire quella dei database sui server. Le credenziali rendono possibile l'individuazione prima dei server host, quindi dei database che vi risiedono. È necessario individuare i server del sistema operativo prima di eseguire l'individuazione dei database su tali server. Tieni presente che le

credenziali che utilizzi per consentire a un server LDAP di rilevare i server del sistema operativo nella rete potrebbero differire dalle credenziali necessarie per individuare i database su un particolare server del sistema operativo. Pertanto, ti consigliamo di aggiungere i server del sistema operativo agli oggetti monitorati, verificare le credenziali e correggerle se necessario, quindi controllare la connettività prima di procedere.

Nell'elenco dei server del sistema operativo individuati nella rete, puoi selezionare i server che desideri aggiungere agli oggetti monitorati.

Per selezionare i server del sistema operativo come oggetti da monitorare

1. Nella pagina Individuazione scegli la scheda Server del sistema operativo.
2. Nell'elenco dei server del sistema operativo individuati seleziona la casella di controllo accanto a ciascun server che desideri monitorare.
3. Scegli Aggiungi agli oggetti monitorati.

È possibile visualizzare l'elenco dei server del sistema operativo da monitorare e verificare le connessioni nella pagina Monitoraggio degli oggetti.

Per verificare le connessioni dei server del sistema operativo selezionati da monitorare

1. Nel riquadro di navigazione del raccogliore di dati DMS scegli Oggetti monitorati.
2. Nella pagina Oggetti monitorati scegli la scheda Server del sistema operativo. Viene visualizzato l'elenco di server del sistema operativo individuati da monitorare.
3. Seleziona la casella di controllo nella parte superiore della colonna per scegliere tutti i server del sistema operativo elencati.
4. Scegli Operazioni, quindi Verifica connessione. Vengono visualizzati i risultati di ogni oggetto del server nella colonna Stato delle connessioni.
5. Seleziona i server con lo stato di connessione diverso da Esito positivo. Quindi scegli Operazioni e Modifica. Viene visualizzata la finestra di dialogo Modifica server.
6. Verifica che le informazioni siano corrette o modificali se necessario. Al termine, scegli Save (Salva). Viene visualizzata la finestra di dialogo Sostituisci credenziali.
7. Scegli Sovrascrivi. Il raccogliore di dati DMS verifica e aggiorna lo stato di ogni connessione in Esito positivo.

A questo punto puoi individuare i database che risiedono sui server che hai scelto di monitorare.

Individuazione dei database in esecuzione sui server

1. Nel riquadro di navigazione del raccoglitore di dati DMS scegli Individuazione.
2. Scegli la scheda Server di database e seleziona Esegui individuazione. Viene visualizzata la finestra di dialogo Parametri di individuazione.
3. Nella finestra di dialogo Parametri di individuazione scegli Oggetti monitorati per Individuazione per. Per Server scegli i server del sistema operativo su cui desideri eseguire l'individuazione dei database.
4. Scegli Esegui individuazione. La pagina mostra l'elenco di tutti i database che risiedono sui server del sistema operativo che scegli di monitorare.

Visualizza informazioni come l'indirizzo del database, il nome del server e il motore del database per permetterti di scegliere i database da monitorare.

Per selezionare i database da monitorare

1. Nella pagina Individuazione scegli la scheda Server di database.
2. Nell'elenco dei database individuati visualizzato, seleziona la casella di controllo accanto a tutti i database che desideri monitorare.
3. Scegli Aggiungi agli oggetti monitorati.

A questo punto puoi verificare le connessioni ai database che scegli di monitorare.

Per verificare le connessioni ai database monitorati

1. Nel riquadro di navigazione del raccoglitore di dati DMS scegli Oggetti monitorati.
2. Nella pagina Oggetti monitorati scegli la scheda Server di database. Viene visualizzato l'elenco di server di database individuati che hai scelto di monitorare.
3. Seleziona la casella di controllo nella parte superiore della colonna per scegliere tutti i server di database elencati.
4. Scegli Operazioni, quindi seleziona Verifica connessione. Vengono visualizzati i risultati di ogni database nella colonna Stato delle connessioni.
5. Seleziona le connessioni che hanno uno stato non definito (vuoto) o lo stato Errore. Quindi scegli Operazioni e Modifica. Viene visualizzata la finestra di dialogo Modifica oggetti monitorati.

6. Inserisci le credenziali di accesso e la password, quindi scegli Salva. Viene visualizzata la finestra di dialogo Modifica credenziali.
7. Scegli Sovrascrivi. Il raccoglitore di dati DMS verifica e aggiorna lo stato di ogni connessione in Esito positivo.

Dopo aver individuato i server del sistema operativo e i database da monitorare, puoi eseguire le azioni per gestire gli oggetti monitorati.

Gestione degli oggetti monitorati

È possibile selezionare gli oggetti da monitorare quando si esegue il processo di individuazione dei server, come descritto in [Individuazione dei server del sistema operativo e di database](#). Inoltre, puoi gestire manualmente gli oggetti, come i server del sistema operativo e i server di database. Per gestire gli oggetti monitorati puoi eseguire le seguenti azioni:

- Aggiunta di nuovi oggetti da monitorare
- Rimozione di oggetti esistenti
- Modifica di oggetti esistenti
- Esportazione e importazione di un elenco di oggetti da monitorare
- Verifica delle connessioni agli oggetti
- Avvio della raccolta dei dati

Ad esempio, è possibile aggiungere manualmente un oggetto da monitorare.

Per aggiungere manualmente un oggetto da monitorare

1. Nella pagina Oggetti monitorati scegli +Server. Viene visualizzata la finestra di dialogo Aggiungi oggetto monitorato.
2. Aggiungi le informazioni sul server, quindi scegli Salva.

Puoi anche usare un file .csv per importare un elenco di diversi oggetti da monitorare. Utilizza il seguente formato di file .csv per importare un elenco di oggetti nel raccoglitore di dati DMS.

```
Hostname - Hostname or IP address of Monitored Object  
Port - TCP port of Monitored Object
```

```
Engine: (one of the following)
  • Microsoft SQL Server
  • Microsoft Windows
  • Oracle Database
  • Linux
  • MySQL Server
  • PostgreSQL

Connection type: (one of the following)
  • Login/Password Authentication
  • Windows Authentication
  • Key-Based Authentication

Domain name:(Windows authentication)
  • Use domain name for the account

User name
Password
```

Per importare un file .csv con un elenco di oggetti da monitorare

1. Seleziona Importa. Viene visualizzata la pagina Importa oggetti monitorati.
2. Individua il file .csv che desideri importare, quindi scegli Successivo.

Puoi visualizzare tutti gli oggetti e selezionare quelli da cui vuoi raccogliere i metadati.

Associazione di un server del sistema operativo a un database aggiunto manualmente

DMS Fleet Advisor non è in grado di raccogliere le metriche delle prestazioni direttamente dai database MySQL e PostgreSQL. Per raccogliere le metriche necessarie per i suggerimenti delle destinazioni, DMS Fleet Advisor utilizza le metriche del sistema operativo in cui vengono eseguiti i database.

Quando aggiungi manualmente i database MySQL e PostgreSQL all'elenco degli oggetti monitorati, il raccogliitore di dati DMS non è in grado di identificare i server del sistema operativo su cui vengono eseguiti questi database. A causa di questo problema, è necessario associare i database MySQL e PostgreSQL ai server del sistema operativo.

Non è necessario associare manualmente i server del sistema operativo ai database che DMS Fleet Advisor ha individuato automaticamente.

Per associare un server del sistema operativo al database

1. Nel riquadro di navigazione del raccogliitore di dati DMS scegli Oggetti monitorati.

2. Nella pagina Oggetti monitorati scegli la scheda Server di database. Viene visualizzato un elenco di server di database.
3. Seleziona la casella di controllo accanto al server database MySQL o PostgreSQL aggiunto manualmente.
4. Scegli Operazioni e seleziona Modifica. Viene visualizzata la finestra di dialogo Modifica database.
5. Se il raccogliatore di dati DMS ha già individuato il server del sistema operativo su cui viene eseguito il database, scegli Individuazione automatica. Il raccogliatore di dati DMS esegue uno script SQL per identificare automaticamente il server del sistema operativo su cui viene eseguito il database. Quindi, il raccogliatore di dati DMS associa questo server del sistema operativo al database. Ignora il prossimo passaggio e salva la configurazione del database che hai modificato.

Se il raccogliatore di dati DMS non è in grado di identificare automaticamente il server del sistema operativo per il database, assicurati di utilizzare le credenziali corrette e di fornire le autorizzazioni di accesso al database. Facoltativamente, puoi aggiungere il server del sistema operativo manualmente.

6. Per aggiungere il server del sistema operativo manualmente, scegli +Aggiungi server del sistema operativo. Viene visualizzata la finestra di dialogo Aggiungi server del sistema operativo host.

Aggiungi le informazioni sul server del sistema operativo, quindi scegli Salva.

7. Nella finestra di dialogo Modifica database scegli Verifica connessione per assicurarti che il raccogliatore di dati DMS possa connettersi al server del sistema operativo.
8. Una volta verificata la connessione, scegli Salva.

Se modifichi il server del sistema operativo associato del database di origine, DMS Fleet Advisor utilizza le metriche aggiornate per generare i suggerimenti. Tuttavia, i CloudWatch grafici di Amazon mostrano i vecchi dati del tuo server di database. Per ulteriori informazioni sui CloudWatch grafici, consulta [Dettagli dei suggerimenti](#).

Utilizzo di SSL con AWS DMS Fleet Advisor

Per proteggere i dati, AWS DMS Fleet Advisor può utilizzare SSL per accedere ai database.

Database supportati

AWS DMS Fleet Advisor supporta l'utilizzo di SSL per accedere ai seguenti database:

- Microsoft SQL Server
- MySQL
- PostgreSQL

Configurazione di SSL

Per utilizzare SSL per accedere al database, configura il server del database in modo che supporti SSL. Per ulteriori informazioni, consulta la documentazione seguente per il database in uso:

- SQL Server: [Enable encrypted connections to the Database Engine](#)
- MySQL: [Configuring MySQL to Use Encrypted Connections](#)
- PostgreSQL: [Secure TCP/IP Connections with SSL](#)

Per utilizzare SSL per la connessione al database, seleziona **Considera attendibile il certificato del server** e **Usa SSL** quando aggiungi un server manualmente. Per un database MySQL puoi usare un certificato personalizzato. Per utilizzare un certificato personalizzato, seleziona la casella di controllo **Verifica CA**. Per informazioni sull'aggiunta di un server, consulta [Gestione degli oggetti monitorati](#).

Verifica del certificato CA (Certificate Authority) del server per SQL Server

Se desideri convalidare il certificato CA (Certificate Authority) del server per SQL Server, **deseleziona** **Considera attendibile il certificato del server** quando aggiungi il server. Se il server utilizza una CA nota e la CA è installata per impostazione predefinita nel sistema operativo, la verifica funziona normalmente. Se DMS Fleet Advisor non riesce a connettersi al server del database, installa il certificato CA utilizzato dal server di database. Per ulteriori informazioni, consulta [Configure client](#).

Raccolta di dati per AWS DMS Fleet Advisor

Per iniziare a raccogliere i dati, seleziona gli oggetti nella pagina **Oggetti monitorati** e scegli **Esegui raccolta dati**. Il raccogliatore di dati DMS può eseguire fino a 100 database contemporaneamente. Inoltre, il raccogliatore di dati DMS può utilizzare fino a otto thread paralleli per connettersi ai database dell'ambiente. Di questi otto thread, il raccogliatore di dati DMS può usare fino a cinque thread paralleli per connettersi a una singola istanza di database.

Important

Prima di iniziare a raccogliere i dati visualizza la sezione **Controllo del software** nella home page del raccogliatore di dati DMS. Verifica che tutti i motori di database che desideri

monitorare abbiano lo stato Superato. Se alcuni motori di database hanno lo stato Non riuscito e nell'elenco degli oggetti monitorati sono presenti server di database con motori corrispondenti, risolvi il problema prima di procedere. Sono disponibili suggerimenti accanto allo stato Non riuscito elencato nella sezione Controllo del software.

Il raccogliatore di dati DMS può funzionare in due modalità: esecuzione singola o monitoraggio continuo. Dopo aver avviato la raccolta dei dati, viene visualizzata la finestra di dialogo Esegui raccolta dati. Quindi scegli una delle due opzioni seguenti.

Metadati e capacità del database

Il raccogliatore di dati DMS raccoglie le informazioni dal database o dai server del sistema operativo. Include schemi, versioni, edizioni, CPU, memoria e capacità del disco. DMS data collector raccoglie e fornisce anche metriche come IOPS, throughput di I/O e connessioni attive ai server di database. Puoi calcolare i suggerimenti delle destinazioni in DMS Fleet Advisor sulla base di queste informazioni. Se il provisioning del database di origine è eccessivo o insufficiente, anche i suggerimenti delle destinazioni avranno un provisioning eccessivo o insufficiente.

Questa è l'opzione predefinita.

Metadati, capacità del database e utilizzo delle risorse

Oltre ai metadati e alle informazioni sulla capacità del database, il raccogliatore di dati DMS raccoglie i parametri di utilizzo effettivo di CPU, memoria e capacità del disco per i database o i server del sistema operativo. DMS data collector raccoglie e fornisce anche metriche come IOPS, throughput I/O e connessioni attive ai server di database. I suggerimenti delle destinazioni forniti saranno più accurati perché si basano sui carichi di lavoro effettivi del database.

Se scegli questa opzione, dovrai impostare il periodo di raccolta dei dati. Puoi raccogliere dati nei successivi 7 giorni o impostare unintervallo personalizzato compreso tra 1 e 60 giorni.

Dopo l'inizio della raccolta dei dati, vieni reindirizzato alla pagina Raccolta dei dati dove puoi vedere come vengono eseguite le query di raccolta e monitorare l'avanzamento in tempo reale. Puoi vedere lo stato generale della raccolta qui oppure sulla home page del raccogliatore di dati DMS. Se lo stato generale della raccolta dei dati è inferiore al 100%, è possibile che si debbano risolvere dei problemi relativi alla raccolta.

Se esegui il raccogliatore di dati DMS in modalità Metadati e capacità del database puoi vedere il numero di query completate nella pagina Raccolta dei dati.

Se esegui il raccogliitore di dati DMS in modalità Metadati, capacità del database e utilizzo delle risorse puoi vedere il tempo rimanente prima che il raccogliitore di dati DMS completi il monitoraggio.

Nella pagina Raccolta dei dati puoi vedere lo stato della raccolta per ogni oggetto. Se qualcosa non funziona correttamente, viene visualizzato un messaggio che mostra i problemi che si sono verificati. Per determinare una soluzione per un problema, puoi controllare i dettagli. Le seguenti schede elencano i potenziali problemi:

- Riepilogo per query: mostra lo stato dei test, come il test del ping. Puoi filtrare i risultati nella colonna Stato. La colonna Stato fornisce un messaggio che indica quanti errori si sono verificati durante la raccolta dei dati.
- Riepilogo per oggetto monitorato: mostra lo stato generale di ogni oggetto.
- Riepilogo per tipo di query: mostra lo stato del tipo di query del raccogliitore, ad esempio chiamate SQL, Secure Shell (SSH) o Windows Management Instrumentation (WMI).
- Riepilogo per problema: mostra tutti i problemi univoci che si sono verificati, con i nomi dei problemi e il numero di volte in cui si sono verificati.

Data collection Export to CSV

Collection in progress... ✖ Stop collection
 Metadata, database capacity, and resource utilization data are being collected. Make sure you have proper connectivity to OS and database servers.
 0 d 23 hr 9 min remains

Summary by query
Summary by monitored object
Summary by query type
Summary by issue

Monitored object address	Co...	Query name	User name	Engine	Time	Status
10.100.11.241:22	SSH	Linux CPU Stat	dbmuser	Linux	12-01-2023 03:48:30	✔ Complete
10.100.11.241:22	SSH	Linux Meminfo	dbmuser	Linux	12-01-2023 03:48:29	✔ Complete
10.100.11.241:22	SSH	Linux CPU Info	dbmuser	Linux	12-01-2023 02:57:30	✔ Complete
10.100.11.241:5432	Pgsql	AWS RDS Limitations (Database Level)	FA_Collect_User	PostgreSQL	12-01-2023 02:57:29	✔ Complete

Total items: 13

Per esportare i risultati della raccolta, scegli Esporta in CSV.

Dopo aver identificato i problemi e averli risolti, scegli Avvia raccolta ed esegui nuovamente il processo di raccolta dei dati. Dopo aver eseguito la raccolta dei dati, il raccoglitore di dati utilizza le connessioni sicure per caricare i dati raccolti in un inventario DMS Fleet Advisor. DMS Fleet Advisor archivia le informazioni nel bucket Amazon S3. Per informazioni sulla configurazione delle credenziali per l'inoltro dei dati, consulta [Configurazione delle credenziali per l'inoltro dei dati](#).

Raccolta delle metriche di utilizzo della capacità e delle risorse con AWS DMS Fleet Advisor

È possibile raccogliere metadati e metriche delle prestazioni in due modalità: esecuzione singola o monitoraggio continuo. A seconda dell'opzione selezionata, il raccoglitore di dati DMS tiene traccia di diverse metriche nel tuo ambiente di dati. Durante l'esecuzione singola, il raccoglitore di dati DMS tiene traccia solo delle metriche dei metadati del database e dei server del sistema operativo. Durante il monitoraggio continuo, il raccoglitore di dati DMS tiene traccia dell'utilizzo effettivo delle risorse.

AWS DMS raccoglie i seguenti metadati e metriche durante una singola esecuzione del raccoglitore di dati DMS.

- Memoria disponibile sui server del sistema operativo
- Spazio di archiviazione disponibile sui server del sistema operativo
- Versione ed edizione del database
- Numero di CPU sui server del sistema operativo
- Numero di schemi
- Numero di stored procedure
- Numero di tabelle
- Numero di trigger
- Numero di viste
- Struttura dello schema

DMS Fleet Advisor utilizza queste metriche per creare un inventario dei database e dei server del sistema operativo. Inoltre, DMS Fleet Advisor utilizza questi metadati e metriche per analizzare gli schemi del database di origine.

DMS Fleet Advisor può generare raccomandazioni mirate utilizzando le metriche raccolte durante una singola esecuzione del raccoglitore di dati. Tuttavia, in questo caso, per i database di origine

sovradimensionati, anche la raccomandazione di destinazione è sovrafornita. Pertanto, dovrete sostenere costi aggiuntivi per la manutenzione delle vostre risorse in. Cloud AWS Per i database di origine con provisioning è insufficiente, anche il suggerimento della destinazione è con provisioning insufficiente, il che potrebbe causare problemi di prestazioni. Si consiglia di raccogliere i dati utilizzando il monitoraggio continuo scegliendo i metadati, la capacità del database e la modalità di utilizzo delle risorse per il raccoglitore di dati DMS.

AWS DMS raccoglie le seguenti metriche durante il monitoraggio continuo. Puoi utilizzare il raccoglitore di dati DMS per un periodo compreso tra 1 e 60 giorni.

- Velocità di trasmissione effettiva di I/O sui server di database
- Operazioni di input/output al secondo (IOPS) sui server database
- Numero di CPU utilizzate dai server del sistema operativo
- Utilizzo della memoria sui server del sistema operativo
- Numero di connessioni attive al database e al server del sistema operativo

DMS Fleet Advisor utilizza queste metriche per generare suggerimenti precisi sulle destinazioni, in modo che i database di destinazione soddisfino le esigenze di prestazioni. In questo modo è possibile evitare costi aggiuntivi per la manutenzione delle risorse in. Cloud AWS

In che modo AWS DMS Fleet Advisor raccoglie le metriche di utilizzo della capacità e delle risorse?

DMS Fleet Advisor raccoglie le metriche sulle prestazioni ogni minuto.

Per Oracle e SQL Server, DMS Fleet Advisor esegue query SQL per acquisire i valori per ogni metrica del database.

Per MySQL e PostgreSQL, DMS Fleet Advisor raccoglie le metriche delle prestazioni dal server del sistema operativo su cui viene eseguito il database. In Windows, DMS Fleet Advisor esegue gli script WMI Query Language (WQL) e riceve dati WMI. In Linux, DMS Fleet Advisor esegue i comandi che acquisiscono le metriche del server del sistema operativo.

⚠ Important

L'esecuzione di script SQL remoti può influire sulle prestazioni dei database di produzione. Tuttavia, le query di raccolta dei dati non contengono alcuna logica di calcolo. Pertanto, è improbabile che il processo di raccolta dei dati utilizzi più dell'1% delle risorse del database.

Puoi visualizzare tutte le query eseguite dal raccogliatore di dati per raccogliere le metriche. Per farlo, apri il file `DMSCollector.Collections.json`. Questo file è disponibile nella cartella `etc` situata nella stessa cartella in cui hai installato il raccogliatore di dati. Il percorso predefinito è `C:\ProgramData\Amazon\AWS DMS Collector\etc\DMSCollector.Collections.json`.

Il raccogliatore di dati DMS utilizza il file system locale come archiviazione temporanea per tutti i dati raccolti. Il raccogliatore di dati DMS memorizza i dati raccolti in formato JSON. È possibile utilizzare il raccogliatore locale in modalità offline e controllare o verificare manualmente i file raccolti prima di configurare l'inoltro dei dati. Puoi vedere tutti i file raccolti nella cartella `out` situata nella stessa cartella in cui hai installato il raccogliatore di dati DMS. Il percorso predefinito è `C:\ProgramData\Amazon\AWS DMS Collector\out`.

⚠ Important

Se esegui il raccogliatore di dati DMS in modalità offline e archivi i dati raccolti sul tuo server per più di 14 giorni, non puoi utilizzare Amazon CloudWatch per visualizzare questi parametri. Tuttavia, DMS Fleet Advisor utilizza questi dati per generare i suggerimenti. Per ulteriori informazioni sui CloudWatch grafici, consulta [Dettagli dei suggerimenti](#)

È inoltre possibile controllare o verificare i file di dati raccolti in modalità online. Il raccogliatore di dati DMS inoltra tutti i dati al bucket Amazon S3 specificato nelle impostazioni del raccogliatore di dati DMS.

Puoi utilizzare il raccogliatore di dati DMS per raccogliere i dati dai database on-premise. Inoltre, puoi raccogliere i dati dai database Amazon RDS e Aurora. Tuttavia, non puoi eseguire correttamente tutte le query del raccogliatore di dati DMS nel cloud a causa delle differenze tra Amazon RDS o Aurora e le istanze database on-premise. Poiché il raccogliatore di dati DMS raccoglie le metriche di utilizzo per i database MySQL e PostgreSQL dal sistema operativo host, questo approccio non funziona con Amazon RDS e Aurora.

Risoluzione dei problemi relativi al raccogliitore di dati DMS

Nell'elenco seguente sono disponibili le azioni da intraprendere in caso di problemi specifici durante la raccolta dei dati con il raccogliitore di dati.

Argomenti

- [Problemi di raccolta dei dati relativi alle connessioni di rete e server](#)
- [Problemi di raccolta dei dati relativi a Windows Management Instrumentation](#)
- [Problemi di raccolta dei dati relativi a Windows webpage composer](#)
- [Problemi di raccolta dei dati relativi a SSL](#)

Problemi di raccolta dei dati relativi alle connessioni di rete e server

NET: si è verificata un'eccezione durante una richiesta di ping.

Controlla il nome del computer per vedere se è in uno stato per cui non può essere risolto in un indirizzo IP.

Ad esempio, controlla se il computer è spento, disconnesso dalla rete o disattivato.

NET: timeout

Attiva la regola del firewall in entrata "File and Printer Sharing (Echo Request - ICMPv4-In)". Per esempio:

* Inbound ICMPv4

RETE: DestinationHostUnreachable

Verifica l'indirizzo IP del computer. In particolare, controlla se si trova nella stessa sottorete del computer su cui è in esecuzione il raccogliitore di dati DMS e se risponde alle richieste ARP (Address Resolution Protocol).

Se il computer si trova su una sottorete diversa, l'indirizzo IP del gateway non può essere risolto nell'indirizzo MAC (Media Access Control).

Inoltre, controlla se il computer è spento, disconnesso dalla rete o disattivato.

Problemi di raccolta dei dati relativi a Windows Management Instrumentation

WMI: il server RPC non è disponibile. Eccezione da HRESULT: 0x800706BA

Attiva la regola del firewall in entrata "Windows Management Instrumentation (DCOM-In)". Per esempio:

- * Inbound TCP/IP at local port 135.

Inoltre, attiva la regola del firewall in entrata "Windows Management Instrumentation (WMI-In)". Per esempio:

- * Inbound TCP/IP at local port 49152 - 65535 per Windows Server 2008 e versioni successive.

- * Inbound TCP/IP at local port 1025 - 5000 per Windows Server 2003 e versioni precedenti.

WMI: accesso negato. Eccezione da HRESULT: 0x80070005 (E_ACCESSDENIED)

Eeguire quanto segue:

- Aggiungi l'utente del raccoglitore di dati DMS al gruppo Windows, Distributed COM Users o Administrators.
- Avvia il servizio Windows Management Instrumentation e imposta il tipo di avvio su Automatico.
- Assicurati che il nome utente del raccoglitore di dati DMS sia nel formato \.

WMI: accesso negato

Aggiungi l'autorizzazione Abilitazione remota all'utente del raccoglitore di dati DMS nello spazio dei nomi WMI root.

Utilizza le impostazioni avanzate e assicurati che le autorizzazioni si applichino a questo spazio dei nomi e agli spazi dei nomi secondari.

WMI: la chiamata è stata annullata dal filtro dei messaggi. Eccezione da HRESULT: 0x80010002...

Riavvia il servizio Windows Management Instrumentation.

Problemi di raccolta dei dati relativi a Windows webpage composer

WPC: il percorso di rete non è stato trovato

Attiva la regola del firewall in entrata "File and Printer Sharing (SMB-In)". Per esempio:

* `Inbound TCP/IP at local port 445.`

Inoltre, avvia il servizio Registro di sistema remoto e imposta il tipo di avvio su Automatico.

WPC: accesso negato

Aggiungi l'utente del raccogliore di dati DMS al gruppo Performance Monitor Users or Administrators.

WPC: la categoria non esiste

Esegui `loader /r` per ricostruire la cache del contatore delle prestazioni, quindi riavvia il computer.

Note

Per informazioni sulla risoluzione dei problemi relativi alla migrazione dei dati utilizzando AWS Database Migration Service (AWS DMS), consulta [Risoluzione dei problemi e supporto diagnostico](#).

Problemi di raccolta dei dati relativi a SSL

Errori SSL

Il database richiede una connessione SSL sicura e non hai attivato le opzioni Verifica CA e Usa SSL per la connessione. Attiva queste opzioni e assicurati che sul tuo sistema operativo locale sia installata l'Autorità di certificazione utilizzata dal database. Per ulteriori informazioni, consulta [Configurazione di SSL](#).

Utilizzo degli inventari per l'analisi in AWS DMS Fleet Advisor

Per verificare la fattibilità di potenziali migrazioni di database, puoi utilizzare gli inventari dei database e degli schemi individuati. È possibile utilizzare le informazioni contenute negli inventari per comprendere quali database e schemi sono idonei alla migrazione.

Puoi accedere agli inventari di database e schemi dalla console. Per farlo, scegli Inventario sulla console.

The screenshot shows the AWS DMS console interface. On the left is a navigation sidebar with categories like Discover, Assess, Convert, and Migrate data. The main content area is titled 'Inventory' and includes a sub-header 'Databases (5)'. A search bar is present above a table listing discovered databases. The table has columns for Database ID, Server ID, Number of objects, and Engine type. One entry is visible: a database ID starting with [2a05:d018:d5b:4700:2ad6:e08f:dea0:5..., a server ID 2a05:d018:d5b:4700:2ad6:e08f:dea0:5..., 12 objects, and a Microsoft SQL Server engine.

DMS Fleet Advisor analizza gli schemi del database per determinare la somiglianza tra schemi diversi. Questa analisi non confronta il codice effettivo degli oggetti. DMS Fleet Advisor confronta solo i nomi degli oggetti dello schema, come funzioni e procedure, per identificare oggetti simili in diversi schemi di database.

Argomenti

- [Utilizzo di un inventario dei database per l'analisi](#)
- [Utilizzo di un inventario degli schemi per l'analisi](#)

Utilizzo di un inventario dei database per l'analisi

Per visualizzare l'elenco di tutti i database su tutti i server rilevati all'interno della rete da cui sono stati raccolti i dati, utilizza la procedura seguente.

Per visualizzare l'elenco dei database presenti sui server di rete da cui sono stati raccolti i dati

1. Scegli **Inventario** sulla console.

Viene visualizzata la pagina **Inventario**.

2. Scegli la scheda **Databases (Database)**.

Viene visualizzato l'elenco di database individuati.

Inventory Info

Database servers, schema information, and metadata discovered by data collectors. [Analyze inventories](#)

Analyze inventories
Running the analysis helps in identifying the candidates for migration. All the schemas are analyzed when you take this action, so ensure that the inventory is complete before you run the analysis. This operation can take a few minutes. [Learn more](#)

Databases | Schemas

Databases (7) [Refresh](#) [Export to CSV](#) [Delete](#)

Database inventories that were discovered by data collectors.

Find database inventory

<input type="checkbox"/>	Database	Server	Number of s...	Engine	Engine version	Engine ...
<input type="checkbox"/>	WinServ2016.d...	-	No data	PostgreSQL	-	-
<input type="checkbox"/>	VM-MSSQL14-...	10.11.1.10	44	Microsoft SQL ...	⚠ 2014 (Extended support)	Enterprise
<input type="checkbox"/>	MSSQL01.dbm...	-	No data	Microsoft SQL ...	✅ 2019 (Mainstream support)	Express

- Scegli Analizza gli inventari per determinare le proprietà dello schema, come la somiglianza e la complessità. Il tempo necessario per il processo dipende dal numero di oggetti da analizzare, ma non richiederà più di un'ora. I risultati dell'analisi sono disponibili nella scheda Schemi situata nella pagina Inventario.

DMS Fleet Advisor analizza gli schemi di tutti i database scoperti per definire l'intersezione dei loro oggetti. Il risultato dell'analisi è espresso in percentuale. DMS Fleet Advisor considera gli schemi con intersezioni superiori al 50% come duplicati. Lo schema originale viene identificato come lo schema in cui sono stati trovati i duplicati. Questo aiuta a identificare gli schemi originali da convertire o migrare per primi.

L'intero inventario viene analizzato per identificare schemi duplicati.

Utilizzo di un inventario degli schemi per l'analisi

È possibile visualizzare l'elenco di schemi di database rilevati sui server della rete da cui sono stati raccolti i dati. Esegui la seguente procedura.

Per visualizzare l'elenco degli schemi presenti sui server di rete da cui sono stati raccolti i dati

- Scegli Inventario sulla console. Viene visualizzata la pagina Inventario.

- Scegli la scheda Schemi. Viene visualizzato un elenco di schemi.
- Seleziona uno schema nell'elenco per visualizzarne le informazioni, tra cui server, database, dimensione e complessità.

Per ogni schema, è possibile visualizzare un riepilogo degli oggetti che fornisce informazioni sui tipi di oggetti, sul numero di oggetti, sulle dimensioni degli oggetti e sulle righe di codice.

- (Facoltativo) Scegli Analizza gli inventari per identificare gli schemi duplicati. DMS Fleet Advisor analizza gli schemi di database per definire l'intersezione dei relativi oggetti.
- Puoi esportare le informazioni sull'inventario in un file .csv per un'ulteriore revisione.

Schemas (13)
Schema inventories that were discovered by data collectors.

Find schema inventory

Schema	Server	Database	Engine	Complexity	Similarity...	Original schema
lsa_tests_src.lsa_tests_src	linuxsql02.db.local	linuxsql02.db.local:3306	MySQL Server	Simple	100	lsa_tests_src_100.lsa_tests_s...
lsa_tests_src_90e_30a.lsa_t...	linuxsql02.db.local	linuxsql02.db.local:3306	MySQL Server	Simple	90	lsa_tests_src_49.lsa_tests_sr...
lsa_tests_src_50.lsa_tests_s...	linuxsql02.db.local	linuxsql02.db.local:3306	MySQL Server	Simple	50	lsa_tests_src_100.lsa_tests_s...
lsa_tests_src_49.lsa_tests_s...	linuxsql02.db.local	linuxsql02.db.local:3306	MySQL Server	Simple	-	None

Per identificare gli schemi da migrare e determinare l'obiettivo della migrazione, puoi utilizzare AWS Schema Conversion Tool (AWS SCT) o DMS Schema Conversion. Per ulteriori informazioni, consulta [Using a new project wizard in AWS SCT](#).

Dopo aver identificato gli schemi da migrare, puoi convertirli utilizzando AWS SCT o la conversione dello schema DMS. Per ulteriori informazioni sulla configurazione dello schema DMS, consulta [Conversione degli schemi di database utilizzando la conversione dello schema DMS](#).

Utilizzo della funzionalità dei suggerimenti delle destinazioni di AWS DMS Fleet Advisor

Per esplorare e scegliere una destinazione di migrazione ottimale, puoi generare i suggerimenti delle destinazioni per i database on-premise di origine in DMS Fleet Advisor. Un suggerimento include uno o più possibili motori di destinazione AWS che puoi scegliere per la migrazione del database di origine on-premise. Tra questi possibili motori di destinazione, DMS Fleet Advisor suggerisce un singolo motore di destinazione come destinazione di migrazione della giusta dimensione e indica questo target come consigliato da DMS. Per determinare questa destinazione di migrazione con la dimensione corretta, DMS Fleet Advisor utilizza i metadati e le metriche di inventario raccolti dal raccogliitore di dati.

È possibile utilizzare i suggerimenti prima dell'inizio di una migrazione per individuare le opzioni di migrazione, risparmiare sui costi e ridurre i rischi. Puoi esportare i suggerimenti come file con valori separati da virgole (CSV) e condividerli con le principali parti interessate per facilitare il processo decisionale. È possibile esportare i consigli in formato per ottimizzare ulteriormente AWS Pricing Calculator i costi di manutenzione. Per ulteriori informazioni, consulta <https://calculator.aws/#/>.

Non è possibile modificare i suggerimenti delle destinazioni in DMS Fleet Advisor. Pertanto, non è possibile utilizzare DMS Fleet Advisor per l'analisi what-if. L'analisi what-if è il processo di modifica dei parametri di destinazione per vedere in che modo le modifiche influiscono sulla stima dei prezzi del suggerimento. È possibile eseguire un'analisi what-if nel AWS Pricing Calculator utilizzando i parametri di destinazione suggeriti come punto di partenza nel AWS Pricing Calculator. Per ulteriori informazioni, consulta <https://calculator.aws/#/>.

Ti consigliamo di considerare il suggerimento di DMS Fleet Advisor come un punto di partenza per la pianificazione della migrazione. Quindi puoi decidere di modificare i parametri dell'istanza suggeriti per ottimizzare i costi o le prestazioni dei carichi di lavoro del database.

Argomenti

- [Istanze di destinazione suggerite](#)
- [In che modo DMS Fleet Advisor determina le specifiche dell'istanza di destinazione per il suggerimento?](#)
- [Generazione di suggerimenti delle destinazioni con AWS DMS Fleet Advisor](#)
- [Esplorazione dei dettagli dei suggerimenti delle destinazioni con AWS DMS Fleet Advisor](#)
- [Esportazione dei suggerimenti delle destinazioni con AWS DMS Fleet Advisor](#)

- [Scoperta e analisi dei limiti della migrazione con Fleet Advisor AWS DMS](#)
- [Risoluzione dei problemi per i suggerimenti delle destinazioni](#)

Istanze di destinazione suggerite

Per i suggerimenti delle destinazioni, DMS Fleet Advisor prende in considerazione le seguenti istanze database Amazon RDS per uso generico, ottimizzate per la memoria e a prestazioni espandibili.

- db.m5
- db.m6i
- db.r5
- db.r6i
- db.t3
- db.x1
- db.x1e
- db.z1d

Per ulteriori informazioni sulle classi di istanza database Amazon RDS, consulta [Classi di istanze database](#) nella Guida per l'utente di Amazon RDS.

In che modo DMS Fleet Advisor determina le specifiche dell'istanza di destinazione per il suggerimento?

DMS Fleet Advisor può generare suggerimenti in base alla capacità o all'utilizzo del database.

- Se scegli di generare il suggerimento in base alla capacità del database, DMS Fleet Advisor mappa la capacità del database esistente in base alle specifiche della classe di istanze più vicina.
- Se scegli di generare il suggerimento in base all'utilizzo delle risorse, DMS Fleet Advisor determina il valore del 95° percentile per metriche quali CPU, memoria, velocità di trasmissione effettiva di I/O e IOPS. Il 95° percentile significa che il 95% dei dati raccolti è inferiore a questo valore. Quindi, DMS Fleet Advisor mappa questi valori alle specifiche della classe di istanza più vicina.

Per determinare la dimensione del database di destinazione, DMS Fleet Advisor raccoglie le informazioni sulla dimensione del database di origine. Quindi, DMS Fleet Advisor suggerisce di utilizzare le stesse dimensioni per l'archiviazione di destinazione. Se il provisioning dell'archiviazione

del database di origine è eccessivo, anche la dimensione suggerita dell'archiviazione di destinazione verrà sovradimensionata.

Se desideri migrare i dati utilizzando AWS DMS, potrebbe essere necessario aumentare il provisioning IOPS per l'istanza database di destinazione. Quando DMS Fleet Advisor genera i suggerimenti delle destinazioni, il servizio considera solo le metriche del database di origine. DMS Fleet Advisor non considera gli IOPS aggiuntivi necessari per eseguire le attività di migrazione dei dati. Per ulteriori informazioni, consulta [Attività di migrazione eseguite lentamente](#).

Per stimare i costi IOPS, DMS Fleet Advisor utilizza come riferimento di base una one-to-one mappatura dell'utilizzo degli IOPS di origine. DMS Fleet Advisor considera il carico di picco come valore di base e l'utilizzo al 100% per i prezzi di IOPS.

Per i database di origine PostgreSQL e MySQL, DMS Fleet Advisor può includere istanze database Aurora e Amazon RDS nei suggerimenti delle destinazioni. Se una configurazione Aurora corrisponde ai requisiti di origine, DMS Fleet Advisor contrassegna l'opzione come suggerita.

Generazione di suggerimenti delle destinazioni con AWS DMS Fleet Advisor

Dopo aver completato la raccolta dei dati e l'inventario di database e del parco istanze di analisi, puoi generare i suggerimenti delle destinazioni in DMS Fleet Advisor. A tale scopo, scegli i database di origine e configura le impostazioni utilizzate dalla funzionalità dei suggerimenti delle destinazioni di DMS Fleet Advisor per determinare la dimensione delle istanze di destinazione. Inoltre, la funzionalità dei suggerimenti delle destinazioni di DMS Fleet Advisor utilizza le metriche di capacità e utilizzo raccolte dai database di origine.

Per generare suggerimenti delle destinazioni

1. [Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/). [AWS DMS](#)

Verifica di aver selezionato la Regione AWS in cui desideri utilizzare DMS Fleet Advisor.

2. Nel riquadro di navigazione, scegli **Suggerimenti in Valutazione**, quindi seleziona **Genera suggerimenti**.
3. Nel pannello **Seleziona i database di origine**, seleziona le caselle di controllo relative ai nomi dei database che desideri migrare nel Cloud AWS.

Per **Cerca** nei database di origine inserisci il nome del database per filtrare l'inventario.

DMS Fleet Advisor può generare suggerimenti per un massimo di 100 database contemporaneamente.

4. Per Disponibilità e durata scegli l'opzione di implementazione preferita.

Per calcolare i suggerimenti delle destinazioni per i database di produzione, scegli Produzione (Multi-AZ). DMS Fleet Advisor include due istanze database in diverse zone di disponibilità nel suggerimento della destinazione. Questa opzione di implementazione multi-AZ offre alta disponibilità, ridondanza dei dati e supporto per il failover.

Se Aurora è il motore di destinazione consigliato e Availability and Durability è un'implementazione Multi-AZ, la raccomandazione di destinazione include un'istanza DB di lettura e scrittura.

Per calcolare i suggerimenti delle destinazioni per i database utilizzati per lo sviluppo o il test, scegli Sviluppo/test (AZ singola). DMS Fleet Advisor include una singola istanza database nel suggerimento della destinazione. Questa opzione di implementazione AZ singola riduce i costi di manutenzione.

5. Per Dimensionamento dell'istanza di destinazione scegli l'opzione preferita utilizzata da DMS Fleet Advisor per calcolare i consigli sugli obiettivi.

Per calcolare i suggerimenti delle destinazioni in base al database di origine o alla configurazione del server del sistema operativo, scegli Capacità totale. DMS Fleet Advisor utilizza le metriche come la capacità della CPU totale, della memoria e del disco dei database di origine o dei server del sistema operativo per generare i suggerimenti delle destinazioni. Quindi, DMS Fleet Advisor mappa le metriche di capacità del database alle specifiche della classe di istanze DB Amazon RDS più vicina.

Per calcolare i suggerimenti delle destinazioni in base all'utilizzo effettivo del database di origine o del server del sistema operativo, scegli Utilizzo delle risorse. DMS Fleet Advisor utilizza le metriche di utilizzo della capacità della CPU, della memoria e del disco dei database di origine o dei server del sistema operativo per generare i suggerimenti delle destinazioni. Con le metriche di utilizzo DMS Fleet Advisor calcola il 95° percentile per ogni metrica. Il 95° percentile significa che il 95% dei dati nel periodo è inferiore a questo valore. Quindi, DMS Fleet Advisor mappa questi valori alla classe di istanza database Amazon RDS più vicina.

Ti consigliamo di utilizzare l'opzione Utilizzo delle risorse per ottenere suggerimenti più accurati. Per farlo, verifica di aver raccolto le metriche di capacità totale e utilizzo delle risorse.

6. Scegliere Generate (Genera).

DMS Fleet Advisor genera i suggerimenti delle destinazioni per i database selezionati. Per generare correttamente i suggerimenti, DMS Fleet Advisor imposta lo stato su Calcolato. Inoltre, DMS Fleet Advisor utilizza AWS Pricing Calculator per determinare il costo mensile stimato dell'istanza database di destinazione suggerita. A questo punto puoi esplorare in dettaglio i suggerimenti generati. Per ulteriori informazioni, consulta [Dettagli dei suggerimenti](#).

Per stimare il costo mensile totale dell'inventario dei dati, seleziona le caselle di controllo relative ai database che intendi trasferire nel cloud. DMS Fleet Advisor visualizza il costo mensile totale stimato e il riepilogo dei database di destinazione nel Cloud AWS. DMS Fleet Advisor utilizza l'API di query Listino prezzi AWS per fornire dettagli dei prezzi a solo scopo informativo. Le tariffe effettive dipendono da una varietà di fattori, tra cui l'utilizzo reale dei Servizi AWS. Per ulteriori informazioni sui prezzi del Servizio AWS, consulta [Prezzi dei servizi cloud](#).

Esplorazione dei dettagli dei suggerimenti delle destinazioni con AWS DMS Fleet Advisor

Una volta che DMS Fleet Advisor ha generato i suggerimenti delle destinazioni puoi visualizzare i parametri chiave della destinazione di migrazione consigliata nella tabella Suggerimenti. Questi parametri chiave includono il motore di destinazione, la classe di istanza, il numero di CPU virtuali, la memoria, l'archiviazione e il tipo di archiviazione. Oltre a questi parametri, DMS Fleet Advisor mostra il costo mensile stimato della destinazione di migrazione suggerita.

Ogni suggerimento può includere uno o più possibili motori di destinazione AWS. Se il suggerimento include diversi motori di destinazione, AWS DMS contrassegna uno di essi come consigliato. Inoltre, AWS DMS visualizza i parametri e il costo mensile stimato per questa opzione consigliata nella tabella Suggerimenti.

Per confrontare i suggerimenti delle destinazioni con l'utilizzo e la capacità del database di origine, consulta i suggerimenti in dettaglio. Inoltre, puoi visualizzare le limitazioni di migrazione per un suggerimento selezionato. Queste limitazioni includono funzionalità di database non supportate, azioni e altre considerazioni sulla migrazione.

Per esaminare il suggerimento in dettaglio

1. Genera i suggerimenti delle destinazioni con DMS Fleet Advisor. Per ulteriori informazioni, consulta [Generazione di suggerimenti delle destinazioni](#).

2. Scegli il nome del suggerimento nella tabella Suggerimenti. Si apre la pagina del suggerimento.
3. Se il suggerimento include più di un'opzione di destinazione, scegli l'opzione desiderata per Suggerimenti sulla destinazione.
4. Espandi la sezione Utilizzo e capacità dell'origine. DMS Fleet Advisor visualizza i grafici di utilizzo delle risorse per le seguenti metriche.
 - Numero di CPU
 - Memoria
 - Velocità di trasmissione effettiva di I/O
 - Operazioni di input/output al secondo (IOPS).
 - Storage
 - Numero di connessioni attive al server di database

Utilizza questi grafici per confrontare le metriche del database di origine acquisite dal raccoglitore di dati DMS con le metriche del motore di destinazione selezionato.

Se non riesci a visualizzare i grafici dopo aver ampliato la sezione Utilizzo e capacità del codice sorgente, assicurati di aver concesso al tuo utente IAM le autorizzazioni per visualizzare le dashboard di Amazon CloudWatch . Per ulteriori informazioni, consulta [Using Amazon CloudWatch dashboard](#) nella Amazon CloudWatch User Guide.

5. Scegli il collegamento con il nome del motore di destinazione selezionato. Viene visualizzata la pagina Dettagli della destinazione.
6. Per esportare i consigli target in formato CSV, scegli l'opzione Esporta in CSV dal menu a discesa Azioni.
7. Per esportare i consigli sugli obiettivi in AWS Pricing Calculator, scegli Ottimizza i costi con AWS Pricing Calculator l'opzione dal menu a discesa Azioni.
8. Nella sezione Configurazione, confronta i valori dei parametri del database di origine con i parametri del motore di destinazione. Per il motore di destinazione, DMS Fleet Advisor mostra i costi mensili stimati per le risorse cloud. DMS Fleet Advisor utilizza l'API di query Listino prezzi AWS per fornire dettagli dei prezzi a solo scopo informativo. Le tariffe effettive dipendono da una varietà di fattori, tra cui l'utilizzo reale dei Servizi AWS. Per ulteriori informazioni sui prezzi del Servizio AWS, consulta Prezzi dei servizi cloud all'indirizzo <https://aws.amazon.com/pricing/>.

9. Nella sezione Limitazioni alla migrazione visualizza le limitazioni della migrazione. Ti consigliamo di prendere in considerazione queste limitazioni quando esegui la migrazione del database di origine al Cloud AWS.

Esportazione dei suggerimenti delle destinazioni con AWS DMS Fleet Advisor

Dopo aver generato i suggerimenti delle destinazioni, puoi salvare una copia dell'elenco dei suggerimenti come file CSV (Comma-Separated Value).

Per generare suggerimenti delle destinazioni

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

Verifica di aver selezionato la Regione AWS in cui desideri utilizzare DMS Fleet Advisor.

2. Nel riquadro di navigazione scegli Suggerimenti in Valuta, quindi seleziona i suggerimenti da includere nel file CSV.
3. Scegli Esporta in CSV, inserisci il nome del file e scegli la cartella sul PC in cui vuoi salvare il file.
4. Apri il file CSV.

Il file CSV con i suggerimenti contiene le seguenti informazioni.

- **CreatedDate**— La data in cui DMS Fleet Advisor ha creato la raccomandazione per il motore di destinazione.
- **Databaseld**— L'identificatore del database di origine per il quale DMS Fleet Advisor ha creato questa raccomandazione.
- **DeploymentOption**— L'opzione di distribuzione per l'istanza database Amazon RDS consigliata.
- **EngineEdition**— L'edizione del motore Amazon RDS di destinazione consigliata.
- **EngineName**— Il nome del motore di destinazione.
- **InstanceMemory**— La quantità di memoria sull'istanza database di Amazon RDS consigliata.
- **InstanceSizingType**— La dimensione dell'istanza di destinazione.
- **InstanceType**— Il tipo di istanza Amazon RDS di destinazione consigliato.
- **InstanceVcpu**— Il numero di CPU virtuali sull'istanza database Amazon RDS consigliata.

- **Preferita:** un flag booleano che indica che questa opzione di destinazione è suggerita.
- **Stato:** lo stato del suggerimento del motore di destinazione.
- **StorageIops**— Il numero di operazioni di I/O completate ogni secondo (IOPS) sull'istanza database Amazon RDS consigliata.
- **StorageSize**— La dimensione di storage dell'istanza database Amazon RDS consigliata.
- **StorageType**— Il tipo di storage dell'istanza database Amazon RDS consigliata.
- **WorkloadType**— L'opzione di implementazione per il motore di destinazione, ad esempio l'implementazione Multi-AZ o Single-AZ.

Scoperta e analisi dei limiti della migrazione con Fleet Advisor AWS DMS

Puoi utilizzare il raccoglitore di dati DMS per scoprire le funzionalità del database che il motore di destinazione non supporta. Per scegliere la giusta destinazione di migrazione, è necessario considerare queste limitazioni.

Il raccoglitore di dati DMS rileva funzionalità specifiche del database di origine. Quindi, DMS Fleet Advisor analizza le funzionalità di origine dal punto di vista della migrazione verso la destinazione specificata e fornisce informazioni aggiuntive sulla limitazione e include le azioni consigliate per risolvere o evitare questa limitazione. Inoltre, DMS Fleet Advisor calcola l'impatto di queste limitazioni.

L'elenco delle limitazioni è disponibile nella pagina dei dettagli del motore di Target. Passa a questa pagina dalla pagina Consigli nel menu di navigazione a sinistra. Dall'elenco degli obiettivi, scegli il motore di destinazione da esaminare. L'elenco delle limitazioni si trova in fondo alla pagina.

La tabella seguente include le funzionalità del database MySQL non supportate da Amazon RDS per MySQL.

Limitazione	Descrizione	Impatto
Plug-in di autenticazione	Amazon RDS non supporta i plug-in di autenticazione MySQL.	Bassa
Registrazione degli errori nel log di sistema	Amazon RDS non supporta la scrittura del log degli errori nel log di sistema.	Bassa

Limitazione	Descrizione	Impatto
Identificatori globali di transazione	È possibile utilizzare gli identificatori globali di transazione con tutte le versioni di RDS per MySQL 5.7 e RDS per MySQL 8.0.26 e versioni successive a MySQL 8.0.	Bassa
Replica di gruppi	Amazon RDS non supporta il plug-in per la replica dei gruppi MySQL.	Bassa
Crittografia di spazi tabelle InnoDB	Amazon RDS non supporta la crittografia degli spazi tabelle InnoDB.	Bassa
Parola riservata InnoDB	InnoDB è una parola riservata per Amazon RDS per MySQL. Non è possibile utilizzare questo nome per un database MySQL.	Bassa
Plug-in keyring	Amazon RDS non supporta il plug-in keyring MySQL.	Bassa
Plugin convalida password	Amazon RDS non supporta il plug-in <code>validate_password</code> MySQL.	Bassa
Variabili di sistema persistenti	Amazon RDS non supporta le variabili di sistema persistenti MySQL.	Bassa

Limitazione	Descrizione	Impatto
Accesso limitato	Amazon RDS limita l'accesso ad alcune procedure di sistema e tabelle che richiedono privilegi avanzati. Inoltre, Amazon RDS non consente l'accesso host diretto a un'istanza database tramite Telnet, Secure Shell (SSH) o Windows Remote Desktop Connection.	Bassa
Plug-in di riscrittura delle query Rewriter	Amazon RDS non supporta il plug-in di riscrittura delle query MySQL Rewriter.	Bassa
Replica semi-sincrona	Amazon RDS non supporta la replica semisincrona MySQL.	Bassa
Spazi di tabelle trasportabili	Amazon RDS non supporta la funzionalità degli spazi di tabelle trasportabili MySQL.	Bassa
Plug-in IDE	Amazon RDS non supporta il plug-in X MySQL.	Bassa

La tabella seguente include le funzionalità del database Oracle non supportate da Amazon RDS per Oracle.

Limitazione	Descrizione	Impatto
Active Data Guard	Non puoi utilizzare Active Data Guard con i database container (CDB) multitenant Oracle.	Media

Limitazione	Descrizione	Impatto
Automatic Storage Management	Amazon RDS non supporta Oracle Automatic Storage Management (Oracle ASM).	Media
Flussi di attività di database	Amazon RDS non supporta Oracle Database Activity Streams per l'architettura a tenant singolo.	Elevata
Limite della dimensione dei file	La dimensione massima di un file nelle istanze database RDS per Oracle è pari a 16 TiB.	Media
FTP e SFTP	Amazon RDS non supporta FTP e SFTP.	Media
Tabelle partizionate ibride	Amazon RDS non supporta le tabelle partizionate ibride Oracle.	Elevata
Oracle Data Guard	Amazon RDS non utilizza Oracle Data Guard per l'architettura a tenant singolo.	Elevata
Oracle Database Vault	Amazon RDS non supporta Oracle Database Vault.	Elevata
Vault dei privilegi Oracle DBA	Amazon RDS prevede limitazioni per i privilegi Oracle DBA. Per ulteriori informazioni, consulta Limitazioni per i privilegi Oracle DBA .	Elevata

Limitazione	Descrizione	Impatto
Oracle Enterprise Manager	Amazon RDS non supporta Oracle Enterprise Manager per l'architettura a tenant singolo.	Elevata
Agent Oracle Enterprise Manager	Amazon RDS non utilizza Oracle Enterprise Manager Agent per l'architettura a tenant singolo.	Media
Oracle Enterprise Manager Cloud Control Management Repository	Non puoi utilizzare un'istanza a database Amazon RDS per Oracle per Oracle Enterprise Manager Cloud Control Management Repository.	Elevata
Database Oracle Flashback	Amazon RDS non supporta la funzionalità del database Oracle Flashback.	Elevata
Oracle Label Security	Amazon RDS non supporta Oracle Label Security per l'architettura a tenant singolo. Puoi utilizzare Oracle Label Security solo con database container (Oracle CDB) multitenant.	Elevata
Oracle Messaging Gateway	Amazon RDS non supporta Oracle Messaging Gateway.	Elevata
Oracle Real Application Clusters	Amazon RDS non supporta Oracle Real Application Clusters (Oracle RAC).	Elevata

Limitazione	Descrizione	Impatto
Oracle Real Application Testing	Amazon RDS non supporta Oracle Real Application Testing.	Elevata
Database Oracle Snapshot Standby	Amazon RDS non supporta i database Oracle Snapshot Standby.	Elevata
Sinonimi pubblici	Amazon RDS non supporta sinonimi pubblici per gli schemi forniti da Oracle.	Media
Schemi per funzionalità non supportate	Amazon RDS non supporta gli schemi per funzionalità e componenti Oracle che richiedono privilegi di sistema.	Elevata
Audit unificato puro	Amazon RDS non supporta l'audit unificato puro. Puoi utilizzare l'audit unificato in modalità mista.	Media
Workspace Manager	Amazon RDS non supporta lo schema WMSYS di Oracle Database Workspace Manager.	Elevata

La tabella seguente include le funzionalità del database PostgreSQL non supportate da Amazon RDS per PostgreSQL.

Limitazione	Descrizione	Impatto
Connessioni simultanee	Il numero massimo di connessioni simultanee e all'istanza di RDS per	Bassa

Limitazione	Descrizione	Impatto
	PostgreSQL è limitato dal parametro <code>max_connections</code> .	
Versioni più recenti	Amazon RDS non applica aggiornamenti automatici alla versione principale. Per eseguire un aggiornamento della versione principale, modifica l'istanza database manualmente. Per ulteriori informazioni, consulta Scelta di un aggiornamento di versione principale per PostgreSQL .	Bassa
Connessioni riservate	Amazon RDS riserva fino a 3 connessioni per la manutenzione del sistema. Quando specifichi un valore per il parametro delle connessioni utente, oltre a quelle che pensi di utilizzare, aggiungi altre 3 connessioni.	Bassa

Limitazione	Descrizione	Impatto
Estensioni supportate	RDS per PostgreSQL supporta un numero limitato di estensioni per il motore di database PostgreSQL. L'elenco delle estensioni supportate è disponibile nel gruppo di parametri del database predefinito per la versione di PostgreSQL. Puoi inoltre vedere l'elenco delle estensioni correnti che utilizzano <code>psql</code> mostrando il parametro <code>rds.extensions</code> .	Bassa
Suddivisione o isolamento dello spazio di tabella	Non è possibile utilizzare gli spazi di tabelle per la suddivisione o l'isolamento di I/O. In RDS per PostgreSQL, tutto lo spazio di archiviazione si trova su un singolo volume logico.	Bassa

La tabella seguente include le funzionalità di database SQL Server non supportate da Amazon RDS per SQL Server.

Limitazione	Descrizione	Impatto
Backup su Archiviazione BLOB di Microsoft Azure	RDS per SQL Server non supporta il backup su Microsoft Azure Blob Storage.	Media
Estensione del pool di buffer	RDS per SQL Server non supporta l'estensione del pool di buffer.	Elevata

Limitazione	Descrizione	Impatto
Policy di password personalizzate	RDS per SQL Server non supporta le policy di password personalizzate.	Media
Servizi di Qualità dei Dati	RDS per SQL Server non supporta SQL Server Data Quality Services (DQS).	Elevata
Log di database	RDS per SQL Server non supporta il log del database.	Elevata
Nomi dei database	I nomi dei database presentano o le seguenti limitazioni: non possono iniziare con rdsadmin, non possono iniziare o terminare con uno spazio o una scheda, non possono contenere un carattere che crea una nuova riga, non possono contenere virgolette singole (').	Media
Snapshot del database	RDS per SQL Server non supporta gli snapshot di database. È possibile utilizzare solo snapshot di istanze database in Amazon RDS.	Media
Stored procedure estese	RDS per SQL Server non supporta le stored procedure estese, tra cui xp_cmdshe11 .	Elevata
Tabelle di file	RDS per SQL Server non supporta le tabelle di file.	Media

Limitazione	Descrizione	Impatto
Supporto FILESTREAM	RDS per SQL Server non fornisce il supporto FILESTREAM.	Media
Server collegati	RDS per SQL Server offre un supporto limitato per i server collegati.	Elevata
Machine Learning ed R Services	RDS per SQL Server non supporta Machine Learning ed R Services perché è necessario l'accesso al sistema operativo per installare e questi servizi.	Elevata
Piani di manutenzione	RDS per SQL Server non supporta i piani di manutenzione.	Elevata
Prestazioni della raccolta dati	RDS per SQL Server non supporta il raccogliitore di dati delle prestazioni.	Elevata
Gestione basata sulla Policy	RDS per SQL Server non supporta la gestione basata sulla policy.	Media
PolyBase	RDS per SQL Server non supporta PolyBase.	Elevata
Replica	RDS per SQL Server non supporta la replica.	Media
Direttore delle risorse	RDS per SQL Server non supporta Resource Governor.	Elevata

Limitazione	Descrizione	Impatto
Trigger a livello di server	RDS per SQL Server non supporta i trigger a livello server.	Media
Endpoint del broker del servizio	RDS per SQL Server non supporta gli endpoint del broker del servizio.	Elevata
SSAS	Considera le limitazioni che si applicano all'esecuzione di SQL Server Analysis Services (SSAS) su RDS per SQL Server. Per ulteriori informazioni, consulta Limitazioni .	Bassa
SSIS	Considera le limitazioni che si applicano all'esecuzione di SQL Server Integration Services (SSIS) su RDS per SQL Server. Per ulteriori informazioni, consulta Limitazioni .	Bassa
SSRS	Considera le limitazioni che si applicano all'esecuzione di SQL Server Reporting Services (SSRS) su RDS per SQL Server. Per ulteriori informazioni, consulta Limitazioni .	Bassa

Limitazione	Descrizione	Impatto
Dimensione di archiviazione per le istanze database SQL Server	<p>La dimensione massima di archiviazione per SQL Server General Purpose (SSD) e le istanze di archiviazione con capacità di IOPS allocata è di 16 TiB.</p> <p>La dimensione massima di archiviazione per le istanze di archiviazione SQL Server Magnetic è 1 TiB.</p>	Elevata
Stretch Database	RDS per SQL Server non supporta la funzionalità SQL Server Stretch Database.	Media
Endpoint T-SQL	RDS per SQL Server non supporta tutte le operazioni che utilizzano CREATE ENDPOINT.	Elevata
Proprietà di database TRUSTWORTHY	RDS per SQL Server non supporta la proprietà di database TRUSTWORTHY perché richiede il ruolo sysadmin.	Media

La tabella seguente include un elenco di problemi relativi alle raccomandazioni. DMS Fleet Advisor analizza le funzionalità del database di origine e di destinazione e fornisce queste limitazioni di migrazione. La limitazione con Blocker Impact significa che DMS Fleet Advisor non è in grado di generare raccomandazioni sugli obiettivi per il database di origine.

Limitazione	Descrizione	Impatto
L'istanza appropriata non è stata trovata	AWS DMS non riesco a trovare un'istanza di destinazione che possa funzionare come destinazione di migrazione e delle dimensioni corrette per una combinazione delle metriche del database di origine.	Blocker
L'istanza appropriata non è stata trovata da IOPS	Il database di origine utilizza un numero di IOPS, che supera il numero massimo di IOPS per le possibili istanze DB di destinazione.	Bloccante
L'istanza appropriata non viene trovata dalla RAM	Il database di origine utilizza un numero di GB di RAM, che supera la dimensione e massima della RAM per le possibili istanze DB di destinazione.	Blocker
L'istanza appropriata non viene trovata in base alla dimensione di archiviazione	Il database di origine utilizza un certo numero di TB di spazio di archiviazione, che supera la dimensione massima di archiviazione per le possibili istanze DB di destinazione.	Blocker
L'istanza appropriata non è stata trovata dall'edizione	Il database di origine ha un'edizione che non è supportata da Amazon RDS.	Blocker

Limitazione	Descrizione	Impatto
L'istanza appropriata non viene trovata dai core della CPU	Il database di origine ha un numero di core CPU, che supera il numero massimo di core CPU per le possibili istanze DB di destinazione.	Bloccante
L'istanza appropriata non è stata trovata per versione	La versione del database di origine AWS DMS non viene riconosciuta.	Blocker
Il parametro della CPU non è definito	Il raccogliatore di dati DMS non ha raccolto informazioni sulla CPU utilizzata dal database di origine. Assicurati di aver raccolto le metriche richieste e configurato le credenziali per l'inoltro dei dati nel tuo raccogliatore di dati. Per informazioni, consulta Configurazione delle credenziali per l'inoltro dei dati .	Blocker
Il parametro di memoria non è definito	Il raccogliatore di dati DMS non ha raccolto informazioni sulla memoria utilizzata dal database di origine. Assicurati di aver raccolto le metriche richieste e configurato le credenziali per l'inoltro dei dati nel tuo raccogliatore di dati. Per informazioni, consulta Configurazione delle credenziali per l'inoltro dei dati .	Blocker

Limitazione	Descrizione	Impatto
Il parametro della dimensione di archiviazione non è definito	Il raccogliitore di dati DMS non ha raccolto informazioni sulla dimensione di archiviazione utilizzata dal database di origine. Assicurati di aver raccolto le metriche richieste e configurato le credenziali per l'inoltro dei dati nel tuo raccogliitore di dati. Per informazioni, consulta Configurazione delle credenziali per l'inoltro dei dati .	Blocker
Il parametro Storage IOPS non è definito	Il raccogliitore di dati DMS non ha raccolto i parametri IOPS di storage per gli usi del database di origine. Assicurati di aver raccolto le metriche richieste e configurato le credenziali per l'inoltro dei dati nel tuo raccogliitore di dati.	Blocker
Dati insufficienti	Il raccogliitore di dati DMS non ha raccolto dati sufficienti per generare una raccomandazione mirata. Assicurati di aver configurato le credenziali per l'inoltro dei dati nel tuo raccogliitore di dati. Per informazioni, consulta Configurazione delle credenziali per l'inoltro dei dati .	Blocco

Limitazione	Descrizione	Impatto
L'edizione del database non è definita	Il raccogliatore di dati DMS non ha raccolto informazioni sull'edizione del database di origine. Assicurati di aver raccolto le metriche richieste e configurato le credenziali per l'inoltro dei dati nel tuo raccogliatore di dati. Per informazioni, consulta Configurazione delle credenziali per l'inoltro dei dati .	Blocker
Errore sconosciuto	DMS Fleet Advisor non è in grado di generare raccomandazioni sugli obiettivi per il database di origine.	Bloccante
La versione del database non è definita	DMS Fleet Advisor non ha raccolto informazioni sulla versione del database di origine. DMS Fleet Advisor consiglia di utilizzare la versione più recente del database per il database di origine. Se scegli questo consiglio, devi aggiornare la versione del database. Esamina i consigli sugli obiettivi generati per il tuo database di origine e assicurati che soddisfino i tuoi requisiti.	Elevata

Limitazione	Descrizione	Impatto
Aumenta il numero di connessioni al database nelle impostazioni RDS	Il database di origine richiede un certo numero di connessioni. Per impostazione predefinita, il numero di connessioni disponibili per le istanze di database Amazon RDS è diverso. Assicurati di modificare e questo valore predefinito quando crei l'istanza del database RDS. A tale scopo, aggiorna il valore del <code>max_connections</code> parametro in Parameter Groups.	Media
L'edizione Target è compatibile	La raccomandazione di destinazione per il database di origine utilizza un'edizione del database diversa. L'edizione e del database di origine supporta le stesse funzionalità dell'edizione di destinazione consigliata. Tuttavia, la scelta di questa nuova edizione del database potrebbe aumentare le spese.	Media

Limitazione	Descrizione	Impatto
Il parametro del throughput di archiviazione non è definito	Il raccogliatore di dati DMS non ha raccolto le metriche del throughput di storage per gli usi del database di origine. Esamina i consigli sugli obiettivi generati per il tuo database di origine e assicurati che soddisfino i tuoi requisiti.	Media
Il parametro del numero di connessione al database non è definito	Il raccogliatore di dati DMS non ha raccolto informazioni sul numero di connessioni utilizzate dal database di origine. Esamina i consigli sugli obiettivi generati per il tuo database di origine e assicurati che soddisfino i tuoi requisiti. In alternativa, richiedi un aumento della quota.	Media
Versione di downgrade del database	Il database di origine viene eseguito su una versione superiore rispetto al database Amazon RDS. Per effettuare il downgrade della versione del database, assicurati di non utilizzare le funzionalità che non sono implementate nella versione precedente. In alternativa, usa Amazon EC2 come obiettivo di migrazione.	Media

Limitazione	Descrizione	Impatto
L'edizione Target è diversa	<p>La raccomandazione di destinazione per il database di origine utilizza un'edizione del database diversa. L'edizione del database di origine è compatibile con l'edizione di destinazione consigliata. Tuttavia, l'edizione del database di destinazione consigliata non supporta alcune funzionalità dell'edizione del database di origine. La scelta di questa nuova edizione del database potrebbe aumentare le spese.</p>	Media

Limitazione	Descrizione	Impatto
Esegui l'aggiornamento da una versione non supportata	<p>Il database di origine ha raggiunto la fine della fase di supporto. Per utilizzare la versione più recente del motore DB come destinazione, aggiorna il database prima della migrazione. In alternativa, usa Amazon EC2 come obiettivo di migrazione.</p> <p>A seconda del motore di database, utilizza uno dei seguenti link per saperne di più:</p> <p>Aggiornamento di MySQL</p> <p>Aggiornamento di SQL Server</p> <p>Aggiornamento di OracleDB</p> <p>Aggiorna PostgreSQL</p>	Media

Risoluzione dei problemi per i suggerimenti delle destinazioni

Nell'elenco seguente sono disponibili le azioni da intraprendere in caso di problemi con la funzionalità Suggerimenti sulla destinazione di DMS Fleet Advisor.

Argomenti

- [Non riesco a visualizzare le stime dei prezzi per i suggerimenti delle destinazioni](#)
- [Non riesco a visualizzare i grafici di utilizzo delle risorse](#)
- [Non riesco a vedere lo stato della raccolta delle metriche](#)

Non riesco a visualizzare le stime dei prezzi per i suggerimenti delle destinazioni

Se vedi la voce Nessun dato per Costo mensile stimato per un suggerimento con lo stato Esito positivo, assicurati di aver fornito all'utente IAM le autorizzazioni per accedere all'API del servizio Listino prezzi AWS. A tal fine, dovrai creare la policy che include l'autorizzazione `pricing:GetProducts` e aggiungerla all'utente IAM come descritto in [Creazione di risorse IAM](#).

DMS Fleet Advisor non calcola il costo mensile stimato per i suggerimento con lo stato Non riuscito.

Non riesco a visualizzare i grafici di utilizzo delle risorse

Se vedi il messaggio Failed to load metrics dopo aver espanso la sezione Utilizzo e capacità del codice sorgente, assicurati di aver concesso al tuo utente IAM le autorizzazioni per visualizzare le dashboard di Amazon CloudWatch. A questo scopo, dovrai aggiungere la policy richiesta all'utente IAM come descritto in [Creazione di risorse IAM](#).

In alternativa, puoi creare una policy personalizzata che includa le autorizzazioni `cloudwatch:GetDashboard`, `cloudwatch:ListDashboards`, `cloudwatch:PutDashboard` e `cloudwatch:DeleteDashboards`. Per ulteriori informazioni, consulta [Using Amazon CloudWatch dashboard](#) nella Amazon CloudWatch User Guide.

Non riesco a vedere lo stato della raccolta delle metriche

Se vedi Nessun dato disponibile per Raccolta di parametri quando scegli Genera suggerimenti, assicurati di aver raccolto i dati. Per ulteriori informazioni, consulta [Raccolta di dati per AWS DMS Fleet Advisor](#).

Se riscontri questo problema dopo aver raccolto i dati, assicurati di aver concesso al tuo utente IAM l'`cloudwatch:Get*` autorizzazione ad accedere ad Amazon CloudWatch. DMS Fleet Advisor utilizza un ruolo collegato al servizio per pubblicare le metriche delle prestazioni del database raccolte per CloudWatch tuo conto. Assicurati di creare un ruolo collegato al servizio da utilizzare con DMS Fleet Advisor. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).

Limitazioni di DMS Fleet Advisor

Le limitazioni all'utilizzo di DMS Fleet Advisor includono quanto segue:

- DMS Fleet Advisor genera raccomandazioni one-to-one . Per ogni database di origine, DMS Fleet Advisor determina un singolo motore di destinazione. DMS Fleet Advisor non gestisce server multi-

tenant e non fornisce suggerimenti per l'esecuzione di diversi database su una singola istanza database di destinazione.

- DMS Fleet Advisor non fornisce suggerimenti sugli aggiornamenti delle versioni disponibili del database.
- DMS Fleet Advisor genera suggerimenti per un massimo di 100 database contemporaneamente.
- Se installi DMS data collector, che è un'applicazione Windows, assicurati di installare anche .NET Framework 4.8 e 6.0 e PowerShell versioni successive. Per i requisiti hardware, consulta [Installazione di un raccoglitore di dati](#).
- Il raccoglitore di dati DMS richiede le autorizzazioni per eseguire le richieste utilizzando il protocollo LDAP sul server di dominio.
- Il raccoglitore di dati DMS richiede lo script sudo SSH in esecuzione in Linux.
- Il raccoglitore di dati DMS richiede le autorizzazioni per eseguire script remoti PowerShell, Windows Management Instrumentation (WMI), WMI Query Language (WQL) e script di registro in Windows.
- Per MySQL e PostgreSQL, DMS Fleet Advisor non è in grado di raccogliere le metriche delle prestazioni del database. DMS Fleet Advisor può invece raccogliere le metriche del server del sistema operativo. Pertanto, non è possibile generare suggerimenti basati sulle metriche di utilizzo per i database MySQL e PostgreSQL eseguiti su Amazon RDS e Aurora.

Conversione degli schemi di database utilizzando la conversione dello schema DMS

La conversione dello schema DMS in AWS Database Migration Service (AWS DMS) rende più prevedibili le migrazioni di database tra diversi tipi di database. Puoi utilizzare la conversione dello schema DMS per valutare la complessità della migrazione per il fornitore di dati di origine e per convertire schemi di database e oggetti di codice. Puoi quindi applicare il codice convertito al database di destinazione.

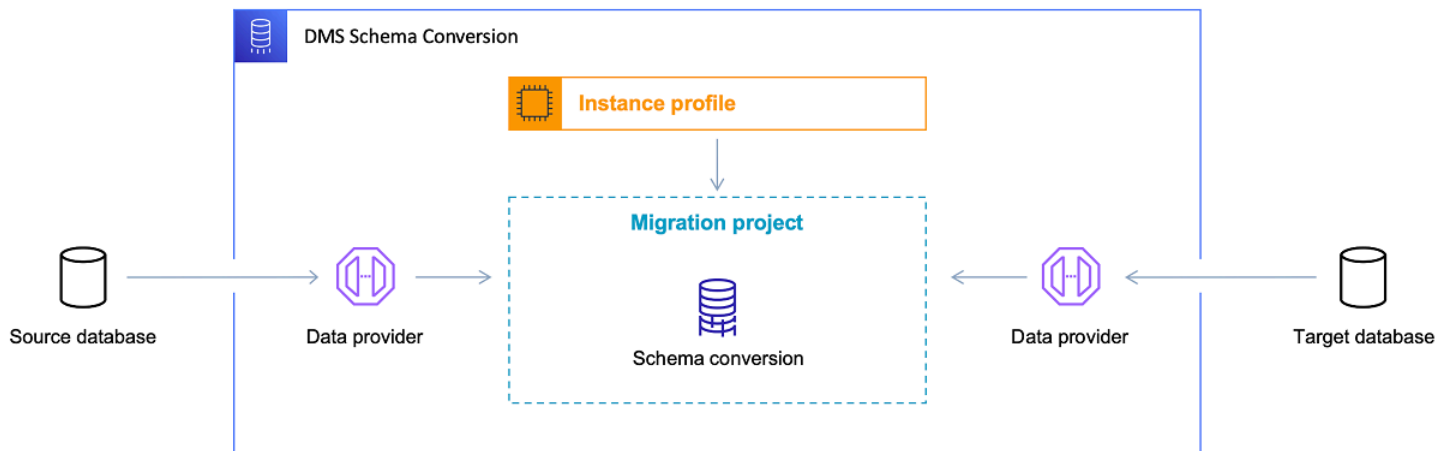
La conversione dello schema DMS converte automaticamente gli schemi del database di origine e la maggior parte degli oggetti di codice del database in un formato compatibile con il database di destinazione. Questa conversione include tabelle, viste, stored procedure, funzioni, tipi di dati, sinonimi e così via. Tutti gli oggetti che la conversione dello schema DMS non è in grado di convertire automaticamente sono contrassegnati in modo chiaro. Per completare la migrazione, puoi convertire questi oggetti manualmente.

Ad alto livello, [la conversione dello schema DMS](#) funziona con i seguenti tre componenti: profili dell'istanza, fornitore di dati e progetti di migrazione. Un profilo dell'istanza specifica le impostazioni di rete e di sicurezza. Un fornitore di dati archivia le credenziali di connessione al database. Un progetto di migrazione contiene fornitori di dati, un profilo di istanza e regole di migrazione. AWS DMS utilizza fornitori di dati e un profilo di istanza per progettare un processo che converte gli schemi di database e gli oggetti di codice.

Per l'elenco dei database di origine supportati, consulta [Origini per la conversione dello schema DMS](#).

Per l'elenco dei database di destinazione supportati, consulta [Destinazioni per la conversione dello schema DMS](#).

Il seguente diagramma illustra il processo di conversione dello schema DMS.



Consulta i seguenti argomenti per comprendere meglio come si usa la conversione dello schema DMS.

Argomenti

- [Supportato Regioni AWS](#)
- [Funzionalità di conversione dello schema](#)
- [Limitazioni della conversione dello schema](#)
- [Nozioni di base sulla conversione dello schema DMS](#)
- [Configurazione di una rete per la conversione dello schema DMS](#)
- [Creazione di fornitori di dati di origine per la conversione dello schema DMS](#)
- [Creazione di fornitori di dati di destinazione per la conversione dello schema DMS](#)
- [Gestione dei progetti di migrazione nella conversione dello schema DMS](#)
- [Creazione di report di valutazione della migrazione del database con la conversione dello schema DMS](#)
- [Utilizzo della conversione dello schema DMS](#)
- [Utilizzo dei pacchetti di estensione nella conversione dello schema DMS](#)

Supportato Regioni AWS

È possibile creare un progetto di migrazione DMS Schema Conversion nel modo seguente. Regioni AWS In altre regioni, è possibile utilizzare AWS Schema Conversion Tool. Per ulteriori informazioni AWS SCT, vedere la [AWS Schema Conversion Tool User Guide](#).

Nome della regione	Regione
US East (N. Virginia)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
US West (Oregon)	us-west-2
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Europe (Frankfurt)	eu-central-1
Europa (Stoccolma)	eu-north-1
Europa (Irlanda)	eu-west-1

Funzionalità di conversione dello schema

La conversione dello schema DMS offre le seguenti funzionalità:

- DMS Schema Conversion gestisce automaticamente le Cloud AWS risorse necessarie per il progetto di migrazione del database. Queste risorse includono profili di istanza, fornitori di dati e AWS Secrets Manager segreti. Includono anche ruoli AWS Identity and Access Management (IAM), bucket Amazon S3 e progetti di migrazione.
- Puoi utilizzare la conversione dello schema DMS per connetterti al database di origine, leggere i metadati e creare report di valutazione della migrazione del database. Quindi, puoi salvare il report in un bucket Amazon S3. Con questi report avrai un riepilogo delle attività di conversione dello schema e i dettagli sugli elementi che non possono essere convertiti automaticamente dalla conversione dello schema DMS nel database di destinazione. I report di valutazione della migrazione del database aiutano a valutare la parte del progetto di migrazione che la conversione dello schema DMS è in grado di automatizzare. Inoltre, questi report aiutano a stimare l'impegno manuale necessario per completare la conversione. Per ulteriori informazioni, consulta [Creazione di report di valutazione della migrazione del database con la conversione dello schema DMS](#).

- Dopo la connessione ai fornitori di dati di origine e di destinazione, la conversione dello schema DMS è in grado di convertire gli schemi del database di origine esistenti nel motore di database di destinazione. Puoi scegliere qualsiasi elemento dello schema dal database di origine da convertire. Dopo aver convertito il codice del database nella conversione dello schema DMS, puoi rivedere il codice sorgente e il codice convertito. Inoltre, puoi salvare il codice SQL convertito in un bucket Amazon S3.
- Prima di convertire gli schemi del database di origine, puoi configurare le regole di trasformazione. Puoi usare le regole per modificare i tipi di dati delle colonne, spostare gli oggetti da uno schema a un altro e cambiare i nomi degli oggetti. Puoi applicare le regole di trasformazione a database, schemi, tabelle e colonne. Per ulteriori informazioni, consulta [Configurazione delle regole di trasformazione](#).
- Puoi modificare le impostazioni di conversione per migliorare le prestazioni del codice convertito. Queste impostazioni sono specifiche per ogni coppia di conversione e dipendono dalle funzionalità del database di origine utilizzato nel codice. Per ulteriori informazioni, consulta [Specifiche delle impostazioni di conversione dello schema](#).
- In alcuni casi, la conversione dello schema DMS non può convertire le funzionalità del database in funzionalità Amazon RDS equivalenti. In questi casi, la conversione dello schema DMS crea un pacchetto di estensione nel database di destinazione per emulare le funzionalità che non sono state convertite. Per ulteriori informazioni, consulta [Utilizzo dei pacchetti di estensione](#).
- È possibile applicare il codice convertito e lo schema del pacchetto di estensione al database di destinazione. Per ulteriori informazioni, consulta [Applicazione del codice convertito](#).
- DMS Schema Conversion supporta tutte le funzionalità dell'ultima versione. AWS SCT Per ulteriori informazioni, consultate [Le note di rilascio più recenti per AWS SCT](#).
- È possibile modificare il codice SQL convertito prima che DMS lo migri nel database di destinazione. Per ulteriori informazioni, consulta [Modifica e salvataggio del codice SQL convertito](#).

Limitazioni della conversione dello schema

DMS Schema Conversion è una versione web di (). AWS Schema Conversion Tool AWS SCT La conversione dello schema DMS supporta meno piattaforme di database e offre funzionalità più limitate rispetto all'applicazione desktop AWS SCT . Per convertire gli schemi di data warehouse, i framework di big data, il codice SQL delle applicazioni e i processi ETL, utilizza AWS SCT. Per ulteriori informazioni AWS SCT, vedere la [AWS Schema Conversion Tool User Guide](#).

Le seguenti limitazioni si applicano all'uso della conversione dello schema DMS per la conversione dello schema del database:

- Non è possibile salvare un progetto di migrazione e utilizzarlo in modalità offline.
- Non è possibile modificare il codice SQL per il codice sorgente in un progetto di migrazione per DMS Schema Conversion. Per modificare il codice SQL del database di origine, utilizza il normale editor SQL. Scegli Aggiorna dal database per aggiungere il codice aggiornato al progetto di migrazione.
- Le regole di migrazione nella conversione dello schema DMS non supportano la modifica della regola di confronto della colonna. Inoltre, non è possibile utilizzare le regole di migrazione per spostare gli oggetti in un nuovo schema.
- Non è possibile applicare filtri agli alberi del database di origine e di destinazione per visualizzare solo gli oggetti di database che soddisfano la clausola di filtro.
- Il pacchetto di estensione DMS Schema Conversion non include AWS Lambda funzioni che emulano l'invio di e-mail, la pianificazione dei lavori e altre funzionalità nel codice convertito.
- DMS Schema Conversion non utilizza chiavi KMS gestite dal cliente per accedere alle risorse dei clienti. AWS Ad esempio, la conversione dello schema DMS non supporta l'utilizzo di una chiave KMS gestita dal cliente per accedere ai dati dei clienti in Amazon S3.

Nozioni di base sulla conversione dello schema DMS

Per iniziare a usare la conversione dello schema DMS, utilizza il seguente tutorial che ti consente di imparare a configurare la conversione dello schema DMS, creare un progetto di migrazione e connetterti ai tuoi fornitori di dati. Quindi, puoi apprendere come si valuta la complessità della migrazione e si converte il database di origine in un formato compatibile con il database di destinazione. Inoltre, puoi imparare ad applicare il codice convertito al database di destinazione.

Il seguente tutorial illustra le attività prerequisite e dimostra la conversione di un database Amazon RDS per SQL Server in Amazon RDS per MySQL. Puoi utilizzare uno qualsiasi dei fornitori di dati di origine e di destinazione supportati. Per ulteriori informazioni, consulta [Provider di dati di origine per la conversione dello schema DMS](#).

[Per ulteriori informazioni sulla conversione dello schema DMS, leggi le procedure dettagliate sulla step-by-step migrazione per le migrazioni da Oracle a PostgreSQL e da SQL Server a MySQL.](#)

[Questo video](#) presenta l'interfaccia utente della conversione dello schema DMS per familiarizzare con i componenti principali di questo servizio.

Argomenti

- [Prerequisiti per l'utilizzo della conversione dello schema DMS](#)
- [Fase 1: creazione di un profilo dell'istanza](#)
- [Fase 2: configurazione dei fornitori di dati](#)
- [Fase 3: creazione di un progetto di migrazione](#)
- [Fase 4: creazione di un report di valutazione](#)
- [Fase 5: conversione del codice sorgente](#)
- [Fase 6: applicazione del codice convertito](#)
- [Fase 7: pulizia e risoluzione dei problemi](#)

Prerequisiti per l'utilizzo della conversione dello schema DMS

Per configurare la conversione dello schema DMS, completa le attività seguenti. Quindi puoi configurare un profilo dell'istanza, aggiungere fornitori di dati e creare un progetto di migrazione.

Argomenti

- [Creazione di un VPC basato su Amazon VPC](#)
- [Creazione di un bucket Amazon S3](#)
- [Memorizza le credenziali del database in AWS Secrets Manager](#)
- [Creazione di ruoli IAM](#)

Creazione di un VPC basato su Amazon VPC

In questo passaggio, crei un cloud privato virtuale (VPC) nel tuo Account AWS. Questo VPC è basato sul servizio Amazon Virtual Private Cloud (Amazon VPC) e contiene le tue risorse AWS.

Per creare un VPC per la conversione dello schema DMS:

1. [Accedi AWS Management Console e apri la console Amazon VPC all'indirizzo https://console.aws.amazon.com/vpc/.](https://console.aws.amazon.com/vpc/)
2. Seleziona Crea VPC.
3. Nella pagina Crea VPC immetti le seguenti impostazioni:
 - Risorse da creare: VPC e altro

- Generazione automatica del tag del nome: scegli Generazione automatica e inserisci un nome univoco a livello globale. Ad esempio, specifica **sc-vpc**.
 - IPv4 CIDR block (Blocco CIDR IPv4): **10.0.1.0/24**
 - Gateway NAT: in 1 AZ
 - VPC endpoints (Endpoint VPC): nessuno
4. Mantieni le restanti impostazioni così come sono e scegli Crea VPC.
 5. Scegli Sottoreti e prendi nota degli ID della sottorete pubblica e privata.

Per connetterti ai database Amazon RDS, crea un gruppo di sottoreti che includa sottoreti pubbliche.

Per connetterti ai database on-premise, crea un gruppo di sottoreti che includa sottoreti private. Per ulteriori informazioni, consulta [Fase 1: creazione di un profilo dell'istanza](#).

6. Seleziona Gateway NAT. Scegli il Gateway NAT e prendi nota del tuo Indirizzo IP elastico.

Configura la tua rete per assicurarti che AWS DMS possa accedere al database locale di origine dall'indirizzo IP pubblico di questo gateway NAT. Per ulteriori informazioni, consulta [Utilizzo di una connessione Internet a un VPC](#).

Usa questo VPC quando crei il profilo dell'istanza e i database di destinazione su Amazon RDS.

Creazione di un bucket Amazon S3

Per archiviare le informazioni del progetto di migrazione puoi creare un bucket Amazon S3. La conversione dello schema DMS utilizza questo bucket Amazon S3 per salvare elementi come report di valutazione, codice SQL convertito, informazioni sugli oggetti dello schema di database e così via.

Per creare un bucket Amazon S3 per la conversione dello schema DMS

1. [Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/](https://console.aws.amazon.com/s3/).
2. Seleziona Crea bucket.
3. Nella pagina Crea bucket seleziona un nome univoco globale per il bucket S3. Ad esempio, specifica **sc-s3-bucket**.
4. Per Regione AWS scegli la tua regione.
5. Per Controllo delle versioni per il bucket scegli Abilita.

6. Mantieni le restanti impostazioni così come sono e scegli Crea bucket.

Memorizza le credenziali del database in AWS Secrets Manager

Archivia le credenziali del database di origine e di destinazione in AWS Secrets Manager Assicurati di replicare questi segreti sul tuo. Regione AWS La conversione dello schema DMS utilizza questi segreti per connettersi ai database del progetto di migrazione.

Per memorizzare le credenziali del database in AWS Secrets Manager

1. Accedi AWS Management Console e apri la AWS Secrets Manager console all'[indirizzo https://console.aws.amazon.com/secretsmanager/](https://console.aws.amazon.com/secretsmanager/).
2. Scegli Archivia un nuovo segreto.
3. Viene visualizzata la pagina Scegli il tipo di segreto. Per Secret type (Tipo di segreto), scegli il tipo di credenziali del database da archiviare:
 - Credenziali per database Amazon RDS: scegli questa opzione per archiviare le credenziali per il database Amazon RDS. Per Credenziali inserisci le credenziali per il database. Per Database, scegli il database.
 - Credenziali per un altro database: scegli questa opzione per archiviare le credenziali per i database Oracle o SQL Server di origine. Per Credenziali inserisci le credenziali per il database.
 - Altro tipo di segreto: scegli questa opzione per archiviare solo il nome utente e la password per la connessione al database. Scegli Aggiungi riga per aggiungere due coppie chiave-valore. Assicurati di utilizzare **username** e **password** per i nomi delle chiavi. Per i valori relativi a queste chiavi, immetti le credenziali del database.
4. Per Chiave di crittografia, scegli la AWS KMS chiave utilizzata da Secrets Manager per crittografare il valore segreto. Seleziona Successivo.
5. Nella pagina Configura segreto inserisci un nome descrittivo del segreto. Ad esempio, inserisci **sc-source-secret** o **sc-target-secret**.
6. Scegli Replica segreto e per Regione AWS scegli la tua regione. Seleziona Successivo.
7. Nella pagina Configura la rotazione scegli Successivo.
8. Nella pagina Verifica rivedi i dettagli del segreto e quindi scegli Archivia.

Per archiviare le credenziali per i database di origine e di destinazione, ripeti questi passaggi.

Creazione di ruoli IAM

Crea ruoli AWS Identity and Access Management (IAM) da utilizzare nel tuo progetto di migrazione. La conversione dello schema DMS utilizza questi ruoli IAM per accedere al bucket Amazon S3 e alle credenziali del database archiviate in AWS Secrets Manager.

Per creare un ruolo IAM che fornisca accesso al bucket Amazon S3

1. Accedi AWS Management Console e apri la console IAM all'[indirizzo https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella sezione Seleziona un'identità attendibile scegli Servizio AWS . Scegli DMS.
5. Seleziona Successivo. Viene visualizzata la pagina Aggiungi autorizzazioni.
6. Per Filtra le policy immetti **S3**. Scegli AmazonS3 FullAccess.
7. Seleziona Successivo. Viene visualizzata la pagina Nomina, verifica e crea.
8. In Nome ruolo immetti un nome descrittivo. Ad esempio, specifica **sc-s3-role**. Scegli Crea ruolo.
9. Nella pagina Ruoli immetti **sc-s3-role** per Nome ruolo. Scegli sc-s3-role.
10. Nella pagina sc-s3-role seleziona Relazioni di attendibilità. Seleziona Modifica policy di attendibilità.
11. Nella pagina Modifica policy di attendibilità, modifica le relazioni di attendibilità per il ruolo in modo da utilizzare il principale del servizio `schema-conversion.dms.amazonaws.com` come entità attendibile.
12. Scegliere Update trust Policy (Aggiorna policy di attendibilità).

Per creare un ruolo IAM che fornisca l'accesso a AWS Secrets Manager

1. Accedi AWS Management Console e apri la console IAM all'[indirizzo https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella sezione Seleziona un'identità attendibile scegli Servizio AWS . Scegli DMS.
5. Seleziona Successivo. Viene visualizzata la pagina Aggiungi autorizzazioni.

6. Per Filtra le policy immetti **Secret**. Scegli SecretsManagerReadWrite.
7. Seleziona Successivo. Viene visualizzata la pagina Nomina, verifica e crea.
8. In Nome ruolo immetti un nome descrittivo. Ad esempio, specifica **sc-secrets-manager-role**. Scegli Crea ruolo.
9. Nella pagina Ruoli immetti **sc-secrets-manager-role** per Nome ruolo. Scegliete sc-secrets-manager-role.
10. Nella sc-secrets-manager-rolepagina, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.
11. Nella pagina Modifica politica di fiducia, modifica le relazioni di trust per il ruolo da utilizzare schema-conversion.dms.amazonaws.com e il responsabile del servizio AWS DMS regionale come entità fidate. Questo responsabile del servizio AWS DMS regionale ha il seguente formato.

```
dms.region-name.amazonaws.com
```

Sostituisci *region-name* con il nome della tua regione, ad esempio us-east-1.

L'esempio di codice seguente mostra il principale della regione us-east-1.

```
dms.us-east-1.amazonaws.com
```

Il seguente esempio di codice mostra una politica di attendibilità per l'accesso alla conversione AWS DMS dello schema.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.us-east-1.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "schema-conversion.dms.amazonaws.com"
      }
    }
  ]
}
```

```
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

12. Scegliere Update trust Policy (Aggiorna policy di attendibilità).

Fase 1: creazione di un profilo dell'istanza

Prima di creare un profilo dell'istanza, configura un gruppo di sottoreti per il tuo profilo dell'istanza. Per ulteriori informazioni sulla creazione di un gruppo di sottoreti per il progetto di AWS DMS migrazione, consulta [Creazione di un gruppo di sottoreti](#).

È possibile creare un profilo dell'istanza come descritto nella seguente procedura. Nel profilo dell'istanza si specificano le impostazioni di rete e di sicurezza per il progetto della conversione dello schema DMS.

Come creare un profilo dell'istanza

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione scegli Profili dell'istanza, quindi seleziona Crea profilo dell'istanza.
3. Per Nome immetti un nome univoco per il profilo dell'istanza. Ad esempio, specifica **sc-instance**.
4. Per Tipo di rete scegli IPv4 per creare un profilo dell'istanza che supporti solo l'indirizzamento IPv4. Per creare un profilo dell'istanza che supporti l'indirizzamento IPv4 e IPv6, scegli la Modalità dual-stack.
5. Per Cloud privato virtuale (VPC) scegli il VPC creato nella fase dei prerequisiti.
6. Per Gruppo di sottoreti seleziona il gruppo di sottoreti per il profilo dell'istanza. Per connetterti ai database Amazon RDS, utilizza un gruppo di sottoreti che includa sottoreti pubbliche. Per connetterti ai database on-premise, usa un gruppo di sottoreti che includa sottoreti private.
7. Seleziona Crea profilo dell'istanza.

Per creare un progetto di migrazione, usa questo profilo dell'istanza.

Fase 2: configurazione dei fornitori di dati

Successivamente, crea i fornitori di dati che descrivono i database di origine e di destinazione. Per ogni fornitori di dati, si specifica un tipo di datastore e le informazioni sulla posizione. Le credenziali del database non vengono archiviate in un fornitore di dati.

Per creare un fornitore di dati per un database di origine on-premise

1. Accedi a e apri la AWS DMS console. AWS Management Console
2. Nel riquadro di navigazione scegli Fornitori di dati, quindi seleziona Crea un fornitore di dati.
3. Per Nome immetti un nome univoco per il fornitore di dati di origine. Ad esempio, specifica **sc-source**.
4. Per Tipo di motore scegli il tipo di motore di database per il tuo fornitore di dati.
5. Fornisci le informazioni sulla connessione per il database di origine. I parametri di connessione dipendono dal motore di database di origine. Per ulteriori informazioni, consulta [Creazione di fornitori di dati](#).
6. Per Modalità Secure Socket Layer (SSL) scegli il tipo di applicazione SSL.
7. Scegli Crea un fornitore di dati.

Per creare un fornitore di dati per un database Amazon RDS di destinazione

1. Accedi a AWS Management Console e apri la AWS DMS console.
2. Nel riquadro di navigazione scegli Fornitori di dati, quindi seleziona Crea un fornitore di dati.
3. Per Configurazione scegli Istanza di database RDS.
4. Per Database da RDS scegli Sfoglia e seleziona il tuo database. La conversione dello schema DMS recupera automaticamente le informazioni sul tipo di motore, sul nome del server e sulla porta.
5. Per Nome immetti un nome univoco per il fornitore di dati di destinazione. Ad esempio, specifica **sc-target**.
6. In Database name (Nome del database) immettere il nome del database.
7. Per Modalità Secure Socket Layer (SSL) scegli il tipo di applicazione SSL.
8. Scegli Crea un fornitore di dati.

Fase 3: creazione di un progetto di migrazione

A questo punto puoi creare un progetto di migrazione. Nel progetto di migrazione specifichi i fornitori di dati di origine e di destinazione e il profilo dell'istanza.

Per creare un progetto di migrazione

1. Scegli Progetti di migrazione, quindi seleziona Crea un progetto di migrazione.
2. Per Nome immetti un nome univoco per il progetto di migrazione. Ad esempio, specifica **sc-project**.
3. Per Profilo dell'istanza scegli **sc-instance**.
4. Per Origine scegli Sfoglia, quindi seleziona **sc-source**.
5. Per ID segreto scegli **sc-source-secret**.
6. In IAM role (Ruolo IAM) scegliere **sc-secrets-manager-role**.
7. Per Destinazione scegli Sfoglia, quindi seleziona **sc-target**.
8. Per ID segreto scegli **sc-target-secret**.
9. In IAM role (Ruolo IAM) scegliere **schema-conversion-role**.
10. Scegli Crea un progetto di migrazione.

Fase 4: creazione di un report di valutazione

Per valutare la complessità della migrazione puoi creare il report di valutazione della migrazione del database. Questo report include l'elenco di tutti gli oggetti del database che la conversione dello schema DMS non è in grado di convertire automaticamente.

Per creare un report di valutazione

1. Scegli Progetti di migrazione, quindi seleziona **sc-project**.
2. Scegli Conversione dello schema, quindi seleziona Avvia conversione dello schema.
3. Nel riquadro del database di origine scegli lo schema di database da valutare. Inoltre, seleziona la casella di controllo relativa al nome di questo schema.
4. Nel riquadro del database di origine scegli Valuta nel menu Operazioni. Viene visualizzata la finestra di dialogo Valuta.
5. Seleziona Valuta nella finestra di dialogo per confermare la scelta.

La scheda Riepilogo mostra il numero di elementi che la conversione dello schema DMS può convertire automaticamente in oggetti di archiviazione del database e oggetti di codice del database.

6. Scegli Elementi d'azione per visualizzare l'elenco di tutti gli oggetti del database che la conversione dello schema DMS non può convertire automaticamente. Esamina le azioni consigliate per ogni elemento.
7. Per salvare una copia del report di valutazione, scegli Esporta risultati. Quindi, scegli uno dei seguenti formati: CSV o PDF. Viene visualizzata la finestra di dialogo Esporta.
8. Scegli Esporta per confermare la scelta.
9. Scegli Bucket S3. Viene visualizzata la console Amazon S3.
10. Scegli Scarica per salvare il report di valutazione.

Fase 5: conversione del codice sorgente

È possibile convertire lo schema di database di origine utilizzando la seguente procedura. Puoi salvare il codice convertito come script SQL in un file di testo.

Per convertire lo schema di database

1. Nel riquadro del database di origine scegli lo schema di database da convertire. Inoltre, seleziona la casella di controllo relativa al nome di questo schema.
2. Nel riquadro del database di origine scegli Converti nel menu Operazioni. Viene visualizzata la finestra di dialogo Converti.
3. Seleziona Converti nella finestra di dialogo per confermare la scelta.
4. Scegli un oggetto di database nel riquadro del database di origine. La conversione dello schema DMS visualizza il codice sorgente e il codice convertito per questo oggetto. È possibile modificare il codice SQL convertito per un oggetto di database utilizzando la funzione Modifica SQL. Per ulteriori informazioni, consulta [Modifica e salvataggio del codice SQL convertito](#).
5. Nel riquadro del database di destinazione scegli lo schema di database convertito. Inoltre, seleziona la casella di controllo relativa al nome di questo schema.
6. Per Operazioni scegli Salva come SQL. Viene visualizzata la finestra di dialogo Salva.
7. Scegli Salva come SQL per confermare la scelta.
8. Scegli Bucket S3. Viene visualizzata la console Amazon S3.
9. Scegli Scarica per salvare gli script SQL.

Fase 6: applicazione del codice convertito

La conversione dello schema DMS non applica immediatamente il codice convertito al database di destinazione. Per aggiornare il database di destinazione, puoi utilizzare gli script SQL creati nella fase precedente. In alternativa, utilizza la procedura seguente per applicare il codice convertito della conversione dello schema DMS.

Per applicare il codice convertito

1. Nel riquadro del database di destinazione scegli lo schema di database convertito. Inoltre, seleziona la casella di controllo relativa al nome di questo schema.
2. Per Operazioni scegli Applica le modifiche. Viene visualizzata la finestra di dialogo Applica le modifiche.
3. Scegli Applica per confermare la scelta.

Fase 7: pulizia e risoluzione dei problemi

Puoi usare Amazon CloudWatch per rivedere o condividere i tuoi log di conversione dello schema DMS.

Per esaminare i log della conversione dello schema DMS

1. [Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.](https://console.aws.amazon.com/cloudwatch/)
2. Scegli Log, Gruppi di log.

Il nome del gruppo di log della conversione dello schema DMS inizia con `dms-tasks-sct`. È possibile ordinare i gruppi di log in base alla Data creazione per trovare il gruppo di log della conversione dello schema DMS.

Inoltre, il nome del gruppo di log include il nome della risorsa Amazon (ARN) del progetto di migrazione. Puoi vedere l'ARN del tuo progetto nella pagina Progetti di migrazione nella conversione dello schema DMS. Assicurati di scegliere ARN in Preferenze.

3. Scegli il nome del gruppo di log, quindi seleziona il nome del flusso di log.
4. Per Operazioni scegli Esporta risultati per salvare il log della conversione dello schema DMS.

Al termine della conversione dello schema DMS, puoi pulire le risorse.

Per eseguire la pulizia delle risorse di conversione dello schema DMS

1. Accedi a AWS Management Console e apri la AWS DMS console.
2. Nel riquadro di navigazione seleziona Progetti di migrazione.
 - a. Scegli **sc-project**.
 - b. Scegli Conversione dello schema, quindi seleziona Chiudi conversione dello schema.
 - c. Seleziona Elimina per confermare la scelta.
3. Nel riquadro di navigazione scegli Profili dell'istanza.
 - a. Scegli **sc-instance**.
 - b. Seleziona Elimina per confermare la scelta.
4. Nel pannello di navigazione scegli Fornitori di dati.
 - a. Seleziona **sc-source** e **sc-target**.
 - b. Seleziona Elimina per confermare la scelta.

Inoltre, assicurati di ripulire AWS le altre risorse che hai creato, come il bucket Amazon S3, i segreti del database, i ruoli IAM e il cloud privato virtuale (VPC). AWS Secrets Manager

Configurazione di una rete per la conversione dello schema DMS

La conversione dello schema DMS crea un'istanza di conversione dello schema in un cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Puoi specificare il VPC da utilizzare quando crei il profilo dell'istanza. Puoi utilizzare il VPC predefinito per l'account e la Regione AWS oppure crearne uno nuovo.

È possibile utilizzare diverse configurazioni di rete per impostare l'interazione dei database di origine e di destinazione con la conversione dello schema DMS. Queste configurazioni dipendono dalla posizione del fornitore di dati di origine e dalle impostazioni di rete. Nei seguenti argomenti sono descritte le configurazioni di rete più comuni.

Argomenti

- [Utilizzo di un singolo VPC per i fornitori di dati di origine e di destinazione](#)
- [Utilizzo di più VPC per i fornitori di dati di origine e di destinazione](#)
- [Utilizzo di AWS Direct Connect o di una VPN per configurare una rete per un VPC](#)

- [Utilizzo di una connessione Internet a un VPC](#)
- [Utilizzo di un ambiente senza un gateway Internet](#)

Utilizzo di un singolo VPC per i fornitori di dati di origine e di destinazione

La configurazione di rete più semplice per la conversione dello schema DMS è la configurazione di un singolo VPC. In questo caso, il fornitore di dati di origine, il profilo dell'istanza e il fornitore di dati di destinazione si trovano tutti nello stesso VPC. Puoi utilizzare questa configurazione per convertire il database di origine su un'istanza Amazon EC2.

Per usare questa configurazione, assicurati che il gruppo di sicurezza VPC utilizzato dal profilo dell'istanza abbia accesso ai fornitori di dati. Ad esempio, puoi consentire un intervallo per il routing interdominio senza classi (CIDR) del VPC o l'indirizzo IP elastico per il gateway Network Address Translation (NAT).

Utilizzo di più VPC per i fornitori di dati di origine e di destinazione

Se i fornitori di dati di origine e di destinazione si trovano in VPC diversi, puoi creare il profilo dell'istanza in uno dei VPC e collegare i due VPC utilizzando il peering VPC. Puoi utilizzare questa configurazione per convertire il database di origine su un'istanza Amazon EC2.

Una connessione peering VPC è una connessione di rete tra due VPC che consente di eseguire l'instradamento tramite gli indirizzi IP privati di ciascun VPC come se si trovassero sulla stessa rete. Puoi anche creare una connessione di peering VPC tra VPC, con un VPC in un altro account AWS o con un VPC in una Regione AWS diversa. Per ulteriori informazioni sul peering di VPC, consulta [Peering di VPC](#) nella Guida per l'utente di Amazon VPC.

Per implementare il peering VPC, segui le istruzioni in [Utilizzo di connessioni peering VPC](#) nella Guida per l'utente di Amazon VPC. Assicurati che la tabella di routing di un VPC contenga il blocco CIDR dell'altro. Ad esempio, supponi che il VPC A utilizzi la destinazione 10.0.0.0/16 e che il VPC B utilizzi la destinazione 172.31.0.0. In questo caso, la tabella di routing del VPC A deve contenere 172.31.0.0 e la tabella di routing del VPC B deve contenere 10.0.0.0/16. Per informazioni più dettagliate, consulta [Aggiornamento delle tabelle di routing per una connessione peering VPC](#) nella guida Peering di VPC di Amazon VPC.

Utilizzo di AWS Direct Connect o di una VPN per configurare una rete per un VPC

Le reti remote possono connettersi a un VPC utilizzando diverse opzioni, ad esempio AWS Direct Connect oppure una connessione VPN hardware o software. Puoi usare queste opzioni per integrare i servizi locali esistenti estendendo una rete interna nel Cloud AWS. È possibile integrare servizi locali quali monitoraggio, autenticazione, sicurezza, dati o altri sistemi. Questo tipo di estensione di rete consente di connettere facilmente i servizi locali alle risorse ospitate su AWS, come un VPC. Puoi utilizzare questa configurazione per convertire il database on-premise di origine.

In questa configurazione, il gruppo di sicurezza VPC deve includere una regola di indirizzamento che invia a un host il traffico destinato a un intervallo CIDR del VPC o un indirizzo IP specifico. Questo host deve essere in grado di collegare il traffico del VPC nella VPN locale. In questo caso, l'host NAT include le proprie impostazioni del gruppo di sicurezza. Queste impostazioni devono consentire il traffico proveniente dall'intervallo CIDR del VPC o dal gruppo di sicurezza verso l'istanza NAT. Per ulteriori informazioni, consulta [Creazione di una connessione VPN](#) nella Guida per l'utente di AWS Site-to-Site VPN.

Utilizzo di una connessione Internet a un VPC

Se non utilizzi una VPN o AWS Direct Connect per connetterti alle risorse AWS, puoi utilizzare una connessione Internet. Questa configurazione prevede una sottorete privata in un VPC con un gateway Internet. Il gateway contiene il fornitore di dati di destinazione e il profilo dell'istanza. Puoi utilizzare questa configurazione per convertire il database on-premise di origine.

Per aggiungere un gateway Internet al VPC, consulta [Collegamento di un gateway Internet](#) nella Guida per l'utente di Amazon VPC.

La tabella di routing VPC deve includere regole di instradamento che, per impostazione predefinita, inviano al gateway Internet il traffico non destinato al VPC. In questa configurazione, la connessione al fornitore di dati sembra provenire dall'indirizzo IP pubblico del gateway NAT. Per ulteriori informazioni, consulta [Tabelle di routing VPC](#) nella Guida per l'utente di Amazon VPC.

Utilizzo di un ambiente senza un gateway Internet

Per creare un ambiente per la conversione dello schema senza utilizzare un gateway Internet, procedi come segue.

1. Segui le fasi 1-3 del tutorial [Nozioni di base](#), con le seguenti modifiche:

- Scegli le sottoreti private anziché pubbliche.
- Durante la creazione dell'istanza scegli No per Assegna IP pubblico.
2. Apri la console Amazon VPC.
3. Scegli Endpoint, quindi Crea endpoint.
4. Nella pagina Crea endpoint esegui le operazioni seguenti:
 - In Categoria servizio scegli Servizi AWS.
 - Nell'elenco Servizi scegli com.amazonaws.**{region}**.secretsmanager
 - Nella sezione VPC scegli il VPC che hai creato.
 - Scegli le sottoreti per il VPC.
 - Scegli il gruppo di sicurezza per il VPC.
 - Per Policy lascia selezionata l'opzione Accesso completo.
5. Termina il resto del tutorial [Nozioni di base](#).

Creazione di fornitori di dati di origine per la conversione dello schema DMS

È possibile utilizzare un database Microsoft SQL Server, Oracle o PostgreSQL come fornitore di dati di origine nei progetti di migrazione per DMS Schema Conversion. Il fornitore di dati di origine può essere un motore autogestito in esecuzione on-premise o su un'istanza Amazon EC2.

Assicurati di configurare la rete per consentire l'interazione tra il fornitore di dati di origine e la conversione dello schema DMS. Per ulteriori informazioni, consulta [Configurazione di una rete per la conversione dello schema DMS](#).

Argomenti

- [Utilizzo di un database Microsoft SQL Server come origine nella conversione dello schema DMS](#)
- [Utilizzo di un database Oracle come origine nella conversione dello schema DMS](#)
- [Utilizzo di un database Oracle Data Warehouse come origine nella conversione dello schema DMS](#)
- [Utilizzo di un database PostgreSQL come sorgente in DMS Schema Conversion](#)
- [Utilizzo di un database MySQL come sorgente in DMS Schema Conversion](#)

Utilizzo di un database Microsoft SQL Server come origine nella conversione dello schema DMS

È possibile utilizzare i database SQL Server come origine della migrazione nella conversione dello schema DMS.

È possibile utilizzare la conversione dello schema DMS per convertire gli oggetti di codice del database da SQL Server alle seguenti destinazioni:

- Aurora MySQL
- Aurora PostgreSQL
- RDS for MySQL
- RDS per PostgreSQL

Per informazioni sulle versioni supportate del database SQL Server, consulta [Provider di dati di origine per la conversione dello schema DMS](#).

Per ulteriori informazioni sull'utilizzo di DMS Schema Conversion con un database SQL Server di origine, consulta la procedura dettagliata per la [migrazione da SQL Server a MySQL step-by-step](#).

Privilegi per Microsoft SQL Server come origine

Esamina il seguente elenco di privilegi necessari per Microsoft SQL Server come origine:

- VIEW DEFINITION
- VIEW DATABASE STATE

Il privilegio VIEW DEFINITION consente agli utenti con accesso pubblico di visualizzare le definizioni degli oggetti. La conversione dello schema DMS utilizza il privilegio VIEW DATABASE STATE per verificare le funzionalità di SQL Server Enterprise Edition.

Ripeti l'assegnazione per ogni database di cui desideri convertire lo schema.

Inoltre, assegna i seguenti privilegi sul database master:

- VIEW SERVER STATE
- VIEW ANY DEFINITION

La conversione dello schema DMS utilizza il privilegio VIEW SERVER STATE per raccogliere le impostazioni e la configurazione del server. Assicurati di fornire il privilegio VIEW ANY DEFINITION per visualizzare i fornitori di dati.

Per leggere le informazioni su Microsoft Analysis Services, esegui il seguente comando sul database master.

```
EXEC master..sp_addsrvrolemember @loginame = N'<user_name>', @rolename = N'sysadmin'
```

Nell'esempio precedente, sostituisci il segnaposto *<user_name>* con il nome dell'utente a cui sono stati precedentemente assegnati i privilegi richiesti.

Per leggere informazioni su SQL Server Agent, aggiungi il tuo utente al ruolo SQL. AgentUser Esegui il comando seguente sul database msdb.

```
EXEC sp_addrolemember <SQLAgentRole>, <user_name>;
```

Nell'esempio precedente, sostituisci il segnaposto *<SQLAgentRole>* con il nome del ruolo SQL Server Agent. Sostituisci il segnaposto *<user_name>* con il nome dell'utente a cui sono stati precedentemente assegnati i privilegi richiesti. Per ulteriori informazioni, consulta [Aggiungere un utente al AgentUser ruolo SQL](#) nella Amazon RDS User Guide.

Per rilevare l'invio dei log, fornisci il privilegio SELECT on dbo.log_shipping_primary_databases sul database msdb.

Per utilizzare l'approccio di notifica della replica DDL (Data Definition Language), assegna il privilegio RECEIVE ON *<schema_name>.<queue_name>* sui database di origine. In questo esempio, sostituisci il segnaposto *<schema_name>* con il nome dello schema di database. Quindi, sostituisci il segnaposto *<queue_name>* con il nome di una tabella di coda.

Utilizzo di un database Oracle come origine nella conversione dello schema DMS

È possibile utilizzare i database Oracle come origine della migrazione nella conversione dello schema DMS.

Per connettersi al database Oracle, utilizza il SID (System ID) Oracle. Per individuare il SID Oracle, invia la seguenti query al database Oracle:

```
SELECT sys_context('userenv','instance_name') AS SID FROM dual;
```

È possibile utilizzare la conversione dello schema DMS per convertire gli oggetti di codice del database da Oracle Database alle seguenti destinazioni:

- Aurora MySQL
- Aurora PostgreSQL
- RDS for MySQL
- RDS per PostgreSQL

Per informazioni sulle versioni supportate del database Oracle, consulta [Provider di dati di origine per la conversione dello schema DMS](#).

Per ulteriori informazioni sull'utilizzo di DMS Schema Conversion con un database Oracle di origine, consulta la procedura dettagliata per la migrazione [da Oracle a PostgreSQL](#). step-by-step

Privilegi per Oracle come origine

I privilegi necessari per Oracle come origine sono i seguenti:

- CONNECT
- SELECT_CATALOG_ROLE
- SELECT ANY DICTIONARY
- SELECT ON SYS.ARGUMENT\$

Utilizzo di un database Oracle Data Warehouse come origine nella conversione dello schema DMS

È possibile utilizzare i database Oracle Data Warehouse come origine della migrazione per la conversione dello schema DMS al fine di convertire gli oggetti del codice del database e il codice dell'applicazione in Amazon Redshift.

Per informazioni sulle versioni supportate del database Oracle, consulta [Provider di dati di origine per la conversione dello schema DMS](#). Per ulteriori informazioni sull'utilizzo di DMS Schema Conversion con un database Oracle di origine, consulta la procedura dettagliata per la migrazione [da Oracle a PostgreSQL](#). step-by-step

Privilegi per l'utilizzo di un database Oracle Data Warehouse come origine

I privilegi necessari per Oracle Data Warehouse come origine sono i seguenti:

- CONNECT
- SELECT_CATALOG_ROLE
- SELECT ANY DICTIONARY

Impostazioni di conversione da Oracle Data Warehouse ad Amazon Redshift

Per informazioni sulla modifica delle impostazioni della conversione dello schema DMS, consulta [Specifiche delle impostazioni di conversione dello schema per i progetti di migrazione](#).

Le impostazioni di conversione da Oracle Data Warehouse ad Amazon Redshift sono le seguenti:

- Aggiungi commenti nel codice convertito per gli elementi d'azione con la gravità selezionata o superiore: questa impostazione limita il numero di commenti per gli elementi d'azione nel codice convertito. DMS aggiunge i commenti nel codice convertito per gli elementi d'azione con la gravità selezionata o superiore.

Ad esempio, per ridurre al minimo il numero di commenti nel codice convertito, scegli Solo errori. Per includere commenti per tutti gli elementi d'azione nel codice convertito, scegli Tutti i messaggi.

- Numero massimo di tabelle per il cluster Amazon Redshift di destinazione: questa impostazione specifica il numero massimo di tabelle che DMS può applicare al cluster Amazon Redshift di destinazione. Amazon Redshift dispone di quote che limitano l'utilizzo delle tabelle per diversi tipi di nodo cluster. Questa impostazione supporta i seguenti valori:
 - Automatico: DMS determina il numero di tabelle da applicare al cluster Amazon Redshift di destinazione in base al tipo di nodo.
 - Imposta un valore: specifica il numero di tabelle manualmente.

DMS converte tutte le tabelle di origine, anche se il numero di tabelle è superiore a quello che il cluster Amazon Redshift può archiviare. DMS archivia il codice convertito nel progetto e non lo applica al database di destinazione. Se raggiungi la quota del cluster Amazon Redshift per le tabelle quando applichi il codice convertito, DMS visualizza un messaggio di avviso. Inoltre, DMS applica le tabelle al cluster Amazon Redshift di destinazione fino a quando il numero di tabelle non raggiunge il limite.

Per informazioni sulle quote delle tabelle Amazon Redshift, consulta [Quote e limiti in Amazon Redshift](#).

- Utilizza la vista UNION ALL: questa impostazione consente di specificare il numero massimo di tabelle di destinazione che DMS può creare per una singola tabella di origine.

Amazon Redshift non supporta il partizionamento della tabella. Per emulare il partizionamento della tabella e accelerare l'esecuzione delle query, DMS può migrare ogni partizione della tabella di origine in una tabella separata in Amazon Redshift. Quindi, DMS genera una vista che include i dati di tutte le tabelle di destinazione che crea.

DMS determina automaticamente il numero di partizioni nella tabella di origine. A seconda del tipo di partizionamento della tabella di origine, questo numero può superare la quota delle tabelle che puoi applicare al cluster Amazon Redshift. Per evitare di raggiungere questa quota, inserisci il numero massimo di tabelle di destinazione che DMS può creare per le partizioni di una singola tabella di origine. L'opzione predefinita è 368 tabelle, che rappresenta una partizione per 366 giorni all'anno, più due tabelle per le partizioni NO RANGE e UNKNOWN.

- Gli elementi del formato datatype utilizzati nel codice Oracle sono simili alle stringhe del formato datetime in Amazon Redshift: utilizza questa impostazione per convertire le funzioni di formattazione dei tipi di dati come TO_CHAR, TO_DATE e TO_NUMBER con elementi del formato datetime non supportati da Amazon Redshift. Per impostazione predefinita, DMS utilizza le funzioni dei pacchetti di estensione per emulare questi elementi del formato non supportati nel codice convertito.

Il modello del formato datetime di Oracle include più elementi rispetto alle stringhe del formato datetime di Amazon Redshift. Se il codice sorgente include solo elementi del formato datetime supportati da Amazon Redshift, imposta questo valore per evitare le funzioni dei pacchetti di estensione nel codice convertito e accelerare l'esecuzione del codice convertito.

- Gli elementi del formato numerico utilizzati nel codice Oracle sono simili alle stringhe del formato numerico in Amazon Redshift: utilizza questa impostazione per convertire le funzioni di formattazione dei tipi di dati numerici non supportati da Amazon Redshift. Per impostazione predefinita, DMS utilizza le funzioni dei pacchetti di estensione per emulare questi elementi del formato non supportati nel codice convertito.

Il modello del formato numerico di Oracle include più elementi rispetto alle stringhe del formato numerico di Amazon Redshift. Se il codice sorgente include solo elementi del formato numerico supportati da Amazon Redshift, imposta questo valore per evitare le funzioni dei pacchetti di estensione nel codice convertito e accelerare l'esecuzione del codice convertito.

- Utilizza la funzione NVL per emulare il comportamento delle funzioni Oracle LEAD e LAG: se il codice sorgente non utilizza i valori predefiniti per l'offset delle funzioni LEAD e LAG, DMS può emularle con la funzione NVL. Per impostazione predefinita, DMS genera un elemento d'azione per ogni utilizzo delle funzioni LEAD e LAG. L'emulazione di queste funzioni tramite NVL accelera l'esecuzione del codice convertito.
- Emula il comportamento delle chiavi primarie e univoche: specifica questa impostazione per fare in modo che DMS emuli il comportamento dei vincoli delle chiavi primarie e univoche nel cluster Amazon Redshift di destinazione. Amazon Redshift non impone i vincoli delle chiavi primarie e univoche e li utilizza solo a scopo informativo. Se il codice sorgente utilizza i vincoli delle chiavi primarie e univoche, specifica questa impostazione per assicurarti che DMS ne emuli il comportamento.
- Usa la codifica di compressione: specifica questa impostazione per applicare la codifica di compressione alle colonne della tabella Amazon Redshift. DMS assegna automaticamente la codifica di compressione utilizzando l'algoritmo Redshift predefinito. Per informazioni sulla codifica di compressione, consulta [Codifiche di compressione](#) nella Guida per sviluppatori di database di Amazon Redshift.

Amazon Redshift per impostazione predefinita non applica la compressione alle colonne definite come chiavi di ordinamento e distribuzione. Per applicare la compressione a queste colonne, imposta Usa la codifica di compressione per le colonne KEY. Puoi selezionare questa opzione solo quando imposti Usa la codifica di compressione.

Utilizzo di un database PostgreSQL come sorgente in DMS Schema Conversion

È possibile utilizzare i database PostgreSQL come origine di migrazione in DMS Schema Conversion.

È possibile utilizzare DMS Schema Conversion per convertire gli oggetti del codice del database dal database PostgreSQL ai seguenti obiettivi:

- MySQL
- Aurora MySQL

I privilegi richiesti per PostgreSQL come sorgente sono i seguenti:

- CONNECT ON DATABASE <database_name>

- USAGE ON SCHEMA <database_name>
- SELECT ON ALL TABLES IN SCHEMA <database_name>
- SELECT ON ALL SEQUENCES IN SCHEMA <database_name>

Utilizzo di un database MySQL come sorgente in DMS Schema Conversion

È possibile utilizzare i database MySQL come origine di migrazione in DMS Schema Conversion.

È possibile utilizzare DMS Schema Conversion per convertire gli oggetti del codice del database dal database MySQL ai seguenti obiettivi:

- PostgreSQL
- Aurora PostgreSQL

I privilegi richiesti per MySQL come sorgente sono i seguenti:

- SELECT ON *.*
- SHOW VIEW ON *.*

Impostazioni di conversione da MySQL a PostgreSQL

Per informazioni sulla modifica delle impostazioni della conversione dello schema DMS, consulta [Specifiche delle impostazioni di conversione dello schema per i progetti di migrazione](#).

Le impostazioni di conversione da MySQL a PostgreSQL includono quanto segue:

- Commenti nel codice SQL convertito: imposta questa impostazione per aggiungere commenti nel codice convertito per le azioni con la gravità selezionata o superiore.

Valori validi:

- Solo errori
- Errori e avvertenze
- Tutti i messaggi

Creazione di fornitori di dati di destinazione per la conversione dello schema DMS

È possibile utilizzare i database MySQL e PostgreSQL come fornitore di dati di destinazione nei progetti di migrazione per la conversione dello schema DMS. Il fornitore di dati di destinazione può essere un'istanza Amazon EC2, Amazon RDS o Amazon Aurora.

Argomenti

- [Utilizzo di un database MySQL come destinazione nella conversione dello schema DMS](#)
- [Utilizzo di un database PostgreSQL come destinazione nella conversione dello schema DMS](#)
- [Utilizzo di un cluster Amazon Redshift come destinazione nella conversione dello schema DMS](#)

Utilizzo di un database MySQL come destinazione nella conversione dello schema DMS

È possibile utilizzare i database MySQL come destinazione di migrazione nella conversione dello schema DMS.

Per informazioni sui database di destinazione supportati, consulta [Provider di dati di destinazione per la conversione dello schema DMS](#).

Privilegi per MySQL come destinazione

I privilegi necessari per MySQL come destinazione sono i seguenti:

- CREATE ON *.*
- ALTER ON *.*
- DROP ON *.*
- INDEX ON *.*
- REFERENCES ON *.*
- SELECT ON *.*
- CREATE VIEW ON *.*
- SHOW VIEW ON *.*
- TRIGGER ON *.*

- CREATE ROUTINE ON *.*
- ALTER ROUTINE ON *.*
- EXECUTE ON *.*
- CREATE TEMPORARY TABLES ON *.*
- AWS_LAMBDA_ACCESS
- INSERT, UPDATE ON AWS_ORACLE_EXT.*
- INSERT, UPDATE, DELETE ON AWS_ORACLE_EXT_DATA.*
- INSERT, UPDATE ON AWS_SQLSERVER_EXT.*
- INSERT, UPDATE, DELETE ON AWS_SQLSERVER_EXT_DATA.*
- CREATE TEMPORARY TABLES ON AWS_SQLSERVER_EXT_DATA.*

È possibile utilizzare il seguente esempio di codice per creare un utente del database e assegnare i privilegi.

```
CREATE USER 'user_name' IDENTIFIED BY 'your_password';
GRANT CREATE ON *.* TO 'user_name';
GRANT ALTER ON *.* TO 'user_name';
GRANT DROP ON *.* TO 'user_name';
GRANT INDEX ON *.* TO 'user_name';
GRANT REFERENCES ON *.* TO 'user_name';
GRANT SELECT ON *.* TO 'user_name';
GRANT CREATE VIEW ON *.* TO 'user_name';
GRANT SHOW VIEW ON *.* TO 'user_name';
GRANT TRIGGER ON *.* TO 'user_name';
GRANT CREATE ROUTINE ON *.* TO 'user_name';
GRANT ALTER ROUTINE ON *.* TO 'user_name';
GRANT EXECUTE ON *.* TO 'user_name';
GRANT CREATE TEMPORARY TABLES ON *.* TO 'user_name';
GRANT AWS_LAMBDA_ACCESS TO 'user_name';
GRANT INSERT, UPDATE ON AWS_ORACLE_EXT.* TO 'user_name';
GRANT INSERT, UPDATE, DELETE ON AWS_ORACLE_EXT_DATA.* TO 'user_name';
GRANT INSERT, UPDATE ON AWS_SQLSERVER_EXT.* TO 'user_name';
GRANT INSERT, UPDATE, DELETE ON AWS_SQLSERVER_EXT_DATA.* TO 'user_name';
GRANT CREATE TEMPORARY TABLES ON AWS_SQLSERVER_EXT_DATA.* TO 'user_name';
```

Nell'esempio precedente, sostituisci *user_name* con il nome dell'utente. Quindi, sostituisci *your_password* con una password sicura.

Per utilizzare Amazon RDS per MySQL o Aurora MySQL come destinazione, imposta il parametro `lower_case_table_names` su 1. Questo valore indica che il server MySQL gestisce gli identificatori di nomi di oggetti come tabelle, indici, trigger e database senza distinzione tra maiuscole e minuscole. Se hai attivato la registrazione binaria nell'istanza di destinazione, imposta il parametro `log_bin_trust_function_creators` su 1. In questo caso, non è necessario utilizzare le caratteristiche `DETERMINISTIC`, `READS SQL DATA` o `NO SQL` per creare funzioni archiviate. Per configurare questi parametri, crea un nuovo gruppo di parametri di database o modifica un gruppo di parametri di database esistente.

Utilizzo di un database PostgreSQL come destinazione nella conversione dello schema DMS

È possibile utilizzare i database PostgreSQL come destinazione di migrazione nella conversione dello schema DMS.

Per informazioni sui database di destinazione supportati, consulta [Provider di dati di destinazione per la conversione dello schema DMS](#).

Privilegi per PostgreSQL come destinazione

Per utilizzare PostgreSQL come destinazione, la conversione dello schema DMS richiede il privilegio `CREATE ON DATABASE`. Crea un utente e assegnagli questo privilegio per ogni database che desideri utilizzare nel progetto di migrazione per la conversione dello schema DMS.

Per utilizzare Amazon RDS per PostgreSQL come destinazione, la conversione dello schema DMS richiede il ruolo `rds_superuser`.

Per utilizzare i sinonimi pubblici convertiti, modifica il percorso di ricerca predefinito del database usando il seguente comando.

```
ALTER DATABASE <db_name> SET SEARCH_PATH = "$user", public_synonyms, public;
```

In questo esempio, sostituisci il segnaposto `<db_name>` con il nome del database.

In PostgreSQL, solo il proprietario di uno schema o un `superuser` può rilasciare uno schema. Il proprietario può rilasciare uno schema e tutti gli oggetti inclusi, anche se il proprietario dello schema non è proprietario di alcuni degli oggetti.

Quando si utilizzano utenti diversi per convertire e applicare schemi diversi al database di destinazione, è possibile che venga visualizzato un messaggio di errore quando la conversione

dello schema DMS non è in grado di eliminare uno schema. Per evitare questo messaggio di errore, utilizza il ruolo `superuser`.

Utilizzo di un cluster Amazon Redshift come destinazione nella conversione dello schema DMS

È possibile utilizzare i database Amazon Redshift come destinazione della migrazione nella conversione dello schema DMS. Per informazioni sui database di destinazione supportati, consulta [Provider di dati di destinazione per la conversione dello schema DMS](#).

Privilegi per Amazon Redshift come destinazione

L'utilizzo di Amazon Redshift come destinazione per la conversione dello schema DMS richiede i seguenti privilegi:

- `CREATE ON DATABASE`: consente a DMS di creare nuovi schemi nel database.
- `CREATE ON SCHEMA`: consente a DMS di creare oggetti nello schema del database.
- `GRANT USAGE ON LANGUAGE`: consente a DMS di creare nuove funzioni e procedure nel database.
- `GRANT SELECT ON ALL TABLES IN SCHEMA pg_catalog`: fornisce al sistema dell'utente le informazioni sul cluster Amazon Redshift.
- `GRANT SELECT ON pg_class_info`: fornisce all'utente le informazioni sullo stile di distribuzione delle tabelle.

È possibile utilizzare il seguente esempio di codice per creare un utente del database e assegnare le autorizzazioni. Sostituisci i valori di esempio con i tuoi valori.

```
CREATE USER user_name PASSWORD your_password;  
GRANT CREATE ON DATABASE db_name TO user_name;  
GRANT CREATE ON SCHEMA schema_name TO user_name;  
GRANT USAGE ON LANGUAGE plpythonu TO user_name;  
GRANT USAGE ON LANGUAGE plpgsql TO user_name;  
GRANT SELECT ON ALL TABLES IN SCHEMA pg_catalog TO user_name;  
GRANT SELECT ON pg_class_info TO user_name;  
GRANT SELECT ON sys_serverless_usage TO user_name;  
GRANT SELECT ON pg_database_info TO user_name;  
GRANT SELECT ON pg_statistic TO user_name;
```

Ripeti l'operazione `GRANT CREATE ON SCHEMA` per ogni schema di destinazione in cui applichi il codice convertito o esegui la migrazione dei dati.

Puoi applicare un pacchetto di estensione al database Amazon Redshift di destinazione. Un pacchetto di estensione è un modulo aggiuntivo che emula le funzioni del database di origine che sono necessarie per la conversione degli oggetti in Amazon Redshift. Per ulteriori informazioni, consulta [Utilizzo dei pacchetti di estensione nella conversione dello schema DMS](#).

Gestione dei progetti di migrazione nella conversione dello schema DMS

Dopo aver creato un profilo dell'istanza e fornitori di dati compatibili per la conversione dello schema, puoi creare un progetto di migrazione. Per ulteriori informazioni, consulta [Creazione di progetti di migrazione](#).

Per utilizzare questo nuovo progetto nella conversione dello schema DMS, scegli il progetto dall'elenco nella pagina Progetti di migrazione. Successivamente, nella scheda Conversione dello schema, scegli Avvia conversione dello schema.

Il primo avvio della conversione dello schema DMS richiede alcune configurazioni. AWS Database Migration Service (AWS DMS) avvia un'istanza di conversione dello schema che richiede fino a 15 minuti. Questo processo legge anche i metadati dai database di origine e di destinazione. Una volta completato correttamente il primo avvio, puoi accedere più rapidamente alla conversione dello schema DMS.

Amazon interrompe l'istanza di conversione dello schema utilizzata dal progetto di migrazione entro tre giorni dal completamento del progetto. Puoi recuperare lo schema convertito e il report di valutazione dal bucket Amazon S3 che usi per la conversione dello schema DMS.

Specificazione delle impostazioni del progetto di migrazione per la conversione dello schema DMS

Dopo aver creato il progetto di migrazione e avviato la conversione dello schema, puoi specificare le impostazioni del progetto di migrazione. Puoi modificare le impostazioni di conversione per migliorare le prestazioni del codice convertito. Inoltre, puoi personalizzare la vista della conversione dello schema.

Le impostazioni di conversione dipendono dalle piattaforme di database di origine e di destinazione. Per ulteriori informazioni, consulta [Creazione di fornitori di dati di origine](#) e [Creazione di fornitori di dati di destinazione](#).

Per specificare gli schemi e i database che desideri visualizzare nei riquadri del database di origine e di destinazione, utilizza le impostazioni della vista ad albero. Puoi nascondere schemi vuoti, database vuoti, database di sistema, oltre a database o schemi definiti dall'utente.

Nascondere database e schemi nella visualizzazione ad albero

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione e nella scheda Conversione dello schema seleziona Avvia conversione dello schema.
4. Seleziona Impostazioni. Viene visualizzata la pagina Impostazioni.
5. Nella sezione Vista ad albero procedi nel seguente modo:
 - Scegli Nascondi schemi vuoti per nascondere gli schemi vuoti.
 - Scegli Nascondi database vuoti per nascondere i database vuoti.
 - In Database o schemi di sistema seleziona i database e gli schemi di sistema per nome per nasconderli.
 - Per Database o schemi definiti dall'utente immetti i nomi degli schemi e dei database definiti dall'utente che intendi nascondere. Scegli Aggiungi. I nomi non fanno distinzione tra maiuscole e minuscole.

Per aggiungere più database o schemi, usa una virgola per separare i nomi. Per aggiungere più oggetti con un nome simile, utilizza il simbolo di percentuale (%) come carattere jolly. Questo carattere jolly sostituisce qualsiasi numero di simboli nel nome del database o dello schema.

Ripeti questi passaggi per le sezioni Origine e Destinazione.

6. Seleziona Applica, quindi scegli Conversione dello schema.

Creazione di report di valutazione della migrazione del database con la conversione dello schema DMS

Una parte importante della conversione dello schema DMS è il report che genera per aiutarti a eseguire l'operazione. Questo report di valutazione della migrazione del database riassume tutte le attività di conversione dello schema. Inoltre, descrive in dettaglio gli elementi d'azione dello schema che non possono essere convertiti nel motore di database dell'istanza database di destinazione. È possibile visualizzare il report nella console AWS DMS o salvarne una copia come file PDF o CSV (valori separati da virgole).

Il report di valutazione della migrazione include i seguenti elementi:

- Sintesi esecutiva
- Raccomandazioni, incluse conversione di oggetti server, suggerimenti di backup e modifiche al server collegato

Se ci sono elementi che la conversione dello schema DMS non è in grado di convertire automaticamente, il report fornisce la stima dell'impegno necessario per scrivere il codice equivalente per l'istanza database di destinazione.

Argomenti

- [Creazione di un report di valutazione della migrazione del database](#)
- [Visualizzazione del report di valutazione della migrazione del database](#)
- [Salvataggio del report di valutazione della migrazione del database](#)

Creazione di un report di valutazione della migrazione del database

Dopo aver creato un progetto di migrazione, utilizza la procedura seguente per creare un report di valutazione della migrazione del database.

Creazione di un report di valutazione della migrazione del database

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Conversione dello schema.

4. Scegli **Avvia conversione dello schema**. Viene visualizzata la pagina **Conversione dello schema**.
5. Nel riquadro del database di origine, scegli lo schema o gli elementi dello schema del database che desideri valutare. Per includere più oggetti nel report, assicurati di selezionare tutti gli elementi.
6. Dopo aver selezionato le caselle di controllo per tutti gli oggetti dello schema che vuoi valutare, dovrai scegliere il nodo principale per gli oggetti selezionati. Il menu **Operazioni** nel riquadro del database di origine è ora disponibile.
7. Nel menu **Operazioni** scegli **Valuta**. Viene visualizzata una finestra di dialogo di conferma.
8. Seleziona **Valuta** nella finestra di dialogo per confermare la scelta.

Visualizzazione del report di valutazione della migrazione del database

Dopo aver creato un report di valutazione, la conversione dello schema DMS aggiunge informazioni nelle seguenti schede:

- Riepilogo
- Elementi d'azione

La scheda **Riepilogo** mostra il numero di elementi che la conversione dello schema DMS può convertire automaticamente.

La scheda **Elementi d'azione** mostra gli elementi che la conversione dello schema DMS non è in grado di convertire automaticamente e fornisce consigli su come gestirli.

Riepilogo del report di valutazione

Nella scheda **Summary (Riepilogo)** vengono visualizzate le informazioni di riepilogo del report di valutazione della migrazione del database. Mostra il numero di elementi che la conversione dello schema DMS può convertire automaticamente in oggetti di archiviazione del database e oggetti di codice del database.

Nella maggior parte dei casi, la conversione dello schema DMS non è in grado di convertire automaticamente tutti gli elementi dello schema nel motore di database di destinazione. La scheda **Riepilogo** include una stima dell'impegno necessario per creare elementi dello schema nella istanza database di destinazione che siano equivalenti a quelli presenti nell'origine.

Per visualizzare il riepilogo della conversione per gli oggetti di archiviazione del database come tabelle, sequenze, vincoli, tipi di dati e così via, scegli Oggetti di archiviazione database.

Per visualizzare il riepilogo delle conversioni per gli oggetti di codice del database come procedure, funzioni, viste, trigger e così via, scegli Oggetti codice database.

Per modificare l'ambito del report di valutazione, seleziona il nodo richiesto nell'albero del database di origine. La conversione dello schema DMS aggiorna il riepilogo del report di valutazione in modo che corrisponda all'ambito selezionato.

Elementi d'azione del report di valutazione

La scheda Elementi d'azione include un elenco di elementi che la conversione dello schema DMS non può convertire automaticamente in un formato compatibile con il motore di database di destinazione. Per ogni elemento d'azione, la conversione dello schema DMS fornisce la descrizione del problema e l'azione consigliata. La conversione dello schema DMS raggruppa elementi d'azione simili e visualizza il numero di ricorrenze.

Per visualizzare il codice dell'oggetto di database correlato, seleziona un elemento d'azione nell'elenco.

Salvataggio del report di valutazione della migrazione del database

Dopo aver creato un report di valutazione della migrazione del database, puoi salvarne una copia come PDF o file CSV (valori separati da virgole).

Per salvare il report di valutazione della migrazione del database come file PDF

1. Seleziona Esporta, quindi scegli PDF. Esamina la finestra di dialogo e scegli Esporta in PDF.
2. La conversione dello schema DMS crea un archivio con il file PDF e lo memorizza nel tuo bucket Amazon S3. Per modificare il bucket Amazon S3, modifica le impostazioni di conversione dello schema nel profilo dell'istanza.
3. Apri il file del report di valutazione nel bucket Amazon S3.

Per salvare un report di valutazione della migrazione del database come file CSV

1. Seleziona Esporta, quindi scegli CSV. Esamina la finestra di dialogo e scegli Esporta in CSV.

2. La conversione dello schema DMS crea un archivio con i file CSV e lo memorizza nel tuo bucket Amazon S3. Per modificare il bucket Amazon S3, modifica le impostazioni di conversione dello schema nel profilo dell'istanza.
3. Apri i file del report di valutazione nel bucket Amazon S3.

Il file PDF contiene sia il riepilogo, sia le informazioni sulle attività.

Quando esporti il report di valutazione in formato CSV, la conversione dello schema DMS crea tre file CSV.

Il primo file CSV contiene le seguenti informazioni relative agli elementi d'azione:

- Categoria
- Ricorrenza
- Elemento d'azione
- Subject
- Group (Gruppo)
- Descrizione
- Riferimenti della documentazione
- Azione consigliata
- Line (Linea)
- Posizione
- Origine
- Target
- Indirizzo IP e porta del server
- Database
- Schema

Il secondo file CSV include il suffisso `Action_Items_Summary` nel nome e contiene le seguenti informazioni:

- Schema
- Elemento d'azione

- Numero di ricorrenze
- Impegno della curva di apprendimento, ossia la quantità di impegno richiesta per progettare un approccio alla conversione di ogni elemento d'azione
- Impegni per convertire una ricorrenza dell'elemento d'azione, che mostra l'impegno richiesto per convertire ogni elemento d'azione, seguendo l'approccio progettato
- Descrizione dell'elemento d'azione
- Azione consigliata

I valori che indicano il livello di impegno richiesto si basano su una scala ponderata che va da basso (minimo) ad alto (massimo).

Il terzo file CSV include Summary nel nome e contiene le seguenti informazioni:

- Categoria
- Numero di oggetti
- Oggetti convertiti automaticamente
- Oggetti con azioni semplici
- Oggetti con azioni di media complessità
- Oggetti con azioni complesse
- Righe di codice totali

Utilizzo della conversione dello schema DMS

La conversione dello schema DMS converte gli schemi di database esistenti e la maggior parte degli oggetti di codice del database in un formato compatibile con il database di destinazione.

La conversione dello schema DMS automatizza gran parte del processo di conversione degli schemi di database OLTP (Online Transaction Processing) in Amazon RDS per MySQL o RDS per PostgreSQL. I motori di database di origine e di destinazione contengono diverse funzionalità e capacità la conversione dello schema DMS tenta di creare uno schema equivalente, se possibile. Per gli oggetti di database in cui non è possibile la conversione diretta, la conversione dello schema DMS fornisce un elenco di azioni da intraprendere.

Per convertire lo schema di database, utilizza la procedura seguente:

- Prima di convertire gli schemi di database, imposta le regole di trasformazione che modificano i nomi degli oggetti di database durante la conversione.
- Crea un report di valutazione della migrazione del database per stimare la complessità della migrazione. Questo report fornisce i dettagli sugli elementi dello schema che la conversione dello schema DMS non è in grado di convertire automaticamente.
- Converti l'archiviazione e gli oggetti di codice del database di origine. La conversione dello schema DMS crea una versione locale degli oggetti di database convertiti. È possibile accedere agli oggetti convertiti nel progetto di migrazione.
- Salva il codice convertito in file SQL per rivedere, modificare o risolvere le azioni di conversione. Facoltativamente, applica il codice convertito direttamente al database di destinazione.

Per convertire gli schemi di data warehouse, usa il desktop AWS Schema Conversion Tool. Per ulteriori informazioni, consulta [Converting data warehouse schemas to Amazon Redshift](#) nella Guida per l'utente di AWS Schema Conversion Tool.

Argomenti

- [Configurazione delle regole di trasformazione nella conversione dello schema DMS](#)
- [Conversione degli schemi di database nella conversione dello schema DMS](#)
- [Specifica delle impostazioni di conversione dello schema per i progetti di migrazione](#)
- [Aggiornamento degli schemi di database nella conversione dello schema DMS](#)
- [Salvataggio e applicazione del codice convertito nella conversione dello schema DMS](#)

Configurazione delle regole di trasformazione nella conversione dello schema DMS

Prima di convertire lo schema di database con la conversione dello schema DMS, puoi impostare le regole di trasformazione. Le regole di trasformazione possono eseguire operazioni come modificare il nome di un oggetto in minuscolo o maiuscolo, aggiungere o rimuovere un prefisso o un suffisso e rinominare gli oggetti. Supponi, ad esempio, di avere una serie di tabelle nello schema di origine denominato `test_TABLE_NAME`. Puoi impostare una regola che modifichi il prefisso `test_` con il prefisso `demo_` nello schema di destinazione.

Puoi creare regole di trasformazione in grado di eseguire le seguenti attività:

- Aggiunta, rimozione o sostituzione di un prefisso

- Aggiunta, rimozione o sostituzione di un suffisso
- Modifica del tipo di dati di una colonna
- Modifica del nome dell'oggetto in lettere minuscole o maiuscole
- Rinominare oggetti

Puoi creare regole di trasformazione per i seguenti oggetti:

- Schema
- Tabella
- Colonna

Creazione delle regole di trasformazione

La conversione dello schema DMS memorizza le regole di trasformazione come parte del progetto di migrazione. Puoi impostare le regole di trasformazione quando crei il progetto di migrazione o modificarle in un secondo momento.

Puoi aggiungere più regole di trasformazione nel progetto. La conversione dello schema DMS applica le regole di trasformazione durante la conversione nello stesso ordine in cui le hai aggiunte.

Per creare le regole di trasformazione

1. Nella pagina Crea un progetto di migrazione scegli Aggiungi regola di trasformazione. Per ulteriori informazioni, consulta [Creazione di progetti di migrazione](#).
2. Per Destinazione della regola scegli il tipo di oggetti di database a cui si applica la regola.
3. Per Schema di origine scegli Inserisci uno schema. Quindi, inserisci i nomi degli schemi di origine, delle tabelle e delle colonne a cui si applica questa regola. Puoi inserire un nome esatto per selezionare un solo oggetto, oppure puoi inserire un modello per selezionare più oggetti. Utilizza il simbolo di percentuale (%) come carattere jolly per sostituire qualsiasi numero di simboli nel nome dell'oggetto del database.
4. In Operazione scegli l'attività da eseguire.
5. A seconda del tipo di regola, immetti uno o due valori aggiuntivi. Ad esempio, per rinominare un oggetto immetti il nuovo nome dell'oggetto. Per sostituire un prefisso immetti il prefisso precedente e quello nuovo.
6. Scegli Aggiungi regola di trasformazione per aggiungere un'altra regola di trasformazione.

Dopo aver aggiunto le regole, scegli Crea un progetto di migrazione.

Per duplicare una regola di trasformazione esistente scegli Duplica. Per modificare una regola di trasformazione esistente scegli la regola dall'elenco. Per eliminare una regola di trasformazione esistente scegli Rimuovi.

Modifica delle regole di trasformazione

Puoi aggiungere nuove regole di trasformazione, rimuovere o modificare quelle esistenti nel tuo progetto di migrazione. Poiché la conversione dello schema DMS applica le regole di trasformazione durante l'avvio della conversione dello schema, assicurati di chiudere la conversione dello schema e di riavviarla dopo aver modificato le regole.

Per modificare le regole di trasformazione

1. Accedi a e AWS Management Console apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione, quindi seleziona il tuo progetto di migrazione.
3. Scegli Conversione dello schema, quindi seleziona Chiudi conversione dello schema.
4. Dopo aver AWS DMS chiuso la conversione dello schema, scegli Modifica per modificare le impostazioni del progetto di migrazione.
5. Per Regole di trasformazione scegli una delle seguenti azioni:
 - Scegli Duplica per duplicare una regola di trasformazione esistente e aggiungerla alla fine dell'elenco.
 - Scegli Rimuovi per rimuovere una regola di trasformazione esistente.
 - Scegli la regola di trasformazione esistente per modificarla.
6. Dopo aver terminato la modifica delle regole, seleziona Salva modifiche.
7. Nella pagina Progetti di migrazione scegli il tuo progetto dall'elenco. Scegli Conversione dello schema, quindi seleziona Avvia conversione dello schema.

Conversione degli schemi di database nella conversione dello schema DMS

Dopo aver creato il progetto di migrazione e aver effettuato la connessione ai database di origine e di destinazione, è possibile convertire gli oggetti del database di origine in un formato compatibile con

il database di destinazione. La conversione dello schema DMS visualizza lo schema di database di origine nel pannello di sinistra in una visualizzazione ad albero.

Ogni nodo dell'albero del database viene caricato lentamente. Quando scegli un nodo nella visualizzazione ad albero, la conversione dello schema DMS richiede le informazioni sullo schema dal database di origine. Per caricare più velocemente le informazioni sullo schema, scegli lo schema desiderato, quindi seleziona Carica metadati dal menu Operazioni. La conversione dello schema DMS legge i metadati del database e archivia le informazioni in un bucket Amazon S3. A questo punto puoi sfogliare gli oggetti del database più velocemente.

È possibile convertire l'intero schema di database oppure scegliere qualsiasi elemento dello schema da convertire dal database di origine. Se l'elemento dello schema scelto dipende da un elemento padre, la conversione dello schema DMS genera anche lo schema per detto elemento. Ad esempio, quando si sceglie una tabella da convertire, la conversione dello schema DMS crea la tabella convertita e lo schema di database in cui si trova la tabella.

Conversione degli oggetti di database

È possibile utilizzare la conversione dello schema DMS per convertire un intero schema di database o oggetti dello schema di database separati.

Per convertire un intero schema di database

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Conversione dello schema.
4. Scegli Avvia conversione dello schema. Viene visualizzata la pagina Conversione dello schema.
5. Nel riquadro del database di origine, seleziona la casella di controllo relativa al nome dello schema.
6. Scegli questo schema nel riquadro sinistro del progetto di migrazione. La conversione dello schema DMS evidenzia il nome dello schema in blu e attiva il menu Operazioni.
7. Per Operazioni scegli Converti. Viene visualizzata la finestra di dialogo di conversione.
8. Seleziona Converti nella finestra di dialogo per confermare la scelta.

Per convertire gli oggetti del database di origine

1. Accedi a e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/). AWS Management Console
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Conversione dello schema.
4. Scegli Avvia conversione dello schema. Viene visualizzata la pagina Conversione dello schema.
5. Nel riquadro del database di origine, seleziona gli oggetti del database di origine.
6. Dopo aver selezionato tutte le caselle di controllo per gli oggetti che desideri convertire, scegli il nodo padre per tutti gli oggetti selezionati nel pannello di sinistra.

La conversione dello schema DMS evidenzia il nodo padre in blu e attiva il menu Operazioni.

7. Per Operazioni scegli Converti. Viene visualizzata la finestra di dialogo di conversione.
8. Seleziona Converti nella finestra di dialogo per confermare la scelta.

Ad esempio, per convertire due tabelle su 10, seleziona le caselle di controllo relative alle due tabelle che desideri convertire. Nota che il menu Operazioni è inattivo. Dopo aver scelto il nodo Tabelle, la conversione dello schema DMS ne evidenzia il nome in blu e attiva il menu Operazioni. Quindi puoi scegliere Converti dal menu.

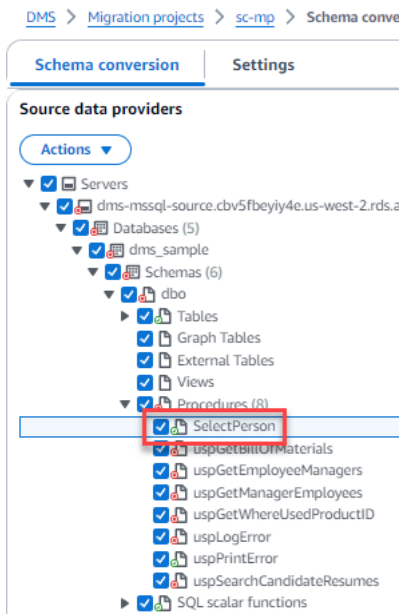
Allo stesso modo, per convertire due tabelle e tre procedure, seleziona le caselle di controllo relative ai nomi degli oggetti. Quindi, scegli il nodo dello schema per attivare il menu Operazioni e seleziona Converti schema.

Modifica e salvataggio del codice SQL convertito

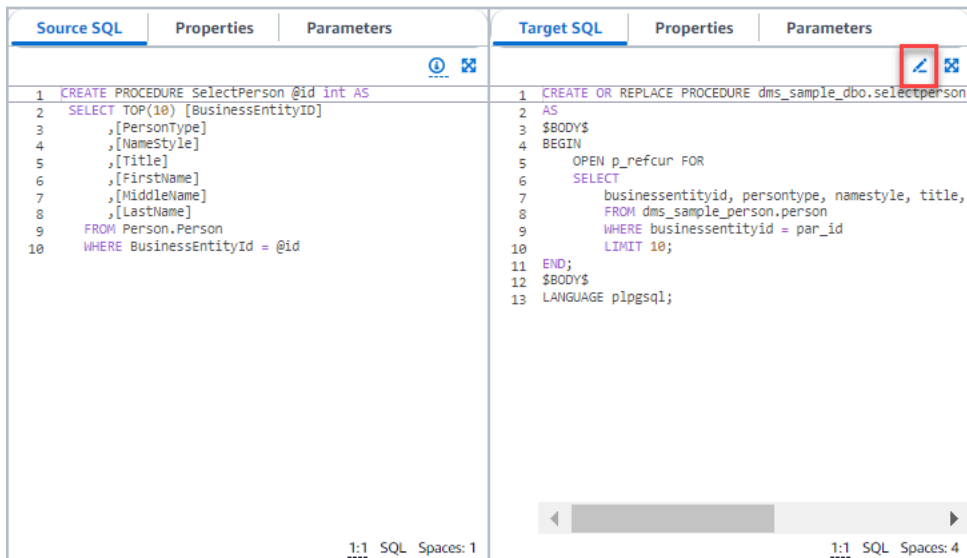
La pagina di conversione dello schema consente di modificare il codice SQL convertito negli oggetti del database. Utilizza la procedura seguente per modificare il tuo codice SQL convertito, per applicare le modifiche e quindi salvarle.

Modifica, applicazione delle modifiche e salvataggio del codice SQL convertito

1. Nella pagina di conversione dello schema, apri la visualizzazione ad albero nel riquadro Provider di dati di origine per visualizzare un oggetto di codice.



2. Dal riquadro Provider di dati di origine, scegli Azioni, Converti. Conferma l'operazione.
3. Al termine della conversione, per visualizzare l'SQL convertito, espandi il riquadro centrale, se necessario. Per modificare l'SQL convertito, scegli l'icona di modifica nel riquadro Target SQL.



4. Dopo aver modificato l'SQL di destinazione, conferma le modifiche scegliendo l'icona di spunta nella parte superiore della pagina. Conferma l'operazione.
5. Nel riquadro dei provider di dati di Target, scegli Azioni, Applica modifiche. Conferma l'operazione.
6. DMS scrive la procedura modificata nell'archivio dati di destinazione.

Audit degli oggetti di database

Dopo aver convertito gli oggetti del database di origine, puoi scegliere un oggetto nel riquadro di sinistra del progetto. È quindi possibile visualizzare il codice sorgente e convertito per quell'oggetto. La conversione dello schema DMS carica automaticamente il codice convertito per l'oggetto selezionato nel riquadro di sinistra. È inoltre possibile visualizzare le proprietà o i parametri dell'oggetto selezionato.

La conversione dello schema DMS memorizza automaticamente il codice convertito come parte del progetto di migrazione. Non applica queste modifiche del codice al database di destinazione. Per ulteriori informazioni sull'applicazione del codice convertito al database di destinazione, consulta [Applicazione del codice convertito](#). Per rimuovere il codice convertito dal progetto di migrazione, seleziona lo schema di destinazione nel riquadro a destra, quindi scegli **Aggiorna dal database** nel menu **Operazioni**.

Dopo aver convertito gli oggetti del database di origine, puoi visualizzare il riepilogo della conversione e gli elementi d'azione nel riquadro in basso al centro. Puoi vedere le stesse informazioni se crei un report di valutazione. Il report di valutazione è utile per identificare e risolvere gli elementi dello schema che non possono essere convertiti automaticamente dalla conversione dello schema DMS. Puoi salvare il riepilogo del report di valutazione e l'elenco delle azioni di conversione in file CSV. Per ulteriori informazioni, consulta [Report di valutazione della migrazione del database](#).

Specifica delle impostazioni di conversione dello schema per i progetti di migrazione

Dopo aver creato un progetto di migrazione, puoi specificare le impostazioni di conversione nella conversione dello schema DMS. La configurazione delle impostazioni di conversione dello schema migliora le prestazioni del codice convertito.

Per modificare le impostazioni di conversione

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli **Progetti di migrazione**. Viene visualizzata la pagina **Progetti di migrazione**.
3. Scegli il tuo progetto di migrazione. Scegli **Conversione dello schema**, quindi seleziona **Avvia conversione dello schema**.
4. Seleziona **Impostazioni**. Viene visualizzata la pagina **Impostazioni**.

5. Modifica le impostazioni nella sezione Conversione.
6. Seleziona Applica, quindi scegli Conversione dello schema.

Per tutte le coppie di conversione, puoi limitare il numero di commenti con elementi d'azione nel codice convertito. Per limitare il numero di commenti nel codice convertito, apri le impostazioni di conversione nel progetto di migrazione.

Per Commenti nel codice SQL convertito scegli il livello di gravità degli elementi d'azione. La conversione dello schema DMS aggiunge i commenti nel codice convertito per gli elementi d'azione con la gravità selezionata o superiore. Ad esempio, per ridurre al minimo il numero di commenti nel codice convertito, scegli Solo errori.

Per includere commenti per tutti gli elementi d'azione nel codice convertito, scegli Tutti i messaggi.

Le altre impostazioni di conversione sono diverse per ogni coppia di database di origine e di destinazione.

Argomenti

- [Impostazioni di conversione da Oracle a MySQL](#)
- [Impostazioni di conversione da Oracle a PostgreSQL](#)
- [Impostazioni di conversione da SQL Server a MySQL](#)
- [Impostazioni di conversione da SQL Server a PostgreSQL](#)
- [Impostazioni di conversione da PostgreSQL a MySQL](#)
- [Impostazioni di conversione da DB2 for z/OS a DB2 LUW](#)

Impostazioni di conversione da Oracle a MySQL

Le impostazioni di conversione da Oracle a MySQL nella conversione dello schema DMS sono le seguenti:

- Il database Oracle di origine può utilizzare la pseudo colonna ROWID. MySQL non supporta funzionalità simili. La conversione dello schema DMS può emulare la pseudo colonna ROWID nel codice convertito. A tale scopo, attiva l'opzione Genera ID riga.

Se il codice Oracle sorgente non utilizza la pseudo colonna ROWID, disattiva l'opzione Genera ID riga. In questo caso, il codice convertito funziona più velocemente.

- Il codice sorgente Oracle può includere le funzioni TO_CHAR, TO_DATE e TO_NUMBER con parametri non supportati da MySQL. Per impostazione predefinita, la conversione dello schema DMS emula l'utilizzo di questi parametri nel codice convertito.

È possibile utilizzare le funzioni TO_CHAR, TO_DATE e TO_NUMBER native di MySQL quando il codice sorgente Oracle non ha parametri non supportati da MySQL. In questo caso, il codice convertito funziona più velocemente. Per farlo, seleziona i seguenti valori:

- Usa una funzione MySQL TO_CHAR nativa
- Usa una funzione MySQL TO_DATE nativa
- Usa una funzione MySQL TO_NUMBER nativa
- Il database e le applicazioni possono essere eseguiti in fusi orari diversi. Per impostazione predefinita, la conversione dello schema DMS emula i fusi orari nel codice convertito. Tuttavia, non è necessaria questa emulazione quando il database e le applicazioni utilizzano lo stesso fuso orario. In tal caso, seleziona Migliora le prestazioni del codice convertito se il database e le applicazioni utilizzano lo stesso fuso orario.

Impostazioni di conversione da Oracle a PostgreSQL

Le impostazioni di conversione da Oracle a PostgreSQL nella conversione dello schema DMS sono le seguenti:

- AWS DMS può convertire le viste materializzate Oracle in tabelle o viste materializzate su PostgreSQL. Per Viste materializzate scegli come convertire le viste materializzate di origine.
- Il database Oracle di origine può utilizzare la pseudo colonna ROWID. PostgreSQL non supporta funzionalità simili. La conversione dello schema DMS può emulare la pseudo colonna ROWID nel codice convertito utilizzando il tipo di dati bigint o character varying. Per farlo, scegli Usa il tipo di dati bigint per emulare la pseudo colonna ROWID o Usa il tipo di dati varchar per emulare la pseudo colonna ROWID per ID riga.

Se il codice sorgente Oracle non utilizza la pseudo colonna ROWID scegli Non generare. In questo caso, il codice convertito funziona più velocemente.

- Il codice sorgente Oracle può includere le funzioni TO_CHAR, TO_DATE e TO_NUMBER con parametri non supportati da PostgreSQL. Per impostazione predefinita, la conversione dello schema DMS emula l'utilizzo di questi parametri nel codice convertito.

È possibile utilizzare le funzioni TO_CHAR, TO_DATE e TO_NUMBER native di PostgreSQL quando il codice sorgente Oracle non ha parametri non supportati da PostgreSQL. In questo caso, il codice convertito funziona più velocemente. Per farlo, seleziona i seguenti valori:

- Usa una funzione PostgreSQL TO_CHAR nativa
- Usa una funzione PostgreSQL TO_DATE nativa
- Usa una funzione PostgreSQL TO_NUMBER nativa
- Il database e le applicazioni possono essere eseguiti in fusi orari diversi. Per impostazione predefinita, la conversione dello schema DMS emula i fusi orari nel codice convertito. Tuttavia, non è necessaria questa emulazione quando il database e le applicazioni utilizzano lo stesso fuso orario. In tal caso, seleziona Migliora le prestazioni del codice convertito se il database e le applicazioni utilizzano lo stesso fuso orario.
- Per continuare a utilizzare le sequenze nel codice convertito, seleziona Popola le sequenze convertite con l'ultimo valore generato sul lato di origine.
- In alcuni casi, il database Oracle di origine potrebbe archiviare solo valori interi nelle colonne con chiave primaria o esterna del tipo di dati NUMBER. In questi casi, AWS DMS può convertire queste colonne nel tipo di dati BIGINT. Questo approccio migliora le prestazioni del codice convertito. A tale scopo, seleziona Converti le colonne chiave primaria ed esterna del tipo di dati NUMBER nel tipo di dati BIGINT. Assicurati che l'origine non includa valori con virgola mobile in queste colonne per evitare la perdita di dati.
- Per ignorare i trigger e i vincoli disattivati nel codice sorgente, scegli Converti solo i trigger e i vincoli attivi.
- Puoi utilizzare la conversione dello schema DMS per convertire le variabili di stringa chiamate come SQL dinamico. Il codice del database può modificare i valori di queste variabili di stringa. Per assicurarti che converta AWS DMS sempre il valore più recente di questa variabile di stringa, seleziona Converti il codice SQL dinamico creato nelle routine chiamate.
- PostgreSQL 10 e versioni precedenti non supportano le procedure. Se non hai familiarità con l'uso delle procedure in PostgreSQL AWS DMS, puoi convertire le procedure Oracle in funzioni PostgreSQL. A tale scopo, seleziona Converti procedure in funzioni.
- Per visualizzare informazioni aggiuntive sugli elementi d'azione eseguiti, è possibile aggiungere funzioni specifiche al pacchetto di estensione. A tale scopo, seleziona Aggiungi funzioni del pacchetto di estensione che generano eccezioni definite dall'utente. Quindi scegli i livelli di gravità per generare le eccezioni definite dall'utente. Assicurati di applicare lo schema del pacchetto di estensione dopo aver convertito gli oggetti del database di origine. Per ulteriori informazioni sui pacchetti di estensione, consulta [Utilizzo dei pacchetti di estensione](#).

- Il database Oracle di origine può includere vincoli per i nomi generati automaticamente. Se il codice sorgente utilizza questi nomi, assicurati di selezionare **Mantieni i nomi dei vincoli generati dal sistema**. Se il codice sorgente utilizza questi vincoli, ma non ne usa i nomi, **deseleziona** questa opzione per aumentare la velocità di conversione.
- Se i database di origine e di destinazione vengono eseguiti in fusi orari diversi, la funzione che emula la funzione integrata Oracle SYSDATE restituisce valori diversi rispetto alla funzione di origine. Per assicurarti che le funzioni di origine e di destinazione restituiscano gli stessi valori, scegli **Imposta il fuso orario del database di origine**.
- Puoi utilizzare le funzioni dell'estensione orafce nel codice convertito. Per farlo, seleziona le funzioni da usare per **Routine integrate Orafce**. [Per ulteriori informazioni su orafce, vedere orafce on. GitHub](#)

Impostazioni di conversione da SQL Server a MySQL

Le impostazioni di conversione da SQL Server a MySQL nella conversione dello schema DMS sono le seguenti:

- Il database SQL Server di origine può memorizzare l'output di EXEC in una tabella. La conversione dello schema DMS crea tabelle temporanee e una procedura aggiuntiva per emulare questa funzionalità. Per utilizzare l'emulazione, seleziona **Crea routine aggiuntive per gestire set di dati aperti**.

Impostazioni di conversione da SQL Server a PostgreSQL

Le impostazioni di conversione da SQL Server a PostgreSQL nella conversione dello schema DMS sono le seguenti:

- In SQL Server puoi usare indici con lo stesso nome in tabelle diverse. Tuttavia, in PostgreSQL tutti i nomi di indice utilizzati nello schema devono essere univoci. Per assicurarti che la conversione dello schema DMS generi nomi univoci per tutti gli indici, seleziona **Genera nomi univoci per gli indici**.
- PostgreSQL 10 e versioni precedenti non supportano le procedure. Se non hai familiarità con l'uso delle procedure in PostgreSQL AWS DMS , puoi convertire le procedure di SQL Server in funzioni PostgreSQL. A tale scopo, seleziona **Converti procedure in funzioni**.
- Il database SQL Server di origine può memorizzare l'output di EXEC in una tabella. La conversione dello schema DMS crea tabelle temporanee e una procedura aggiuntiva per emulare questa

funzionalità. Per utilizzare l'emulazione, seleziona Crea routine aggiuntive per gestire set di dati aperti.

- È possibile definire il modello da utilizzare per i nomi degli schemi nel codice convertito. Per Nomi degli schemi scegli una delle seguenti opzioni:
 - DB: utilizza il nome del database SQL Server come nome dello schema in PostgreSQL.
 - SCHEMA: utilizza il nome dello schema SQL Server come nome dello schema in PostgreSQL.
 - DB_SCHEMA: utilizza una combinazione del database SQL Server e dei nomi degli schemi come nome dello schema in PostgreSQL.
- È possibile mantenere le lettere maiuscole e minuscole dei nomi degli oggetti di origine. Per evitare la conversione dei nomi degli oggetti in lettere minuscole, seleziona Mantieni i nomi degli oggetti nello stesso carattere. Questa opzione si applica solo quando si attiva l'opzione per la distinzione tra maiuscole e minuscole nel database di destinazione.
- È possibile mantenere i nomi dei parametri del database di origine. La conversione dello schema DMS può aggiungere le virgolette doppie ai nomi dei parametri nel codice convertito. A tale scopo, seleziona Conserva i nomi originali dei parametri.
- È possibile mantenere una serie di parametri di routine del database di origine. La conversione dello schema DMS crea i domini e li utilizza per specificare la lunghezza dei parametri di routine. A tale scopo, seleziona Preserva la lunghezza dei parametri.

Impostazioni di conversione da PostgreSQL a MySQL

Le impostazioni di conversione da PostgreSQL a MySQL in DMS Schema Conversion includono quanto segue:

- Commenti nel codice SQL convertito: questa impostazione include i commenti nel codice convertito per le azioni con il livello di gravità selezionato o superiore. Questa impostazione supporta i seguenti valori:
 - Solo errori
 - Errori e avvertenze
 - Tutti i messaggi

Impostazioni di conversione da DB2 for z/OS a DB2 LUW

Le impostazioni di conversione da DB2 for z/OS a DB2 LUW in DMS Schema Conversion includono quanto segue:

- Commenti nel codice SQL convertito: questa impostazione include i commenti nel codice convertito per le azioni con il livello di gravità selezionato o superiore. Questa impostazione supporta i seguenti valori:
 - Solo errori
 - Errori e avvertenze
 - Tutti i messaggi

Aggiornamento degli schemi di database nella conversione dello schema DMS

Dopo aver creato un progetto di migrazione, la conversione dello schema DMS vi archivia le informazioni sugli schemi di origine e di destinazione. La conversione dello schema DMS utilizza il caricamento lento per caricare i metadati solo quando è necessario, ad esempio quando si sceglie un nodo nell'albero del database. È possibile utilizzare il caricamento rapido per caricare più velocemente le informazioni dello schema. Per farlo, scegli lo schema, quindi seleziona Carica metadati nel menu Operazioni.

Dopo aver caricato automaticamente o manualmente l'oggetto nel progetto di migrazione, la conversione dello schema DMS non utilizza più il caricamento lento. Pertanto, quando modifichi gli oggetti come tabelle e procedure nel database, assicurati di aggiornarli nel progetto di migrazione.

Per aggiornare gli schemi dal database, seleziona gli oggetti che desideri aggiornare e scegli Aggiorna dal database nel menu Operazioni. È possibile aggiornare gli oggetti di database negli schemi di database di origine e di destinazione:

- Origine: se aggiorni lo schema del database di origine, scegli Aggiorna dal database per sostituire lo schema del progetto con lo schema più recente dal database di origine.
- Destinazione: se aggiorni lo schema per il database di destinazione, la conversione dello schema DMS sostituisce lo schema del progetto con lo schema più recente del database di destinazione. La conversione dello schema DMS sostituisce il codice convertito con il codice del database di destinazione. Assicurati di aver applicato il codice convertito al database di destinazione prima di scegliere Aggiorna dal database. In caso contrario, converti nuovamente lo schema del database di origine.

Salvataggio e applicazione del codice convertito nella conversione dello schema DMS

Una volta convertiti gli oggetti del database di origine, la conversione dello schema DMS non applica immediatamente il codice convertito al database di destinazione. La conversione dello schema DMS archivia il codice convertito nel progetto finché non sei pronto per applicarlo al database di destinazione.

Prima di applicare il codice convertito, puoi aggiornare il codice del database di origine e convertire nuovamente gli oggetti aggiornati per eseguire gli elementi d'azione esistenti. Per ulteriori informazioni sugli elementi che non possono essere convertiti automaticamente dalla conversione dello schema DMS, consulta [Creazione di report di valutazione della migrazione del database con la conversione dello schema DMS](#). Per ulteriori informazioni sull'aggiornamento degli oggetti del database di origine nel progetto di migrazione per la conversione dello schema DMS, consulta [Aggiornamento degli schemi di database](#).

Anziché applicare il codice convertito direttamente al database nella conversione dello schema DMS, è possibile salvare il codice in un file come script SQL. Puoi esaminare questi script SQL, modificarli se necessario e quindi applicarli manualmente al database di destinazione.

Salvataggio del codice convertito in un file SQL

Puoi salvare lo schema convertito come script SQL in un file di testo. È possibile modificare il codice convertito per eseguire gli elementi d'azione che la conversione dello schema DMS non è in grado di convertire automaticamente. Puoi quindi eseguire gli script SQL aggiornati nel database di destinazione per applicare il codice convertito al database di destinazione.

Per salvare lo schema convertito come script SQL

1. Accedere AWS Management Console e aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Conversione dello schema.
4. Scegli Avvia conversione dello schema. Viene visualizzata la pagina Conversione dello schema.
5. Nel riquadro di destra, scegli lo schema del database di destinazione o seleziona gli oggetti convertiti che desideri salvare. Assicurati che la conversione dello schema DMS evidenzi il nome del nodo padre in blu e attivi il menu Operazioni per il database di destinazione.

6. Scegli Salva come SQL per Operazioni. Viene visualizzata la finestra di dialogo Salva.
7. Scegli Salva come SQL per confermare la scelta.

La conversione dello schema DMS crea un archivio con i file SQL e lo memorizza nel tuo bucket Amazon S3.

8. (Facoltativo) Cambia il bucket S3 per l'archivio modificando le impostazioni di conversione dello schema nel profilo dell'istanza.
9. Apri gli script SQL dal tuo bucket S3.

Applicazione del codice convertito

Quando sei pronto per applicare il codice convertito al database destinazione, scegli gli oggetti del database nel riquadro a destra del progetto. È possibile applicare le modifiche a un intero schema di database o a oggetti selezionati dello schema di database.

Dopo aver selezionato gli oggetti del database, la conversione dello schema DMS evidenzia in blu il nome del nodo selezionato o del nodo padre. Quindi, attiva il menu Operazioni. Scegli Applica le modifiche per Operazioni. Nella finestra di dialogo che viene visualizzata, scegli Applica per confermare la scelta e applicare il codice convertito al database di destinazione.

Applicazione dello schema del pacchetto di estensione

Quando applichi lo schema convertito al database di destinazione per la prima volta, la conversione dello schema DMS potrebbe applicare anche lo schema del pacchetto di estensione. Lo schema del pacchetto di estensione emula le funzioni di sistema del database di origine necessarie per eseguire il codice convertito per il database di destinazione. Se il codice convertito utilizza le funzioni del pacchetto di estensione, assicurati di applicare lo schema del pacchetto di estensione.

Per applicare manualmente il pacchetto di estensione al database di destinazione, scegli Applica le modifiche per Operazioni. Nella finestra di dialogo che viene visualizzata, scegli Conferma per applicare il pacchetto di estensione al database di destinazione.

Ti consigliamo di non modificare lo schema del pacchetto di estensione per evitare risultati imprevisti nel codice convertito.

Per ulteriori informazioni, consulta [Utilizzo dei pacchetti di estensione nella conversione dello schema DMS](#).

Utilizzo dei pacchetti di estensione nella conversione dello schema DMS

Un pacchetto di estensione nella conversione dello schema DMS è un modulo aggiuntivo che emula le funzioni del database di origine che non sono supportate nel database di destinazione. Utilizza un pacchetto di estensione per assicurarti che il codice convertito produca gli stessi risultati del codice sorgente. Prima di installare il pacchetto di estensione è necessario convertire lo schema del database.

Ogni pacchetto di estensione include uno schema di database. Questo schema comprende funzioni, procedure, tabelle e viste SQL per emulare oggetti OLTP (Online Transaction Processing, elaborazione di transazioni online) specifici o funzioni integrate non supportate dal database di origine.

Quando converti il database di origine, la conversione dello schema DMS aggiunge uno schema al database di destinazione. Questo schema implementa le funzioni di sistema SQL del database di origine richieste per eseguire il codice convertito sul database di destinazione. Lo schema aggiuntivo viene chiamato schema del pacchetto di estensione.

Lo schema del pacchetto di estensione viene denominato in base al database di origine come segue:

- Microsoft SQL Server – `aws_sqlserver_ext`
- Oracle – `aws_oracle_ext`

Puoi applicare i pacchetti di estensione in due modi:

- La conversione dello schema DMS può implementare automaticamente un pacchetto di estensione quando applichi il codice convertito. La conversione dello schema DMS usa il pacchetto di estensione prima di applicare tutti gli altri oggetti dello schema.
- È possibile applicare un pacchetto di estensione manualmente. A tale scopo, scegli lo schema del pacchetto di estensione nell'albero del database di destinazione, quindi seleziona **Applica** e **Applica pacchetto di estensione**.

Migrazione dei database agli equivalenti Amazon RDS con AWS DMS

Le migrazioni di dati omogenee in AWS Database Migration Service (AWS DMS) semplificano la migrazione di database locali autogestiti verso gli equivalenti di Amazon Relational Database Service (Amazon RDS). Ad esempio, puoi utilizzare le migrazioni di dati omogenee per migrare un database PostgreSQL on-premise in Amazon RDS per PostgreSQL o Aurora PostgreSQL. Per migrazioni di dati omogenee, AWS DMS utilizza strumenti di database nativi per fornire migrazioni semplici e performanti. like-to-like

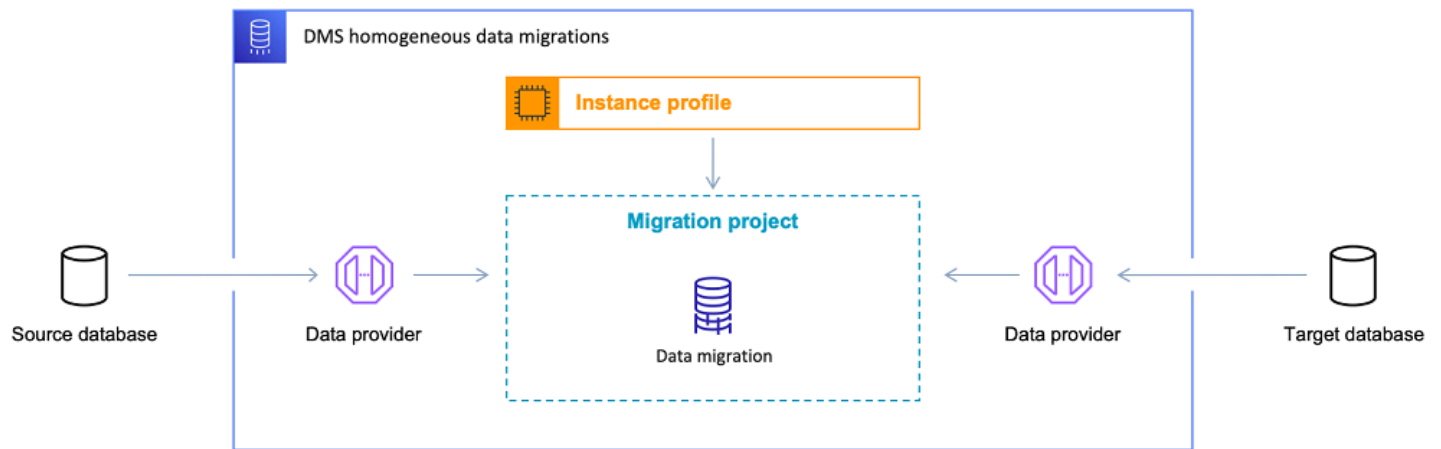
Le migrazioni di dati omogenee sono senza server, il che significa che ridimensionano AWS DMS automaticamente le risorse necessarie per la migrazione. Con le migrazioni di dati omogenee, è possibile migrare dati, partizioni di tabelle, tipi di dati e oggetti secondari come funzioni, stored procedure e così via.

Ad alto livello, le migrazioni di dati omogenee funzionano con profili dell'istanza, fornitori di dati e progetti di migrazione. Quando crei un progetto di migrazione con i provider di dati di origine e di destinazione compatibili dello stesso tipo, AWS DMS implementa un ambiente senza server in cui viene eseguita la migrazione dei dati. Successivamente, AWS DMS si connette al provider di dati di origine, legge i dati di origine, scarica i file sul disco e ripristina i dati utilizzando strumenti di database nativi. Per ulteriori informazioni sui profili dell'istanza, sui fornitori di dati e sui progetti di migrazione, consulta [Collaborazione con fornitori di dati, profili di istanza e progetti di migrazione in AWS DMS](#).

Per l'elenco dei database di origine supportati, consulta [Origini per migrazioni omogenee di dati DMS](#).

Per l'elenco dei database di destinazione supportati, consulta [Destinazioni per migrazioni omogenee di dati DMS](#).

Il seguente diagramma illustra come funzionano le migrazioni di dati omogenee.



Nelle sezioni seguenti vengono fornite informazioni sull'utilizzo delle migrazioni di dati omogenee.

Argomenti

- [Supportato Regioni AWS](#)
- [Funzionalità](#)
- [Limitazioni per le migrazioni di dati omogenee](#)
- [Panoramica del processo di migrazione dei dati omogenea in AWS DMS](#)
- [Configurazione delle migrazioni di dati omogenee in AWS DMS](#)
- [Creazione di fornitori di dati di origine per migrazioni di dati omogenee in AWS DMS](#)
- [Creazione di fornitori di dati target per migrazioni di dati omogenee in AWS DMS](#)
- [Esecuzione di migrazioni di dati omogenee in AWS DMS](#)
- [Risoluzione dei problemi relativi alle migrazioni di dati omogenee in AWS DMS](#)

Supportato Regioni AWS

Di seguito è possibile eseguire migrazioni di dati omogenee. Regioni AWS

Nome della regione	Regione
US East (N. Virginia)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2
US West (Oregon)	us-west-2

Nome della regione	Regione
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacifico (Singapore)	ap-southeast-1
Asia Pacifico (Sydney)	ap-southeast-2
Europa (Frankfurt)	eu-central-1
Europa (Stoccolma)	eu-north-1
Europa (Irlanda)	eu-west-1

Funzionalità

Le migrazioni di dati omogenee forniscono le seguenti funzionalità:

- AWS DMS gestisce automaticamente le risorse di elaborazione e archiviazione necessarie per Cloud AWS migrazioni di dati omogenee. AWS DMS distribuisce queste risorse in un ambiente senza server quando si avvia una migrazione dei dati.
- AWS DMS utilizza strumenti di database nativi per avviare una migrazione completamente automatizzata tra database dello stesso tipo.
- È possibile utilizzare le migrazioni di dati omogenee per migrare i dati e gli oggetti secondari come partizioni, funzioni, stored procedure e così via.
- Puoi eseguire le migrazioni di dati omogenee nelle seguenti tre modalità di migrazione: pieno carico, replica continua e pieno carico con replica continua.
- Per le migrazioni di dati omogenee puoi utilizzare i database Amazon EC2 e Amazon RDS on-premise come origine. Inoltre per le migrazioni di dati omogenee puoi scegliere Amazon RDS o Amazon Aurora come destinazione della migrazione.

Limitazioni per le migrazioni di dati omogenee

Le seguenti limitazioni si applicano quando si utilizzano le migrazioni di dati omogenee:

- Le migrazioni di dati omogenee supportano solo le regole di selezione per le migrazioni di MongoDB e Amazon DocumentDB. DMS non supporta le regole di selezione per altri motori di

database. Inoltre, non puoi utilizzare le regole di trasformazione per modificare il tipo di dati delle colonne, spostare gli oggetti da uno schema a un altro o modificare i nomi degli oggetti.

- Le migrazioni di dati omogenee non forniscono uno strumento integrato per la convalida dei dati.
- Quando si utilizzano migrazioni di dati omogenee con PostgreSQL, AWS DMS migra le viste come tabelle nel database di destinazione.
- Le migrazioni di dati omogenee non acquisiscono le modifiche a livello di schema durante una replica continua dei dati. Se crei una nuova tabella nel database di origine, non puoi AWS DMS migrare questa tabella. Per migrare questa nuova tabella, è necessario riavviare la migrazione dei dati.
- Non è possibile utilizzare migrazioni di dati omogenee AWS DMS per migrare i dati da una versione del database superiore a una versione inferiore del database.
- Non puoi utilizzare le migrazioni di dati omogenee nella CLI o nell'API.
- Le migrazioni di dati omogenee non supportano la creazione di una connessione con istanze database negli intervalli CIDR secondari del VPC.
- Non puoi utilizzare la porta 8081 per le migrazioni omogenee dai fornitori di dati.
- Le migrazioni di dati omogenee non supportano la migrazione di database e tabelle MySQL crittografati.

Panoramica del processo di migrazione dei dati omogenea in AWS DMS

Puoi utilizzare migrazioni di dati omogenee in AWS DMS per migrare i dati tra due database dello stesso tipo. Utilizza il seguente flusso di lavoro per creare ed eseguire una migrazione dei dati.

1. Crea il ruolo e la policy AWS Identity and Access Management (IAM) richiesti. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).
2. Configura i database di origine e di destinazione e crea gli utenti del database con le autorizzazioni minime richieste per le migrazioni di dati omogenee in AWS DMS. Per ulteriori informazioni, consulta [Creazione di fornitori di dati di origine](#) e [Creazione di fornitori di dati di destinazione](#).
3. Archivia le credenziali del database di origine e di destinazione in AWS Secrets Manager. Per ulteriori informazioni, consulta [Fase 1: creazione del segreto](#) nella Guida per l'utente di AWS Secrets Manager.

4. Crea un gruppo di sottoreti, un profilo dell'istanza e i fornitori di dati nella console AWS DMS. Per ulteriori informazioni, consulta [Creazione di un gruppo di sottoreti](#), [Creazione di profili dell'istanza](#) e [Creazione di fornitori di dati](#).
5. Crea un progetto di migrazione utilizzando le risorse create nel passaggio precedente. Per ulteriori informazioni, consulta [Creazione di progetti di migrazione](#).
6. Crea, configura e avvia la migrazione dei dati. Per ulteriori informazioni, consulta [Creazione di una migrazione dei dati](#).
7. Dopo aver completato il pieno carico o la replica continua, puoi interrompere e iniziare a utilizzare il nuovo database di destinazione.
8. Pulisci le risorse. Amazon termina la migrazione dei dati del progetto di migrazione entro tre giorni dal completamento della migrazione. Tuttavia, devi eliminare manualmente risorse come il profilo dell'istanza, i fornitori di dati, il ruolo e la policy IAM e i segreti in AWS Secrets Manager.

Per ulteriori informazioni sulle migrazioni di dati omogenee in AWS DMS, leggi la guida dettagliata per le migrazioni [Da PostgreSQL ad Amazon RDS per PostgreSQL](#).

[Questo video](#) presenta le migrazioni di dati omogenee in AWS DMS e aiuta a familiarizzare con questa funzionalità.

Configurazione delle migrazioni di dati omogenee in AWS DMS

Per configurare migrazioni di dati omogenee in AWS DMS, completa le seguenti attività preliminari.

Argomenti

- [Creazione delle risorse IAM necessarie per le migrazioni di dati omogenee in AWS DMS](#)
- [Configurazione di una rete per le migrazioni di dati omogenee in AWS DMS](#)

Creazione delle risorse IAM necessarie per le migrazioni di dati omogenee in AWS DMS

Per eseguire le migrazioni di dati omogenee, devi creare una policy IAM e un ruolo IAM nel tuo account per interagire con altri servizi AWS. In questa sezione crei queste risorse IAM richieste.

Argomenti

- [Creazione di una policy IAM per le migrazioni di dati omogenee in AWS DMS](#)

- [Creazione di un ruolo IAM per le migrazioni di dati omogenee in AWS DMS](#)

Creazione di una policy IAM per le migrazioni di dati omogenee in AWS DMS

Per accedere ai database e migrare i dati, AWS DMS crea un ambiente serverless per le migrazioni di dati omogenee. In questo ambiente, AWS DMS richiede l'accesso al peering VPC, alle tabelle di routing, ai gruppi di sicurezza e ad altre risorse AWS. Inoltre, AWS DMS archivia log, metriche e avanzamenti di ogni migrazione di dati in Amazon CloudWatch. Per creare un progetto di migrazione dei dati, AWS DMS deve accedere a questi servizi.

In questa fase, viene creata una policy IAM che fornisce ad AWS DMS l'accesso alle risorse Amazon EC2 e CloudWatch. Quindi, crea un ruolo IAM e collegalo alla policy.

Per creare una policy IAM per le migrazioni di dati omogenee in AWS DMS

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Policies (Policy).
3. Scegli Crea policy.
4. Nella pagina Crea policy seleziona la scheda JSON.
5. Incolla il seguente JSON nell'editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcPeeringConnections",
        "ec2:DescribeVpcs",
        "ec2:DescribePrefixLists",
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```



```

        "servicequotas:GetServiceQuota"
    ],
    "Resource": "arn:aws:servicequotas:*:*:vpc/L-0EA8095F"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:DescribeLogStreams"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:dms-data-migration-*"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:dms-data-migration-*:log-
stream:dms-data-migration-*"
},
{
    "Effect": "Allow",
    "Action": "cloudwatch:PutMetricData",
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateRoute",
        "ec2>DeleteRoute"
    ],
    "Resource": "arn:aws:ec2:*:*:route-table/*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:security-group-rule/*",
        "arn:aws:ec2:*:*:route-table/*",
        "arn:aws:ec2:*:*:vpc-peering-connection/*",
    ]
}

```

```

        "arn:aws:ec2:*:*:vpc/*"
    ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": "arn:aws:ec2:*:*:security-group-rule/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupEgress",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:RevokeSecurityGroupEgress",
            "ec2:RevokeSecurityGroupIngress"
        ],
        "Resource": "arn:aws:ec2:*:*:security-group/*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AcceptVpcPeeringConnection",
            "ec2:ModifyVpcPeeringConnectionOptions"
        ],
        "Resource": "arn:aws:ec2:*:*:vpc-peering-connection/*"
    },
    {
        "Effect": "Allow",
        "Action": "ec2:AcceptVpcPeeringConnection",
        "Resource": "arn:aws:ec2:*:*:vpc/*"
    }
]
}

```

6. Scegli Next: Tags (Successivo: Tag) e Next: Review (Successivo: Rivedi).
7. Immetti **HomogeneousDataMigrationsPolicy** per Nome* e scegli Crea policy.

Creazione di un ruolo IAM per le migrazioni di dati omogenee in AWS DMS

In questa fase, crei un ruolo IAM che fornisce ad AWS DMS l'accesso ad AWS Secrets Manager, Amazon EC2 e CloudWatch.

Per creare un ruolo IAM per le migrazioni di dati omogenee in AWS DMS

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Ruoli.
3. Scegli Crea ruolo.
4. Nella pagina Seleziona un'entità attendibile scegli Servizio AWS per Tipo di entità attendibile. Per Casi d'uso per altri servizi AWS scegli DMS.
5. Seleziona la casella di controllo DMS e scegli Successivo.
6. Nella pagina Aggiungi autorizzazioni scegli la policy HomogeneousDataMigrationsPolicy che hai creato in precedenza. Inoltre, scegli SecretsManagerReadWrite. Seleziona Successivo.
7. Nella pagina Nomina, verifica e crea immetti **HomogeneousDataMigrationsRole** per Nome ruolo e scegli Crea ruolo.
8. Nella pagina Ruoli immetti **HomogeneousDataMigrationsRole** per Nome ruolo. Scegli HomogeneousDataMigrationsRole.
9. Nella pagina HomogeneousDataMigrationsRole scegli la scheda Relazioni di attendibilità. Seleziona Edit trust policy (Modifica policy di attendibilità).
10. Nella pagina Modifica policy di attendibilità incolla il seguente codice JSON nell'editor, sostituendo il testo esistente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "dms-data-migrations.amazonaws.com",
          "dms.your_region.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
    }  
  ]  
}
```

Nell'esempio precedente, sostituisci *your_region* con il nome della tua Regione AWS.

La precedente policy basata sulle risorse fornisce ai principali del servizio AWS DMS le autorizzazioni per eseguire le attività in base alla policy gestita da AWS SecretsManagerReadWrite e alla policy gestita dal cliente HomogeneousDataMigrationsPolicy.

11. Scegli Update policy (Aggiorna policy).

Configurazione di una rete per le migrazioni di dati omogenee in AWS DMS

AWS DMS crea un ambiente serverless per le migrazioni di dati omogenee in un cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Puoi specificare il VPC da utilizzare quando crei il profilo dell'istanza. Puoi utilizzare il VPC predefinito per l'account e la Regione AWS oppure crearne uno nuovo.

Per ogni migrazione di dati, AWS DMS stabilisce una connessione peering VPC con il VPC utilizzato per il profilo dell'istanza. Successivamente, AWS DMS aggiunge il blocco CIDR nel gruppo di sicurezza associato al profilo dell'istanza. Poiché AWS DMS associa un indirizzo IP pubblico al profilo dell'istanza, tutte le migrazioni dei dati che utilizzano lo stesso profilo dell'istanza hanno lo stesso indirizzo IP pubblico. Quando la migrazione dei dati si interrompe o non riesce, AWS DMS elimina la connessione peering VPC.

Per evitare che il blocco CIDR si sovrapponga al VPC del VPC del profilo dell'istanza, AWS DMS utilizza il prefisso /24 di uno dei seguenti blocchi CIDR: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16. Ad esempio, se esegui tre migrazioni di dati in parallelo, AWS DMS utilizza i seguenti blocchi CIDR per stabilire una connessione peering VPC.

- 192.168.0.0/24: per la prima migrazione dei dati
- 192.168.1.0/24: per la seconda migrazione dei dati
- 192.168.2.0/24: per la terza migrazione dei dati

È possibile utilizzare diverse configurazioni di rete per impostare l'interazione tra i database di origine e di destinazione con AWS DMS. Anche per la replica continua dei dati è necessario impostare l'interazione tra i database di origine e di destinazione. Queste configurazioni dipendono dalla

posizione del fornitore di dati di origine e dalle impostazioni di rete. Nelle seguenti sezioni sono descritte le configurazioni di rete più comuni.

Argomenti

- [Utilizzo di un singolo VPC per i fornitori di dati di origine e di destinazione](#)
- [Utilizzo di VPC diversi per i fornitori di dati di origine e di destinazione](#)
- [Utilizzo di un fornitore di dati di origine on-premise](#)
- [Configurazione della replica continua dei dati](#)

Utilizzo di un singolo VPC per i fornitori di dati di origine e di destinazione

In questa configurazione, AWS DMS si connette ai fornitori di dati di origine e di destinazione all'interno della rete privata.

Per configurare una rete quando i fornitori di dati di origine e di destinazione si trovano nello stesso VPC

1. Crea il gruppo di sottoreti nella console AWS DMS con il VPC e le sottoreti utilizzati dai fornitori di dati di origine e di destinazione. Per ulteriori informazioni, consulta [Creazione di un gruppo di sottoreti](#).
2. Crea il profilo dell'istanza nella console AWS DMS con il VPC e il gruppo di sottoreti che hai creato. Inoltre, scegli i gruppi di sicurezza VPC utilizzati dai tuoi fornitori di dati di origine e di destinazione. Per ulteriori informazioni, consulta [Creazione di profili dell'istanza](#).

Questa configurazione non richiede l'utilizzo dell'indirizzo IP pubblico per le migrazioni dei dati.

Utilizzo di VPC diversi per i fornitori di dati di origine e di destinazione

In questa configurazione, AWS DMS utilizza una rete privata per connettersi al fornitore di dati di origine o di destinazione. Per un altro fornitore di dati, AWS DMS utilizza una rete pubblica. A seconda del fornitore di dati presente nello stesso VPC del profilo dell'istanza, scegli una delle seguenti configurazioni.

Per configurare una rete privata per il fornitore di dati di origine e una rete pubblica per il fornitore di dati di destinazione

1. Crea il gruppo di sottoreti nella console AWS DMS con il VPC e le sottoreti utilizzati dal fornitore di dati di origine. Per ulteriori informazioni, consulta [Creazione di un gruppo di sottoreti](#).

2. Crea il profilo dell'istanza nella console AWS DMS con il VPC e il gruppo di sottoreti che hai creato. Inoltre, scegli i gruppi di sicurezza VPC utilizzati dal fornitore di dati di origine. Per ulteriori informazioni, consulta [Creazione di profili dell'istanza](#).
3. Apri il progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati. Prendi nota dell'indirizzo IP pubblico in Connettività e sicurezza nella scheda Dettagli.
4. Consenti l'accesso dall'indirizzo IP pubblico della migrazione dei dati nel gruppo di sicurezza del database di destinazione. Per ulteriori informazioni, consulta [Controllo dell'accesso con i gruppi di sicurezza](#) nella Guida per l'utente di Amazon Relational Database Service.

Per configurare una rete pubblica per il fornitore di dati di origine e una rete privata per il fornitore di dati di destinazione

1. Crea il gruppo di sottoreti nella console AWS DMS con il VPC e le sottoreti utilizzati dal fornitore di dati di destinazione. Per ulteriori informazioni, consulta [Creazione di un gruppo di sottoreti](#).
2. Crea il profilo dell'istanza nella console AWS DMS con il VPC e il gruppo di sottoreti che hai creato. Inoltre, scegli i gruppi di sicurezza VPC utilizzati dal fornitore di dati di destinazione. Per ulteriori informazioni, consulta [Creazione di profili dell'istanza](#).
3. Apri il progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati. Prendi nota dell'indirizzo IP pubblico in Connettività e sicurezza nella scheda Dettagli.
4. Consenti l'accesso dall'indirizzo IP pubblico della migrazione dei dati nel gruppo di sicurezza del database di origine. Per ulteriori informazioni, consulta [Controllo dell'accesso con i gruppi di sicurezza](#) nella Guida per l'utente di Amazon Relational Database Service.

Utilizzo di un fornitore di dati di origine on-premise

In questa configurazione, AWS DMS si connette al fornitore di dati di origine all'interno della rete pubblica. AWS DMS utilizza una rete privata per connettersi al fornitore di dati di destinazione.

Per configurare una rete per il fornitore di dati on-premise di origine

1. Crea il gruppo di sottoreti nella console AWS DMS con il VPC e le sottoreti utilizzati dal fornitore di dati di destinazione. Per ulteriori informazioni, consulta [Creazione di un gruppo di sottoreti](#).
2. Crea il profilo dell'istanza nella console AWS DMS con il VPC e il gruppo di sottoreti che hai creato. Inoltre, scegli i gruppi di sicurezza VPC utilizzati dal fornitore di dati di destinazione. Per ulteriori informazioni, consulta [Creazione di profili dell'istanza](#).

3. Apri il progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati. Prendi nota dell'indirizzo IP pubblico in Connettività e sicurezza nella scheda Dettagli.
4. Consenti l'accesso al database di origine dall'indirizzo IP pubblico della migrazione dei dati in AWS DMS.

AWS DMS crea regole in entrata o in uscita nei gruppi di sicurezza VPC. Assicurati di non eliminare queste regole perché questa azione può portare all'esito negativo della migrazione dei dati. Puoi configurare le tue regole nei gruppi di sicurezza VPC. Ti consigliamo di aggiungere una descrizione alle tue regole per poterle gestire.

Configurazione della replica continua dei dati

Per eseguire migrazioni di dati di tipo Pieno carico e acquisizione dei dati di modifica (CDC) o Acquisizione dei dati di modifica (CDC), devi consentire la connessione tra i database di origine e di destinazione.

Per configurare una connessione tra i database di origine e di destinazione accessibili pubblicamente

1. Prendi nota degli indirizzi IP pubblici dei database di origine e di destinazione.
2. Consenti l'accesso al database di origine dall'indirizzo IP pubblico del database di destinazione.
3. Consenti l'accesso al database di destinazione dall'indirizzo IP pubblico del database di origine.

Per configurare una connessione tra i database di origine e di destinazione accessibili privatamente in un singolo VPC

1. Prendi nota degli indirizzi IP privati dei database di origine e di destinazione.

Important

Se i database di origine e di destinazione si trovano in VPC diversi o in reti diverse, puoi utilizzare solo indirizzi IP pubblici per i database di origine e di destinazione. È possibile utilizzare solo nomi di host o indirizzi IP pubblici nei fornitori di dati.

2. Consenti l'accesso al database di origine dall'indirizzo IP privato del database di destinazione.
3. Consenti l'accesso al database di destinazione dall'indirizzo IP privato del database di origine.

Creazione di fornitori di dati di origine per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare database compatibili con MySQL, PostgreSQL e MongoDB come provider di dati di origine per in. [Migrazioni di database omogenee](#) AWS DMS

Per le versioni di database supportate [Provider di dati di origine per migrazioni omogenee di dati DMS](#), vedi.

Il fornitore di dati di origine può essere un database on-premise, Amazon EC2 o Amazon RDS.

Argomenti

- [Utilizzo di un database compatibile con MySQL come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database PostgreSQL come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee in AWS DMS](#)

Utilizzo di un database compatibile con MySQL come fonte per migrazioni di dati omogenee in AWS DMS

È possibile utilizzare un database compatibile con MySQL (MySQL o MariaDB) come origine per [Migrazioni di database omogenee](#) in AWS DMS. In questo caso, il fornitore di dati di origine può essere un database on-premise, Amazon EC2 o RDS per MySQL o MariaDB.

Per eseguire migrazioni di dati omogenee, è necessario usare un utente del database con i privilegi SELECT per tutte le tabelle di origine e gli oggetti secondari della replica. Per le attività di acquisizione dei dati di modifica (CDC), questo utente deve disporre anche dei privilegi REPLICATION CLIENT (BINLOG MONITOR per le versioni di MariaDB successive alla 10.5.2) e REPLICATION SLAVE. Per una migrazione dei dati con pieno carico, non sono necessari questi due privilegi.

Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database MySQL. Esegui le GRANT query per tutti i database verso cui esegui la migrazione. AWS

```
CREATE USER 'your_user'@'%' IDENTIFIED BY 'your_password';  
  
GRANT REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'your_user'@'%';
```



```
GRANT SELECT, RELOAD, LOCK TABLES, SHOW VIEW, EVENT, TRIGGER ON *.* TO 'your_user'@'%';  
  
GRANT BACKUP_ADMIN ON *.* TO 'your_user'@'%';
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni. Se la versione del database MySQL di origine è inferiore alla 8.0, puoi ignorare il comando GRANT BACKUP_ADMIN.

Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database MariaDB. Esegui le query GRANT per tutti i database verso cui esegui la migrazione. AWS

```
CREATE USER 'your_user'@%' IDENTIFIED BY 'your_password';  
GRANT SELECT, RELOAD, LOCK TABLES, REPLICATION SLAVE, BINLOG MONITOR, SHOW VIEW ON *.*  
TO 'your_user'@'%';
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Nelle sezioni seguenti vengono descritti i prerequisiti di configurazione specifici per i database MySQL autogestiti e gestiti da AWS.

Argomenti

- [Utilizzo di un database compatibile con MySQL autogestito come origine per migrazioni di dati omogenee](#)
- [Utilizzo di un database compatibile con MySQL AWS gestito come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Limitazioni all'utilizzo di un database compatibile con MySQL come origine per migrazioni di dati omogenee](#)

Utilizzo di un database compatibile con MySQL autogestito come origine per migrazioni di dati omogenee

In questa sezione viene descritto come configurare i database compatibili con MySQL ospitati on-premise o su istanze Amazon EC2.

Controlla la versione MySQL o MariaDB del database di origine. Assicurati che AWS DMS supporti la versione del database MySQL o MariaDB di origine come descritto in [Origini per migrazioni omogenee di dati DMS](#)

Per utilizzare CDC, assicurati di abilitare la registrazione binaria. Per abilitare la registrazione binaria, configura i seguenti parametri nel file `my.ini` (Windows) o `my.cnf` (UNIX) del database MySQL o MariaDB.

Parametro	Valore
<code>server-id</code>	Imposta questo parametro su un valore uguale o maggiore di 1.
<code>log-bin</code>	Imposta il percorso del file di log binario, ad esempio <code>log-bin=E:\MySQL_Logs\BinLog</code> . Non includere l'estensione del file.
<code>binlog_format</code>	Imposta questo parametro su ROW. Si consiglia questa impostazione per la replica perché, in alcuni casi, quando <code>binlog_format</code> è impostato su STATEMENT, si possono verificare incoerenze della replica dei dati sulla destinazione. Anche il motore di database scrive dati incoerenti simili sulla destinazione quando <code>binlog_format</code> è impostato su MIXED, perché il motore di database passa automaticamente alla registrazione basata su STATEMENT.
<code>expire_logs_days</code>	Imposta questo parametro su un valore uguale o maggiore di 1. Per prevenire un utilizzo eccessivo di spazio su disco, si consiglia di non utilizzare il valore predefinito di 0.
<code>binlog_checksum</code>	Imposta questo parametro su NONE.
<code>binlog_row_image</code>	Imposta questo parametro su FULL.
<code>log_slave_updates</code>	Imposta questo parametro su TRUE se stai utilizzando come origine una replica MySQL o MariaDB.

Utilizzo di un database compatibile con MySQL AWS gestito come fonte per migrazioni di dati omogenee in AWS DMS

In questa sezione viene descritto come configurare le istanze di database Amazon RDS per MySQL e Amazon RDS per MariaDB.

Quando utilizzi un database MySQL o MariaDB AWS gestito come origine per AWS DMS migrazioni di dati omogenee in, assicurati di avere i seguenti prerequisiti per CDC:

- Per abilitare i log binari per RDS per MySQL e MariaDB, attiva i backup automatici a livello di istanza. Per abilitare i log binari per un cluster Aurora MySQL, modifica la variabile `binlog_format` nel gruppo di parametri. Non è necessario abilitare i backup automatici per un cluster Aurora MySQL.

Quindi imposta il parametro `binlog_format` su `ROW`.

Per ulteriori informazioni sull'impostazione dei backup automatici, consulta [Abilitazione dei backup automatici](#) nella Guida per l'utente di Amazon RDS.

Per ulteriori informazioni sulla configurazione della registrazione binaria per un database Amazon RDS per MySQL o MariaDB, consulta [Configurazione del log binario](#) nella Guida per l'utente di Amazon RDS.

Per ulteriori informazioni sulla configurazione della registrazione binaria per un cluster MySQL Aurora, consulta [Come posso attivare la registrazione binaria per il cluster Amazon Aurora MySQL edizione compatibile?](#)

- Assicurati che i log binari siano disponibili per. AWS DMS Poiché i database MySQL e MariaDB AWS gestiti eliminano i log binari il prima possibile, è necessario aumentare il periodo di tempo in cui i log rimangono disponibili. Ad esempio, per aumentare il periodo di conservazione dei log binari a 24 ore, esegui il comando seguente.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

- Imposta il parametro `binlog_row_image` su `Full`.
- Imposta il parametro `binlog_checksum` su `NONE`.
- Se stai utilizzando una replica Amazon RDS MySQL o MariaDB come origine, abilita i backup sulla replica di lettura e assicurati che il parametro `log_slave_updates` sia impostato su `TRUE`.

Limitazioni all'utilizzo di un database compatibile con MySQL come origine per migrazioni di dati omogenee

Le seguenti limitazioni si applicano quando si utilizza un database compatibile con MySQL come origine per migrazioni di dati omogenee:

- Gli oggetti MariaDB come le sequenze non sono supportati in attività di migrazioni omogenee.
- La migrazione da MariaDB ad Amazon RDS MySQL/Aurora MySQL potrebbe non riuscire a causa di differenze tra oggetti incompatibili.
- Il nome utente che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 2 a 64 caratteri.
 - Non può includere spazi.
 - Può includere i seguenti caratteri: a-z, A-Z, 0-9, carattere di sottolineatura (_).
 - Deve iniziare con a-z o A-Z.
- La password che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 1 a 128 caratteri.
 - Non può contenere i seguenti caratteri: virgoletta singola ('), virgolette doppie ("), punto e virgola (;) o spazio.

Utilizzo di un database PostgreSQL come fonte per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare un database PostgreSQL come origine per [Migrazioni di database omogenee](#) in AWS DMS. In questo caso, il fornitore di dati di origine può essere un database on-premise, Amazon EC2 o RDS per PostgreSQL.

Per eseguire migrazioni di dati omogenee, concedi le autorizzazioni di superutente per l'utente del database che hai specificato per il AWS DMS tuo database di origine PostgreSQL. Le autorizzazioni di superuser sono necessarie all'utente del database per accedere alle funzioni specifiche della replica nell'origine. Per una migrazione dei dati con pieno carico, l'utente del database necessita delle autorizzazioni SELECT sulle tabelle per migrarle.

Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database di origine PostgreSQL. Esegui la GRANT query per tutti i database verso cui esegui la migrazione. AWS

```
CREATE USER your_user WITH LOGIN PASSWORD 'your_password';  
ALTER USER your_user WITH SUPERUSER;  
GRANT SELECT ON ALL TABLES IN SCHEMA schema_name TO your_user;
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Nelle sezioni seguenti vengono descritti i prerequisiti di configurazione specifici per i database PostgreSQL autogestiti e gestiti da AWS.

Argomenti

- [Utilizzo di un database PostgreSQL autogestito come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database PostgreSQL AWS gestito come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Limitazioni relative all'utilizzo di un database compatibile con PostgreSQL come origine per migrazioni di dati omogenee](#)

Utilizzo di un database PostgreSQL autogestito come fonte per migrazioni di dati omogenee in AWS DMS

In questa sezione viene descritto come configurare i database PostgreSQL ospitati on-premise o su istanze Amazon EC2.

Controlla la versione del database PostgreSQL di origine. Assicurati che AWS DMS supporti la versione del database PostgreSQL di origine come descritto in [Origini per migrazioni omogenee di dati DMS](#)

Le migrazioni di dati omogenee supportano l'acquisizione dei dati di modifica (CDC) tramite la replica logica. Per attivare la replica logica su un database di origine PostgreSQL autogestito, imposta i seguenti parametri e valori nel file di configurazione `postgresql.conf`:

- Imposta `wal_level` su `logical`.
- Imposta `max_replication_slots` su un valore maggiore di 1.

Imposta il valore `max_replication_slots` in base al numero di attività che desideri eseguire. Ad esempio, per eseguire cinque attività dovrai impostare un minimo di cinque slot. Gli slot si aprono automaticamente non appena viene avviata un'attività e restano aperti anche quando l'attività non è più in esecuzione. Assicurati di eliminare manualmente gli slot aperti.

- Imposta `max_wal_senders` su un valore maggiore di 1.

Il parametro `max_wal_senders` imposta il numero di attività simultanee che è possibile eseguire.

- Il parametro `wal_sender_timeout` termina le connessioni di replica che sono inattive per un tempo maggiore del numero specificato di millisecondi. Il valore predefinito è 60000 millisecondi

(60 secondi). L'impostazione del valore su 0 (zero) disabilita il meccanismo di timeout ed è un'opzione valida per DMS.

Alcuni parametri sono statici e possono essere impostati solo all'avvio del server. Qualsiasi modifica alle voci nel file di configurazione viene ignorata fino al riavvio del server. Per ulteriori informazioni, consultare la [documentazione di PostgreSQL](#).

Utilizzo di un database PostgreSQL AWS gestito come fonte per migrazioni di dati omogenee in AWS DMS

In questa sezione viene descritto come configurare le istanze di database Amazon RDS per PostgreSQL.

Usa l'account utente AWS principale per l'istanza DB PostgreSQL come account utente per il provider di dati di origine PostgreSQL per migrazioni di dati omogenee in AWS DMS. L'account utente master dispone dei ruoli necessari che consentono di configurare il CDC. Se utilizzi un account diverso dall'account utente master, è necessario che l'account disponga dei ruoli `rds_superuser` e `rds_replication`. Il ruolo `rds_replication` fornisce le autorizzazioni per gestire gli slot logici e per eseguire lo streaming dei dati utilizzando gli slot logici.

Usa il seguente esempio di codice per assegnare i ruoli `rds_superuser` e `rds_replication`.

```
GRANT rds_superuser to your_user;  
GRANT rds_replication to your_user;
```

Nell'esempio precedente sostituisci `your_user` con il nome dell'utente del database.

Per attivare la replica logica, imposta su 1 il parametro `rds.logical_replication` nel gruppo di parametri del database. Questo parametro statico richiede un riavvio dell'istanza database per avere effetto.

Limitazioni relative all'utilizzo di un database compatibile con PostgreSQL come origine per migrazioni di dati omogenee

Quando si utilizza un database compatibile con PostgreSQL come origine per migrazioni di dati omogenee si applicano le seguenti limitazioni:

- Il nome utente che usi per connetterti all'origine dati presenta le seguenti limitazioni:

- Può contenere da 2 a 64 caratteri.
- Non può includere spazi.
- Può includere i seguenti caratteri: a-z, A-Z, 0-9, carattere di sottolineatura (_).
- Deve iniziare con a-z o A-Z.
- La password che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 1 a 128 caratteri.
 - Non può contenere i seguenti caratteri: virgoletta singola ('), virgolette doppie ("), punto e virgola (;) o spazio.

Utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare un database compatibile con MongoDB come fonte per migrazioni di dati omogenee in AWS DMS. In questo caso, il tuo fornitore di dati di origine può essere un database Amazon EC2 per MongoDB locale o Amazon DocumentDB (con compatibilità con MongoDB).

Per le versioni del database supportate, consulta [Provider di dati di origine per migrazioni omogenee di dati DMS](#)

Le sezioni seguenti descrivono i prerequisiti di configurazione specifici per i database MongoDB autogestiti e i database Amazon DocumentDB gestiti. AWS

Argomenti

- [Utilizzo di un database MongoDB autogestito come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database Amazon DocumentDB come fonte per migrazioni di dati omogenee in AWS DMS](#)
- [Funzionalità per l'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee](#)
- [Limitazioni all'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee](#)
- [Le migliori pratiche per l'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee](#)

Utilizzo di un database MongoDB autogestito come fonte per migrazioni di dati omogenee in AWS DMS

Questa sezione descrive come configurare i database MongoDB ospitati in locale o su istanze Amazon EC2.

Controlla la versione del tuo database MongoDB sorgente. Assicurati che AWS DMS supporti la versione del database MongoDB di origine come descritto in [Provider di dati di origine per migrazioni omogenee di dati DMS](#)

Per eseguire migrazioni di dati omogenee con una fonte MongoDB, puoi creare un account utente con privilegi di root o un utente con autorizzazioni solo sul database da migrare. Per ulteriori informazioni sulla creazione di utenti, vedere [Autorizzazioni necessarie per l'uso di MongoDB come origine per AWS DMS](#)

Per utilizzare la replica continua o CDC con MongoDB, è necessario l' AWS DMS accesso al registro delle operazioni di MongoDB (oplog). Per ulteriori informazioni, consulta [Configurazione di un set di repliche MongoDB per CDC](#).

Per informazioni sui metodi di autenticazione MongoDB, consulta [Requisiti di sicurezza per l'uso di MongoDB come origine per AWS DMS](#)

Per MongoDB come fonte, le migrazioni di dati omogenee supportano tutti i tipi di dati supportati da Amazon DocumentDB.

Per MongoDB come sorgente, per memorizzare le credenziali utente in Secrets Manager, è necessario fornirle in testo semplice, utilizzando il tipo Altro tipo di segreti. Per ulteriori informazioni, consulta [Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service](#).

Il seguente esempio di codice mostra come archiviare i segreti del database utilizzando testo semplice.

```
{
  "username": "dbuser",
  "password": "dbpassword"
}
```


Utilizzo di un database Amazon DocumentDB come fonte per migrazioni di dati omogenee in AWS DMS

Questa sezione descrive come configurare le istanze del database Amazon DocumentDB da utilizzare come origine per migrazioni di dati omogenee.

Utilizza il nome utente principale per l'istanza Amazon DocumentDB come account utente per il provider di dati di origine compatibile con MongoDB per migrazioni di dati omogenee in AWS DMS. L'account utente master dispone dei ruoli necessari che consentono di configurare il CDC. Se utilizzi un account diverso dall'account utente principale, l'account deve avere il ruolo root. Per ulteriori informazioni sulla creazione dell'utente come account root, vedere [Impostazione delle autorizzazioni per utilizzare Amazon DocumentDB come origine](#).

Per attivare la replica logica, impostate il `change_stream_log_retention_duration` parametro nel gruppo di parametri del database su un'impostazione appropriata per il carico di lavoro delle transazioni. La modifica di questo parametro statico richiede il riavvio dell'istanza DB per avere effetto. Prima di iniziare la migrazione dei dati per tutti i tipi di attività, incluso Full Load Only, abilita i flussi di modifica di Amazon DocumentDB per tutte le raccolte all'interno di un determinato database o solo per raccolte selezionate. Per ulteriori informazioni sull'abilitazione dei flussi di modifica per Amazon DocumentDB, [consulta Enabling Change Streams](#) nella guida per sviluppatori di Amazon DocumentDB.

Note

AWS DMS utilizza il flusso di modifiche di Amazon DocumentDB per acquisire le modifiche durante la replica in corso. Se Amazon DocumentDB elimina i record dal flusso di modifiche prima che DMS li legga, le attività avranno esito negativo. Consigliamo di impostare il `change_stream_log_retention_duration` parametro per conservare le modifiche per almeno 24 ore.

Per utilizzare Amazon DocumentDB per la migrazione omogenea dei dati, archivia le credenziali utente in Secrets Manager nella sezione Credentials for Amazon DocumentDB database.

Funzionalità per l'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee

- Puoi migrare tutti gli indici secondari supportati da Amazon DocumentDB durante la fase di caricamento completo.

- AWS DMS migra le raccolte in parallelo. la migrazione omogenea dei dati calcola i segmenti in fase di esecuzione in base alla dimensione media di ogni documento della raccolta per ottenere le massime prestazioni.
- DMS può replicare gli indici secondari creati nella fase CDC. DMS supporta questa funzionalità nella versione 6.0 di MongoDB.
- DMS supporta documenti con un livello di nidificazione superiore a 97.

Limitazioni all'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee

- I documenti non possono avere nomi di campo con un \$ prefisso.
- AWS DMS non supporta la migrazione della raccolta di serie temporali.
- AWS DMS non supporta create gli drop eventi rename collection DDL durante la fase CDC.
- AWS DMS non supporta tipi di dati incoerenti nella raccolta per il campo. `_id` Ad esempio, la seguente raccolta non supportata contiene più tipi di dati per il campo. `_id`

```
rs0 [direct: primary] test> db.collection1.aggregate([
...  {
...    $group: {
...      _id: { $type: "$_id" },
...      count: { $sum: 1 }
...    }
...  }
... ])
[ { _id: 'string', count: 6136 }, { _id: 'objectId', count: 848033 } ]
```

- Per le attività esclusivamente CDC, supporta AWS DMS solo la `immediate` modalità di avvio.
- AWS DMS non supporta documenti con caratteri UTF8 non validi.
- AWS DMS non supporta raccolte condivise.

Le migliori pratiche per l'utilizzo di un database compatibile con MongoDB come fonte per migrazioni di dati omogenee

- Per più database e raccolte di grandi dimensioni ospitati sulla stessa istanza di MongoDB, ti consigliamo di utilizzare regole di selezione per ogni database e raccolta per suddividere l'attività

tra più attività e progetti di migrazione dei dati. È possibile ottimizzare le divisioni di database e raccolta per ottenere le massime prestazioni.

Creazione di fornitori di dati target per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare database compatibili con MySQL, PostgreSQL e Amazon DocumentDB come provider di dati di destinazione per migrazioni di dati omogenee in AWS DMS.

Per le versioni di database supportate [Provider di dati di destinazione per migrazioni omogenee di dati DMS](#), consulta.

Il fornitore di dati di destinazione può essere un'istanza database Amazon RDS o un cluster di database Amazon Aurora. Tieni presente che la versione del database del provider di dati di destinazione deve essere uguale o superiore alla versione del database del provider di dati di origine.

Argomenti

- [Utilizzo di un database compatibile con MySQL come destinazione per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database PostgreSQL come destinazione per migrazioni di dati omogenee in AWS DMS](#)
- [Utilizzo di un database Amazon DocumentDB come destinazione per migrazioni di dati omogenee in AWS DMS](#)

Utilizzo di un database compatibile con MySQL come destinazione per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare un database compatibile con MySQL come destinazione per migrazioni di dati omogenee in AWS DMS.

AWS DMS richiede determinate autorizzazioni per migrare i dati nel database Amazon RDS for MySQL o MariaDB o Amazon Aurora MySQL di destinazione. Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database MySQL di destinazione.

```
CREATE USER 'your_user'@'%' IDENTIFIED BY 'your_password';
```

```
GRANT ALTER, CREATE, DROP, INDEX, INSERT, UPDATE, DELETE, SELECT, CREATE VIEW, CREATE  
ROUTINE, ALTER ROUTINE, EVENT, TRIGGER, EXECUTE, REFERENCES ON *.* TO 'your_user'@'%';  
GRANT REPLICATION SLAVE, REPLICATION CLIENT ON *.* TO 'your_user'@'%';
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database MariaDB. Esegui le query GRANT per tutti i database verso cui esegui la migrazione. AWS

```
CREATE USER 'your_user'@'%' IDENTIFIED BY 'your_password';  
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, INDEX, ALTER, CREATE VIEW, CREATE  
ROUTINE, ALTER ROUTINE, EVENT, TRIGGER, EXECUTE, SLAVE MONITOR, REPLICATION SLAVE ON  
*.* TO 'your_user'@'%';
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Note

In Amazon RDS, quando attivi il backup automatico per un'istanza database MySQL/MariaDB, abiliti anche la registrazione binaria. Quando queste impostazioni sono abilitate, l'attività di migrazione dei dati potrebbe non riuscire con il seguente errore durante la creazione di oggetti secondari, come funzioni, procedure e trigger, sul database di destinazione. Se nel database di destinazione è abilitata la registrazione binaria, imposta `true` su `log_bin_trust_function_creators` nel gruppo di parametri del database prima di iniziare l'attività.

```
ERROR 1419 (HY000): You don't have the SUPER privilege and binary logging is  
enabled (you might want to use the less safe log_bin_trust_function_creators  
variable)
```

Limitazioni relative all'utilizzo di un database compatibile con MySQL come destinazione per migrazioni di dati omogenee

Quando si utilizza un database compatibile con MySQL come origine per migrazioni di dati omogenee si applicano le seguenti limitazioni:

- Il nome utente che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 2 a 64 caratteri.
 - Non può includere spazi.
 - Può includere i seguenti caratteri: a-z, A-Z, 0-9, carattere di sottolineatura (_).
 - Non può includere un trattino (-).
 - Deve iniziare con a-z o A-Z.
- La password che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 1 a 128 caratteri.
 - Non può contenere i seguenti caratteri: virgoletta singola ('), virgolette doppie ("), punto e virgola (;) o spazio.

Utilizzo di un database PostgreSQL come destinazione per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare un database PostgreSQL come destinazione per migrazioni di dati omogenee in AWS DMS.

AWS DMS richiede determinate autorizzazioni per migrare i dati nel database Amazon RDS for PostgreSQL o Amazon Aurora PostgreSQL di destinazione. Usa lo script seguente per creare un utente del database con le autorizzazioni necessarie nel tuo database PostgreSQL di destinazione.

```
CREATE USER your_user WITH LOGIN PASSWORD 'your_password';
GRANT USAGE ON SCHEMA schema_name TO your_user;
GRANT CONNECT ON DATABASE db_name TO your_user;
GRANT CREATE ON DATABASE db_name TO your_user;
GRANT CREATE ON SCHEMA schema_name TO your_user;
GRANT UPDATE, INSERT, SELECT, DELETE, TRUNCATE ON ALL TABLES IN SCHEMA schema_name
  TO your_user;
      #For "Full load and change data capture (CDC)" and "Change data capture
      (CDC)" data migrations, setting up logical replication requires rds_superuser
      privileges
GRANT rds_superuser TO your_user;
```

Nell'esempio precedente, sostituisci ogni *segnaposto dell'input utente* con le tue informazioni.

Per attivare la replica logica per la destinazione RDS per PostgreSQL, imposta su 1 il parametro `rds.logical_replication` nel gruppo di parametri del database. Per rendere effettivo questo parametro statico è necessario il riavvio dell'istanza database o del cluster di database. Alcuni parametri sono statici e puoi impostarli solo all'avvio del server. AWS DMS ignora le modifiche alle relative voci nel gruppo di parametri DB fino al riavvio del server.

PostgreSQL utilizza i trigger per implementare i vincoli di chiave esterna. Durante la fase di pieno carico, AWS DMS carica ogni tabella una alla volta. Si consiglia di disattivare i vincoli di chiave esterna sul database di destinazione durante il pieno carico. A tale scopo, usa uno dei seguenti metodi:

- Disattiva temporaneamente tutti i trigger dell'istanza e termina il pieno carico.
- Modifica il valore del parametro `session_replication_role` in PostgreSQL.

In qualsiasi momento, un trigger può trovarsi in uno dei seguenti stati: `origin`, `replica`, `always` o `disabled`. Quando imposti il parametro `session_replication_role` su `replica`, sono attivi solo i trigger nello stato `replica`. In caso contrario, i trigger rimangono inattivi.

Limitazioni relative all'utilizzo di un database compatibile con PostgreSQL come destinazione per migrazioni di dati omogenee

Quando si utilizza un database compatibile con PostgreSQL come destinazione per migrazioni di dati omogenee si applicano le seguenti limitazioni:

- Il nome utente che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 2 a 64 caratteri.
 - Non può includere spazi.
 - Può includere i seguenti caratteri: a-z, A-Z, 0-9, carattere di sottolineatura (`_`).
 - Deve iniziare con a-z o A-Z.
- La password che usi per connetterti all'origine dati presenta le seguenti limitazioni:
 - Può contenere da 1 a 128 caratteri.
 - Non può contenere i seguenti caratteri: virgoletta singola (`'`), virgolette doppie (`"`), punto e virgola (`;`) o spazio.

Utilizzo di un database Amazon DocumentDB come destinazione per migrazioni di dati omogenee in AWS DMS

Puoi utilizzare un database Amazon DocumentDB (con compatibilità MongoDB) e un cluster Elastic DocumentDB come destinazione di migrazione per migrazioni di dati omogenee in AWS DMS.

Per eseguire migrazioni di dati omogenee per una destinazione Amazon DocumentDB, puoi creare un account utente con privilegi di amministratore o un utente con autorizzazioni di lettura/scrittura solo sul database da migrare.

Le migrazioni di dati omogenee supportano tutti i tipi di dati BSON supportati da Amazon DocumentDB. Per un elenco di questi tipi di dati, consulta [Data Types](#) nella Amazon DocumentDB Developer Guide.

Per utilizzare le funzionalità shard del cluster DocumentDB Elastic per la migrazione della raccolta non frammentata dall'origine, crea una raccolta di shard da migrare prima di iniziare l'attività di migrazione dei dati. Per ulteriori informazioni sulla raccolta di shard in un cluster Amazon DocumentDB Elastic, [consulta Step 5: Shard your collection](#) nella Amazon DocumentDB Developer Guide.

Per un target Amazon DocumentDB, AWS DMS supporta le modalità `none` o `require SSL`.

Esecuzione di migrazioni di dati omogenee in AWS DMS

Puoi utilizzare [Migrazioni di database omogenee](#) in AWS DMS per migrare i dati dal tuo database di origine al motore equivalente su Amazon Relational Database Service (Amazon RDS), Amazon Aurora o Amazon DocumentDB. AWS DMS automatizza il processo di migrazione dei dati utilizzando strumenti di database nativi nei database di origine e di destinazione.

Dopo aver creato un profilo dell'istanza e i fornitori di dati compatibili per migrazioni di dati omogenee, puoi creare un progetto di migrazione. Per ulteriori informazioni, consulta [Creazione di progetti di migrazione](#).

Nelle seguenti sezioni viene descritto come creare, configurare ed eseguire le migrazioni di dati omogenee.

Argomenti

- [Creazione di una migrazione dei dati in AWS DMS](#)

- [Regole di selezione per migrazioni di dati omogenee](#)
- [Gestione delle migrazioni dei dati in AWS DMS](#)
- [Monitoraggio delle migrazioni dei dati in AWS DMS](#)
- [Stati delle migrazioni di dati omogenee in AWS DMS](#)
- [Migrazione dei dati dai database MySQL con migrazioni di dati omogenee in AWS DMS](#)
- [Migrazione dei dati dai database PostgreSQL con migrazioni di dati omogenee in AWS DMS](#)
- [Migrazione dei dati dai database MongoDB con migrazioni di dati omogenee in AWS DMS](#)

Creazione di una migrazione dei dati in AWS DMS

Puoi utilizzare il progetto di migrazione che hai creato con fornitori di dati compatibili dello stesso tipo per le migrazioni di dati omogenee. Per ulteriori informazioni, consulta [Creazione di progetti di migrazione](#).

Per iniziare a utilizzare le migrazioni di dati omogenee, crea una nuova migrazione dei dati. È possibile creare diverse migrazioni di dati omogenee di differenti tipi in un unico progetto di migrazione.

AWS DMS dispone del numero massimo di migrazioni di dati omogenee che puoi creare per il tuo Account AWS. Per informazioni sulle quote di AWS DMS servizio, consulta la sezione seguente. [Quote per AWS Database Migration Service](#)

Prima di creare una migrazione dei dati, assicurati di configurare le risorse necessarie, come i database di origine e di destinazione, un ruolo e una policy IAM, un profilo dell'istanza e i fornitori di dati. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#), [Creazione di profili dell'istanza](#) e [Creazione di fornitori di dati](#).

Inoltre, ti consigliamo di non utilizzare le migrazioni di dati omogenee per migrare i dati una versione del database più recente a una versione precedente del database. Controlla le versioni dei database che usi per i fornitori di dati di origine e di destinazione e aggiorna la versione del database di destinazione, se necessario.

Per creare una migrazione dei dati

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.

3. Scegli il progetto di migrazione e nella scheda Migrazioni dei dati scegli Crea migrazione dei dati.
4. Per Nome immetti un nome per la migrazione dei dati. Assicurati di utilizzare un nome univoco per la migrazione dei dati in modo da poterlo identificare facilmente.
5. Per Tipo di replica scegli il tipo di migrazione dei dati che desideri configurare. Puoi scegliere una delle seguenti opzioni.
 - Pieno carico: migra i dati di origine esistenti.
 - Pieno carico e acquisizione dei dati di modifica (CDC): migra i dati di origine esistenti e replica le modifiche in corso.
 - Acquisizione dei dati di modifica (CDC): replica le modifiche in corso.
6. Seleziona la casella di controllo Attiva CloudWatch i log per archiviare i log di migrazione dei dati in Amazon. CloudWatch Se non si sceglie questa opzione, non sarà possibile esaminare i file di log quando la migrazione dei dati non riesce.
7. (Facoltativo) Espandi Advanced settings (Impostazioni avanzate). Per Numero di lavori, inserisci il numero di thread paralleli che AWS DMS puoi utilizzare per migrare i dati di origine verso la destinazione.
8. Per Ruolo di servizio IAM scegli il ruolo IAM che hai creato nei prerequisiti. Per ulteriori informazioni, consulta [Creazione di un ruolo IAM per le migrazioni di dati omogenee in AWS DMS](#).
9. Configura la Modalità di avvio per le migrazioni dei dati di tipo Acquisizione dei dati di modifica (CDC). Puoi scegliere una delle seguenti opzioni.
 - Immediatamente: avvia la replica continua insieme alla migrazione dei dati.
 - Utilizzo di un punto di avvio nativo: avvia la replica continua dal punto specificato.

Per i database PostgreSQL, immetti il nome dello slot di replica logica per Nome dello slot e il numero di sequenza del log delle transazioni per Punto di avvio nativo.

Per i database MySQL, immetti il numero di sequenza del log delle transazioni per Numero di sequenza del registro (LSN).
10. Configura la Modalità di interruzione per le migrazioni dei dati di tipo Acquisizione dei dati di modifica (CDC) o Pieno carico e acquisizione dei dati di modifica (CDC). Puoi scegliere una delle seguenti opzioni.
 - Non interrompere CDC: AWS DMS continua la replica continua fino a quando non interrompi la migrazione dei dati.

- Utilizzo di un punto temporale del server: AWS DMS interrompe la replica in corso all'ora specificata.

Se scegli questa opzione, immetti in Data e ora di fine la data e l'ora in cui vuoi interrompere automaticamente la replica continua.

11. Scegli Crea migrazione dei dati.

AWS DMS crea la migrazione dei dati e la aggiunge all'elenco nella scheda Migrazioni dei dati del progetto di migrazione. In questa scheda puoi vedere lo stato della migrazione dei dati. Per ulteriori informazioni, consulta [Stati di migrazione](#).

Important

Per le migrazioni di dati di tipo Full load e Full load and change data capture (CDC), AWS DMS elimina tutti i dati, le tabelle e gli altri oggetti di database presenti nel database di destinazione. Assicurati di avere un backup del database di destinazione.

Dopo aver AWS DMS creato la migrazione dei dati, lo stato di questa migrazione dei dati è impostato su Pronto. Per migrare i dati, è necessario avviare la migrazione dei dati manualmente. Per farlo, scegli la migrazione dei dati dall'elenco. Quindi per Operazioni scegli Avvia. Per ulteriori informazioni, consulta [Gestione delle migrazioni dei dati](#).

Il primo avvio di una migrazione omogenea dei dati richiede alcune configurazioni. AWS DMS crea un ambiente serverless per la migrazione dei dati. Questo processo può richiedere fino a 15 minuti. Dopo aver interrotto e riavviato la migrazione dei dati, AWS DMS non crea più l'ambiente e puoi accedere più rapidamente alla migrazione dei dati.

Regole di selezione per migrazioni di dati omogenee

È possibile utilizzare le regole di selezione per scegliere lo schema, le tabelle o entrambi da includere nella replica.

Note

AWS DMS supporta solo regole di selezione per migrazioni di dati omogenee quando si utilizza un database compatibile con MongoDB come fonte.

Quando crei un'attività di migrazione dei dati, scegli Aggiungi regola di selezione.

Per le impostazioni delle regole, fornisci i seguenti valori:

- Schema: scegli Inserisci uno schema.
- Nome dello schema: fornisci il nome dello schema che desideri replicare o usalo % come jolly.
- Nome tabella:: Fornisci il nome della tabella che desideri replicare o usa % come jolly.

Per impostazione predefinita, l'unica azione di regola supportata da DMS è Include, e l'unico carattere jolly supportato da DMS è. %

Example Migrazione di tutte le tabelle in uno schema

Nell'esempio seguente viene eseguita la migrazione di tutte le tabelle da uno schema denominato dmsst nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "dmsst",
        "table-name": "%"
      },
      "filters": [],
      "rule-id": "1",
      "rule-name": "1"
    }
  ]
}
```

Example Migrazione di alcune tabelle in uno schema

L'esempio seguente migra tutte le tabelle con un nome che inizia con collectionTest, da uno schema denominato dmsst nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
```

```
    "rule-type": "selection",
    "rule-action": "include",
    "object-locator": {
      "schema-name": "dmsst",
      "table-name": "collectionTest%"
    },
    "filters": [],
    "rule-id": "1",
    "rule-name": "1"
  }
]
}
```

Example Migra tabelle specifiche da più schemi

L'esempio seguente migra alcune tabelle da più schemi denominati dmsst e Test presenti nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "dmsst",
        "table-name": "collectionTest1"
      },
      "filters": [],
      "rule-id": "1",
      "rule-name": "1"
    },
    {
      "rule-type": "selection",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "products"
      },
      "filters": [],
      "rule-id": "2",
      "rule-name": "2"
    }
  ]
}
```

}

Gestione delle migrazioni dei dati in AWS DMS

Dopo aver creato una migrazione dei dati, AWS DMS non avvia automaticamente la migrazione dei dati. La migrazione dei dati viene avviata manualmente quando necessario.

Prima di iniziare una migrazione dei dati, puoi modificare tutte le relative impostazioni. Una volta avviata la migrazione dei dati non è più possibile modificare il tipo di replica. Per utilizzare un altro tipo di replica è necessario creare una nuova migrazione dei dati.

Per avviare una migrazione dei dati

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il tuo progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati. Viene visualizzata la pagina Riepilogo relativa alla tua migrazione dei dati.
4. In Actions (Operazioni), scegliere Start (Avvia).

Dopodiché, AWS DMS crea un ambiente serverless per la migrazione dei dati. Questo processo può richiedere fino a 15 minuti.

Dopo aver avviato una migrazione dei dati, AWS DMS imposta lo stato su Avvio. Lo stato successivo AWS DMS utilizzato per la migrazione dei dati dipende dal tipo di replica scelto nelle impostazioni di migrazione dei dati. Per ulteriori informazioni, consulta [Stati di migrazione](#).

Per modificare una migrazione dei dati

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il tuo progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati. Viene visualizzata la pagina Riepilogo relativa alla tua migrazione dei dati.
4. Scegli Modifica.
5. Configura le impostazioni per la migrazione dei dati.

⚠ Important

Se la migrazione dei dati è avviata, non puoi modificare il tipo di replica.

6. Per visualizzare i log di migrazione dei dati in Amazon CloudWatch, seleziona la casella di controllo Attiva i CloudWatch registri.
7. Seleziona Salvataggio delle modifiche.

Dopo aver AWS DMS avviato una migrazione dei dati, puoi interromperla. Per farlo, scegli la migrazione dei dati nella scheda Migrazioni dei dati. Quindi per Operazioni scegli Interrompi.

Dopo aver interrotto una migrazione dei dati, AWS DMS imposta lo stato su Interruzione. Successivamente, AWS DMS imposta lo stato della migrazione dei dati su Interrotto. Dopo aver AWS DMS interrotto una migrazione dei dati, è possibile modificare, riavviare o eliminare la migrazione dei dati.

Per continuare la replica dei dati, scegli la migrazione dei dati che hai interrotto nella scheda Migrazioni dei dati. Quindi, per Operazioni scegli Riprendi l'elaborazione.

Per riavviare il caricamento dei dati, scegli la migrazione dei dati che hai interrotto nella scheda Migrazioni dei dati. Quindi, per Azioni, scegli Riavvia. AWS DMS elimina tutti i dati dal database di destinazione e avvia la migrazione dei dati da zero.

Puoi eliminare una migrazione di dati che hai interrotto o che non hai avviato. Per eliminare una migrazione di dati, selezionala nella scheda Migrazioni di dati. Per Operazioni scegli Elimina. Per eliminare il progetto di migrazione, interrompi ed elimina tutte le migrazioni di dati.

Monitoraggio delle migrazioni dei dati in AWS DMS

Dopo aver avviato la migrazione di dati omogenea, puoi monitorarne lo stato e l'avanzamento. Le migrazioni di dati di set di dati di grandi dimensioni, ad esempio centinaia di gigabyte, richiedono ore per essere completate. Per mantenere l'affidabilità, la disponibilità e le prestazioni elevate della migrazione dei dati, è necessario monitorarne regolarmente l'avanzamento.

Per verificare lo stato e l'avanzamento della migrazione dei dati

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione e passa alla scheda Migrazioni dei dati.
4. Per la tua migrazione dei dati, osserva la colonna Stato. Per ulteriori informazioni sui valori di questa colonna, consulta [Stati di migrazione](#).
5. Per una migrazione dei dati in corso, la colonna Progressi della migrazione mostra la percentuale di dati migrati.

Per verificare i dettagli della migrazione dei dati

1. Accedi a AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il tuo progetto di migrazione. Nella scheda Migrazioni dei dati scegli la tua migrazione dei dati.
4. Nella scheda Dettagli puoi vedere lo stato di avanzamento della migrazione. In particolare, è possibile vedere le metriche riportate di seguito.
 - Indirizzo IP pubblico: l'indirizzo IP pubblico della migrazione dei dati. Questo valore è necessario per configurare la rete. Per ulteriori informazioni, consulta [Configurazione di una rete](#).
 - Tabelle caricate: il numero di tabelle caricate correttamente.
 - Caricamento delle tabelle in corso: il numero di tabelle attualmente in caricamento.
 - Tabelle in coda: il numero di tabelle attualmente in attesa di essere caricate.
 - Tabelle con errori: il numero di tabelle che non sono state caricate.
 - Tempo trascorso: la quantità di tempo trascorsa dall'inizio della migrazione dei dati.
 - Latenza CDC: il tempo medio che intercorre tra il momento in cui si verifica una modifica su una tabella di origine e il momento in cui tale modifica viene AWS DMS applicata alla tabella di destinazione.
 - Migrazione iniziata: l'ora in cui hai avviato questa migrazione dei dati.
 - Migrazione arrestata: l'ora in cui hai interrotto questa migrazione dei dati.
5. Per visualizzare i file di registro per la migrazione dei dati, scegli Visualizza CloudWatch registri in Impostazioni di migrazione dei dati omogenee. Puoi attivare CloudWatch i log quando crei o modifichi una migrazione di dati. Per ulteriori informazioni, consulta [Creazione di una migrazione dei dati](#) e [Gestione delle migrazioni dei dati](#).

Puoi utilizzare gli CloudWatch allarmi o gli eventi di Amazon per monitorare da vicino la migrazione dei dati. Per ulteriori informazioni, consulta [Cosa sono Amazon CloudWatch, Amazon CloudWatch Events e Amazon CloudWatch Logs?](#) nella Amazon CloudWatch User Guide. Tieni presente che l'utilizzo di Amazon è a pagamento CloudWatch.

Per migrazioni di dati omogenee, AWS DMS include le seguenti metriche in Amazon. CloudWatch

Parametro	Descrizione
OverallCDCLatency	<p>La latenza complessiva durante la fase CDC.</p> <p>Per i database MySQL, questa metrica mostra il numero di secondi trascorsi tra la modifica del log binario di origine e la replica della modifica.</p> <p>Per i database PostgreSQL, questa metrica mostra il numero di secondi trascorsi tra <code>last_msg_receipt_time</code> e <code>last_msg_send_time</code> dalla vista <code>pg_stat_subscription</code>.</p> <p>Unità: secondi</p>
StorageConsumption	<p>Lo spazio di archiviazione utilizzato per la migrazione dei dati.</p> <p>Unità: byte</p>

Stati delle migrazioni di dati omogenee in AWS DMS

Per ogni migrazione di dati eseguita, AWS DMS visualizza lo stato nella console. AWS DMS L'elenco seguente include gli stati disponibili.

- **Creating**— AWS DMS sta creando la migrazione dei dati.
- **Ready**: la migrazione dei dati è pronta per iniziare.
- **Starting**— AWS DMS sta creando l'ambiente serverless per la migrazione dei dati. Questo processo può richiedere fino a 15 minuti.
- **Load running**— AWS DMS sta eseguendo la migrazione a pieno carico.
- **Load complete, replication ongoing**— AWS DMS ha completato il caricamento completo e ora replica le modifiche in corso. AWS DMS utilizza questo stato solo per le migrazioni di dati del tipo CDC (Full Load and Change Data Capture).

- **Replication ongoing**— AWS DMS sta replicando le modifiche in corso. AWS DMS utilizza questo stato solo per le migrazioni del tipo Change Data Capture (CDC).
- **Reloading target**— AWS DMS sta riavviando una migrazione dei dati ed esegue il tipo di migrazione specificato.
- **Stopping**— interrompe AWS DMS la migrazione dei dati. AWS DMS imposta questo stato dopo aver scelto di interrompere la migrazione dei dati nel menu Azioni.
- **Stopped**— AWS DMS ha interrotto la migrazione dei dati.
- **Failed**: la migrazione dei dati non è riuscita. Per ulteriori informazioni, consulta i file di log.

Per visualizzare i file di log, scegli la migrazione dei dati nella scheda Migrazioni dei dati. Successivamente, scegli Visualizza CloudWatch registri in Impostazioni di migrazione dei dati omogenee.

Important

Puoi visualizzare i file di registro se selezioni la casella di controllo Attiva CloudWatch i registri quando crei la migrazione dei dati.

- **Deleting**— AWS DMS sta eliminando la migrazione dei dati. AWS DMS imposta questo stato dopo aver scelto di eliminare la migrazione dei dati nel menu Azioni.

Migrazione dei dati dai database MySQL con migrazioni di dati omogenee in AWS DMS

È possibile utilizzare [Migrazioni di database omogenee](#) per migrare un database MySQL autogestito su RDS per MySQL o Aurora MySQL. AWS DMS crea un ambiente serverless per la migrazione dei dati. Per diversi tipi di migrazioni di dati, AWS DMS utilizza diversi strumenti di database MySQL nativi.

Per migrazioni di dati omogenee di tipo Full load, AWS DMS utilizza mydumper per leggere i dati dal database di origine e archivarli sul disco collegato all'ambiente serverless. Dopo aver AWS DMS letto tutti i dati di origine, utilizza myloader nel database di destinazione per ripristinare i dati.

Per migrazioni di dati omogenee di tipo Full load and change data capture (CDC), AWS DMS utilizza mydumper per leggere i dati dal database di origine e archivarli sul disco collegato all'ambiente serverless. Dopo aver AWS DMS letto tutti i dati di origine, utilizza myloader nel database di

destinazione per ripristinare i dati. Dopo aver AWS DMS completato il caricamento completo, imposta la replica binlog con la posizione binlog impostata all'inizio del caricamento completo. Per evitare incoerenze tra i dati, imposta su 1 Numero di processi per acquisire lo stato coerente dei dati esistenti. Per ulteriori informazioni, consulta [Creazione di una migrazione dei dati](#).

Per le migrazioni di dati omogenee del tipo Acquisizione dei dati di modifica (CDC), AWS DMS richiede il Punto di avvio CDC nativo per avviare la replica. Se fornisci il punto di partenza del CDC nativo, AWS DMS acquisisce le modifiche da quel punto. In alternativa, scegli Immediatamente nelle impostazioni della migrazione dei dati per acquisire automaticamente il punto di avvio per la replica all'inizio della migrazione effettiva dei dati.

Note

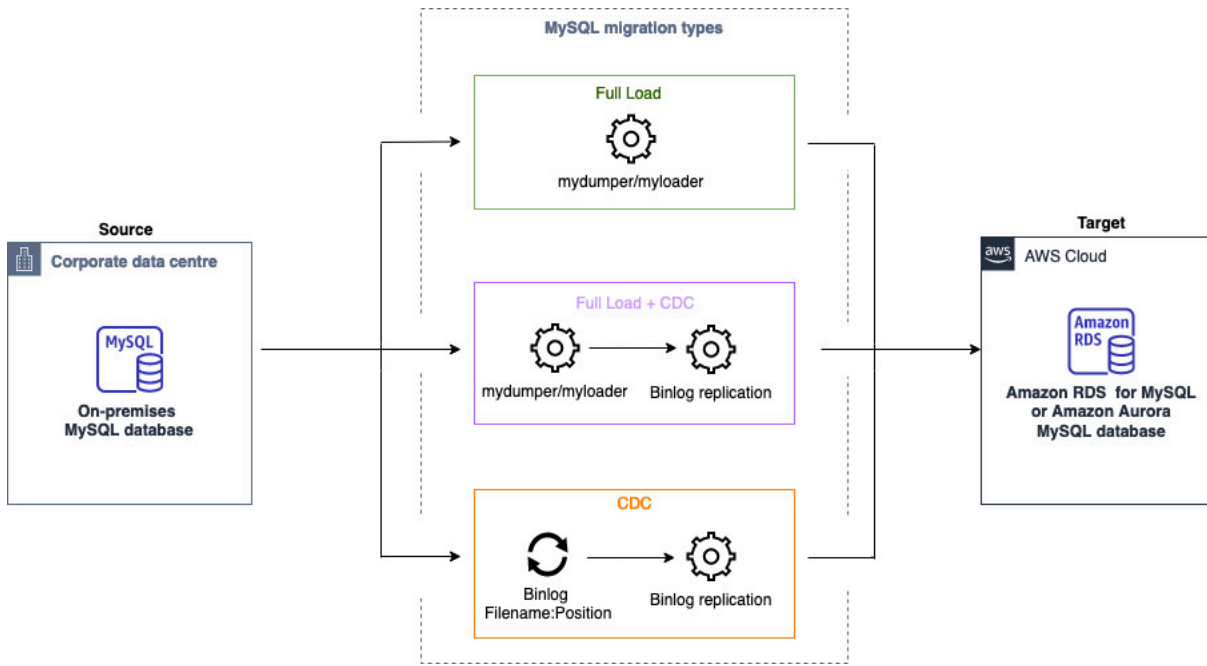
Affinché una migrazione sola CDC funzioni correttamente, tutti gli schemi e gli oggetti del database di origine devono essere già presenti nel database di destinazione. Tuttavia, la destinazione può avere oggetti che non sono presenti nell'origine.

È possibile utilizzare il seguente esempio di codice per ottenere il numero di sequenza di log (LSN) corrente nel database MySQL.

```
show master status
```

Questa query restituisce il nome e la posizione del file binlog. Il punto di avvio nativo è una combinazione del nome del file binlog e della posizione. Ad esempio, `mysql-bin-change1og.000024:373`. In questo esempio, `mysql-bin-change1og.000024` è il nome del file binlog ed `373` è la posizione in cui AWS DMS inizia l'acquisizione delle modifiche.

Il diagramma seguente mostra il processo di utilizzo di migrazioni di dati omogenee per migrare un database MySQL AWS DMS a RDS for MySQL o Aurora MySQL.



Migrazione dei dati dai database PostgreSQL con migrazioni di dati omogenee in AWS DMS

È possibile utilizzare [Migrazioni di database omogenee](#) per migrare un database PostgreSQL autogestito su RDS per PostgreSQL o Aurora PostgreSQL. AWS DMS crea un ambiente serverless per la migrazione dei dati. Per diversi tipi di migrazioni di dati, AWS DMS utilizza diversi strumenti di database PostgreSQL nativi.

Per migrazioni di dati omogenee di tipo Full load, AWS DMS utilizza `pg_dump` per leggere i dati dal database di origine e archivarli sul disco collegato all'ambiente serverless. Dopo aver AWS DMS letto tutti i dati di origine, utilizza `pg_restore` nel database di destinazione per ripristinare i dati.

Per migrazioni di dati omogenee del tipo Full load and change data capture (CDC), AWS DMS viene utilizzato `pg_dump` per leggere gli oggetti dello schema senza dati di tabella dal database di origine e archivarli sul disco collegato all'ambiente serverless. Viene quindi utilizzato `pg_restore` nel database di destinazione per ripristinare gli oggetti dello schema. Una volta AWS DMS completato il `pg_restore` processo, passa automaticamente a un modello di editore e sottoscrittore per la replica logica con la `Initial Data Synchronization` possibilità di copiare i dati della tabella iniziale direttamente dal database di origine al database di destinazione, quindi avvia la replica continua. In questo modello uno o più abbonati sottoscrivono una o più pubblicazioni su un nodo editore.

Per le migrazioni di dati omogenee di tipo Change data Capture (CDC), è AWS DMS necessario il punto di partenza nativo per avviare la replica. Se fornisci il punto di partenza nativo, AWS DMS

acquisisce le modifiche da quel punto. In alternativa, scegli **Immediatamente** nelle impostazioni della migrazione dei dati per acquisire automaticamente il punto di avvio per la replica all'inizio della migrazione effettiva dei dati.

Note

Affinché una migrazione sola CDC funzioni correttamente, tutti gli schemi e gli oggetti del database di origine devono essere già presenti nel database di destinazione. Tuttavia, la destinazione può avere oggetti che non sono presenti nell'origine.

È possibile utilizzare il seguente esempio di codice per ottenere il punto di avvio nativo nel database PostgreSQL.

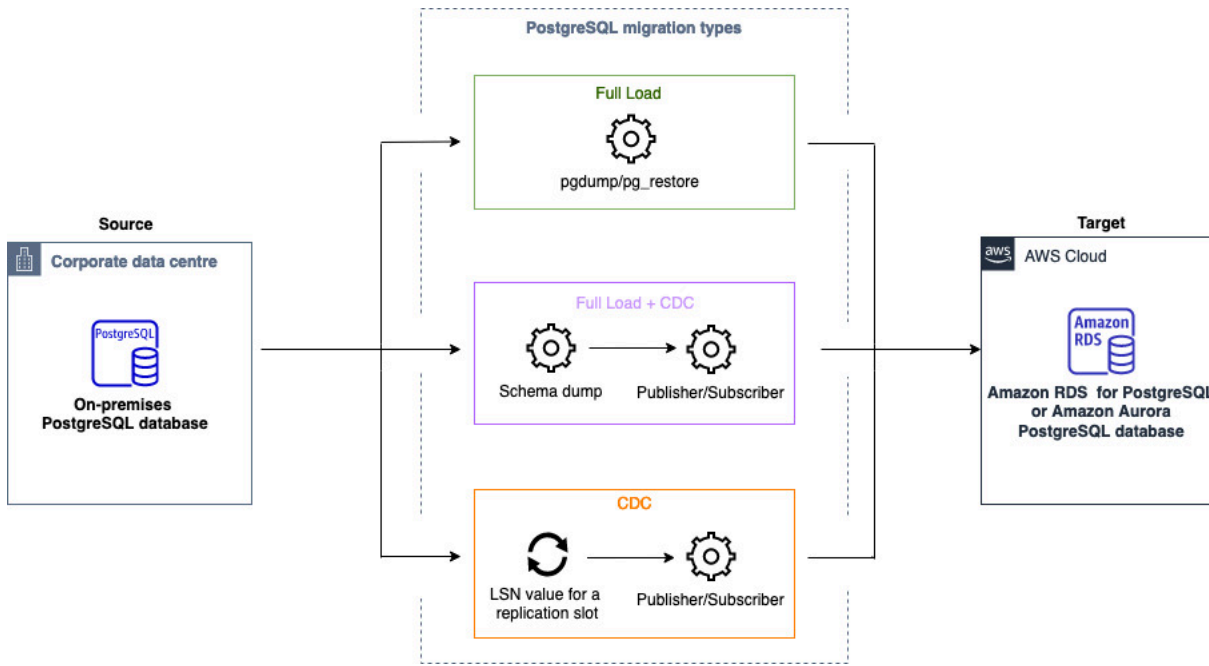
```
select confirmed_flush_lsn from pg_replication_slots where
slot_name='migrate_to_target';
```

Questa query utilizza la vista `pg_replication_slots` del database PostgreSQL per acquisire il valore del numero di sequenza di log (LSN).

Dopo aver AWS DMS impostato lo stato della migrazione omogenea dei dati di PostgreSQL su `Stopped`, `Failed` o `Deleted`, l'editore e la replica non vengono rimossi. Se non desideri riprendere la migrazione, elimina lo slot di replica e l'editore utilizzando il comando seguente.

```
SELECT pg_drop_replication_slot('migration_subscriber_{ARN}');
DROP PUBLICATION publication_{ARN};
```

Il diagramma seguente mostra il processo di utilizzo di migrazioni di dati omogenee per migrare un database PostgreSQL AWS DMS a RDS for PostgreSQL o Aurora PostgreSQL.



Migrazione dei dati dai database MongoDB con migrazioni di dati omogenee in AWS DMS

Puoi usarlo [Migrazioni di database omogenee](#) per migrare un database MongoDB autogestito su Amazon DocumentDB. AWS DMS crea un ambiente serverless per la migrazione dei dati. Per diversi tipi di migrazioni di dati, AWS DMS utilizza diversi strumenti di database MongoDB nativi.

Per migrazioni di dati omogenee di tipo Full load, AWS DMS viene utilizzato `mongodump` per leggere i dati dal database di origine e archivarli sul disco collegato all'ambiente serverless. Dopo aver AWS DMS letto tutti i dati di origine, li utilizza `mongoexport` nel database di destinazione per ripristinare i dati.

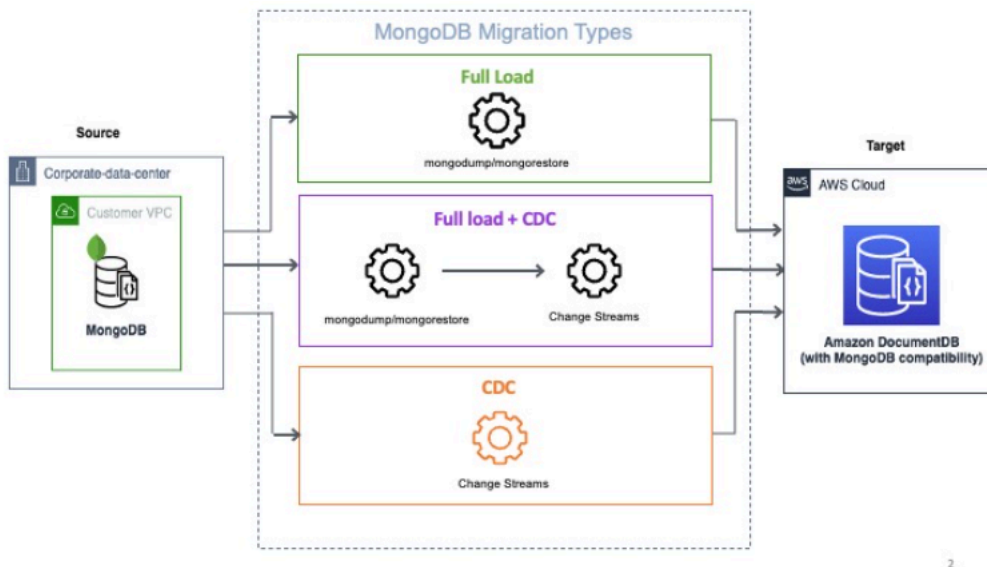
Per migrazioni di dati omogenee di tipo CDC (Full Load and Change Data Capture), AWS DMS viene utilizzato `mongodump` per leggere i dati dal database di origine e archivarli sul disco collegato all'ambiente serverless. Dopo aver AWS DMS letto tutti i dati di origine, li utilizza `mongoexport` nel database di destinazione per ripristinare i dati. Dopo aver AWS DMS completato il caricamento completo, passa automaticamente a un modello di editore e abbonato per la replica logica. In questo modello, si consiglia di ridimensionare l'oplog in modo da conservare le modifiche per almeno 24 ore.

Per migrazioni di dati omogenee del tipo Change data capture (CDC), scegli `immediately` nelle impostazioni di migrazione dei dati di acquisire automaticamente il punto di partenza per la replica all'inizio della migrazione effettiva dei dati.

Note

Per ogni raccolta nuova o rinominata, è necessario creare una nuova attività di migrazione dei dati per tali raccolte sotto forma di migrazioni di dati omogenee. Per un codice sorgente compatibile con MongoDB, AWS DMS non supporta operazioni `create`, `rename` `drop collection`

Il diagramma seguente mostra il processo di utilizzo di migrazioni di dati omogenee AWS DMS per migrare un database MongoDB in Amazon DocumentDB.



Risoluzione dei problemi relativi alle migrazioni di dati omogenee in AWS DMS

Nell'elenco seguente sono disponibili le azioni da intraprendere in caso di problemi con le migrazioni omogenee dei dati in AWS DMS.

Argomenti

- [Non riesco a creare una migrazione dei dati omogenea in AWS DMS](#)
- [Non riesco ad avviare una migrazione dei dati omogenea in AWS DMS](#)
- [Non riesco a connettermi al database di destinazione durante una migrazione dei dati in AWS DMS](#)
- [AWS DMS esegue la migrazione delle viste come tabelle in PostgreSQL](#)

Non riesco a creare una migrazione dei dati omogenea in AWS DMS

Se ricevi un messaggio di errore che indica che AWS DMS non è in grado di connettersi ai tuoi fornitori di dati dopo aver scelto Crea migrazione dei dati, assicurati di aver configurato il ruolo IAM necessario. Per ulteriori informazioni, consulta [Creazione di un ruolo IAM](#).

Se hai configurato il ruolo IAM e ricevi ancora questo messaggio di errore, aggiungi il ruolo IAM al tuo utente chiave nella configurazione della chiave AWS KMS. Per ulteriori informazioni, consulta [Consente agli utenti della chiave di utilizzare la chiave KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service.

Non riesco ad avviare una migrazione dei dati omogenea in AWS DMS

Se vedi lo stato `Failed` quando avvii una migrazione dei dati nell'ambito del tuo progetto di migrazione, controlla le versioni dei fornitori di dati di origine e di destinazione. A questo scopo, esegui la query `SELECT VERSION()`; nel database MySQL o PostgreSQL. Assicurati di utilizzare la versione del database supportata.

Per l'elenco dei database di origine supportati, consulta [Origini per migrazioni omogenee di dati DMS](#).

Per l'elenco dei database di destinazione supportati, consulta [Destinazioni per migrazioni omogenee di dati DMS](#).

Se utilizzi una versione del database non supportata, aggiorna il database di origine o di destinazione e riprova.

Controlla il messaggio di errore relativo alla migrazione dei dati nella console AWS DMS. Per farlo, apri il tuo progetto di migrazione e scegli la migrazione dei dati. Nella scheda Dettagli, seleziona Ultimo messaggio di errore in Generale.

Infine, analizza il log di CloudWatch. Per farlo, apri il tuo progetto di migrazione e scegli la migrazione dei dati. Nella scheda Dettagli scegli Visualizza i log di CloudWatch.

Non riesco a connettermi al database di destinazione durante una migrazione dei dati in AWS DMS

Se ricevi il messaggio di errore `Unable to connect to target` esegui le seguenti azioni.

1. Assicurati che il gruppo di sicurezza collegato ai database di origine e di destinazione contenga una regola per il traffico in entrata e in uscita. Per ulteriori informazioni, consulta [Configurazione della replica continua dei dati](#).

2. Verifica la lista di controllo degli accessi (ACL) di rete e le regole della tabella di routing.
3. Il database deve essere accessibile dal VPC che hai creato. Aggiungi gli indirizzi IP pubblici nei gruppi di sicurezza VPC e consenti le connessioni di input nel firewall.
4. Nella scheda Migrazioni dei dati del tuo progetto di migrazione, scegli la migrazione dei dati. Prendi nota dell'indirizzo IP pubblico in Connettività e sicurezza nella scheda Dettagli. Successivamente, consenti l'accesso dall'indirizzo IP pubblico della migrazione dei dati nei database di origine e di destinazione.
5. Per la replica continua dei dati, assicurati che i database di origine e di destinazione possano comunicare tra loro.

Per ulteriori informazioni, consulta [Controlla il traffico verso le risorse utilizzando gruppi di sicurezza](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

AWS DMS esegue la migrazione delle viste come tabelle in PostgreSQL

La migrazione omogenea dei dati non supporta la migrazione delle viste come viste in PostgreSQL. Per PostgreSQL, AWS DMS esegue la migrazione delle viste come tabelle.

Collaborazione con fornitori di dati, profili di istanza e progetti di migrazione in AWS DMS

Quando utilizzi DMS Schema Conversion e migrazioni di dati omogenee in AWS Database Migration Service, lavori con progetti di migrazione. A loro volta, i progetti di migrazione AWS DMS utilizzano gruppi di sottoreti, profili dell'istanza e fornitori di dati.

una sottorete è un intervallo di indirizzi IP nel VPC; Un gruppo di sottoreti di replica include sottoreti provenienti da diverse zone di disponibilità che il profilo dell'istanza può utilizzare. Tieni presente che un gruppo di sottoreti di replica è una risorsa DMS e si distingue dai gruppi di sottoreti utilizzati da Amazon VPC e Amazon RDS.

Un profilo dell'istanza specifica le impostazioni di rete e di sicurezza per l'ambiente serverless in cui viene eseguito il progetto di migrazione.

Un fornitore di dati archivia un tipo di datastore e le informazioni sulla posizione del database. Dopo aver aggiunto un provider di dati al progetto di migrazione, fornisci le credenziali del database da AWS Secrets Manager. AWS DMS utilizza queste informazioni per connettersi al database.

Dopo aver creato i provider di dati, il profilo dell'istanza e altre AWS risorse, puoi creare un progetto di migrazione. Un progetto di migrazione descrive il profilo dell'istanza, i fornitori di dati di origine e di destinazione e i segreti di AWS Secrets Manager. Puoi creare più progetti di migrazione per diversi fornitori di dati di origine e di destinazione.

La maggior parte del lavoro avviene nel progetto di migrazione. Per la conversione dello schema DMS, si utilizza un progetto di migrazione per valutare gli oggetti del fornitore di dati di origine e convertirli in un formato compatibile con il database di destinazione. È quindi possibile applicare il codice convertito al fornitore di dati di destinazione o salvarlo come script SQL. Per migrazioni di dati omogenee, si utilizza un progetto di migrazione per migrare i dati dal database di origine a un database di destinazione dello stesso tipo nel Cloud AWS.

I progetti di migrazione in AWS DMS sono solo serverless. AWS DMS effettua automaticamente il provisioning delle risorse cloud per i tuoi progetti di migrazione.

AWS DMS dispone del numero massimo di profili di istanza, fornitori di dati e progetti di migrazione che puoi creare per i tuoi Account AWS. Per informazioni sulle quote di servizio di AWS DMS , consulta [Quote per AWS Database Migration Service](#).

Argomenti

- [Creazione di un gruppo di sottoreti per un progetto di AWS DMS migrazione](#)
- [Creazione di profili di istanza per AWS Database Migration Service](#)
- [Creazione di fornitori di dati in AWS Database Migration Service](#)
- [Creazione di progetti di migrazione in AWS Database Migration Service](#)
- [Gestione dei progetti di migrazione in AWS Database Migration Service](#)

Creazione di un gruppo di sottoreti per un progetto di AWS DMS migrazione

Prima di creare un profilo dell'istanza, configura un gruppo di sottoreti per il tuo profilo dell'istanza.

Per creare un gruppo di sottoreti

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione, scegli Gruppi di sottoreti, quindi Crea gruppo di sottoreti.
3. Per Nome immetti un nome univoco per il gruppo di sottoreti.
4. Per Descrizione immetti una descrizione del gruppo di sottoreti.
5. Per VPC scegli un VPC con almeno una sottorete in almeno due zone di disponibilità.
6. Per Aggiungi sottoreti scegli le sottoreti da includere nel gruppo di sottoreti. È necessario selezionare le sottoreti in almeno due zone di disponibilità.

Per connetterti ai database Amazon RDS, aggiungi sottoreti pubbliche al tuo gruppo di sottoreti.
Per connetterti ai database on-premise, aggiungi sottoreti private al tuo gruppo di sottoreti.

7. Scegli Crea gruppo di sottoreti.

Creazione di profili di istanza per AWS Database Migration Service

È possibile creare più profili di istanza nella AWS DMS console. Assicurati di selezionare un profilo dell'istanza da utilizzare per ogni progetto di migrazione che crei in AWS DMS.

Come creare un profilo dell'istanza

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

2. Nel riquadro di navigazione scegli Profili dell'istanza.
3. Seleziona Crea profilo dell'istanza.
4. Nella pagina Crea profilo dell'istanza immetti in Nome un valore descrittivo per il tuo profilo dell'istanza.
5. Per Tipo di rete scegli Modalità dual-stack per creare un profilo dell'istanza che supporti gli indirizzi IPv4 e IPv6. Mantieni l'opzione predefinita per creare un profilo dell'istanza che supporti solo gli indirizzi IPv4.
6. Quindi, scegli Cloud privato virtuale (VPC) per eseguire l'istanza del tipo di rete selezionato. Seleziona un Gruppo di sottoreti e i Gruppi di sicurezza VPC per il profilo dell'istanza.

Per connetterti ai database Amazon RDS, utilizza un gruppo di sottoreti che includa sottoreti pubbliche. Per connetterti ai database on-premise, usa un gruppo di sottoreti che includa sottoreti private. Assicurati di aver configurato la rete in modo da AWS DMS poter accedere al database locale di origine utilizzando l'indirizzo IP pubblico del gateway NAT. Per ulteriori informazioni, consulta [Creazione di un VPC basato su Amazon VPC](#).

7. (Facoltativo) Se crei un progetto di migrazione per la conversione dello schema DMS, scegli per Impostazioni di conversione dello schema un bucket Amazon S3 per archiviare le informazioni del tuo progetto di migrazione. Quindi scegli il ruolo AWS Identity and Access Management (IAM) che fornisce l'accesso a questo bucket Amazon S3. Per ulteriori informazioni, consulta [Creazione di un bucket Amazon S3](#).
8. Seleziona Crea profilo dell'istanza.

Dopo aver creato il profilo dell'istanza, sarà possibile modificarlo o eliminarlo.

Per modificare un profilo dell'istanza

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegliere Instance profiles (Profili delle istanze). Si apre la pagina Profili dell'istanza.
3. Scegli il profilo dell'istanza e seleziona Modifica.
4. Aggiorna il nome del profilo dell'istanza, modifica le impostazioni del VPC o del bucket Amazon S3.
5. Seleziona Salvataggio delle modifiche.

Per eliminare un profilo dell'istanza

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegliere Instance profiles (Profili delle istanze). Si apre la pagina Profili dell'istanza.
3. Scegli il profilo dell'istanza e seleziona Elimina.
4. Seleziona Elimina per confermare la scelta.

Creazione di fornitori di dati in AWS Database Migration Service

Puoi creare fornitori di dati e utilizzarli in progetti di AWS DMS migrazione. Il fornitore di dati può essere un motore autogestito in esecuzione on-premise o su un'istanza Amazon EC2. Inoltre, il fornitore di dati può essere un motore completamente gestito, come Amazon Relational Database Service (Amazon RDS) o Amazon Aurora.

Per ogni database puoi creare un singolo fornitore di dati. Puoi utilizzare un singolo fornitore di dati in più progetti di migrazione.

Prima di creare un progetto di migrazione, assicurati di aver creato almeno due fornitori di dati. Uno dei tuoi fornitori di dati deve utilizzare un Servizio AWS. Non puoi utilizzare AWS DMS per convertire i tuoi schemi o migrare i tuoi dati in un database on-premise.

La procedura seguente mostra come creare fornitori di dati nella procedura guidata della AWS DMS console.

Per creare un fornitore di dati

1. Accedere a AWS Management Console, quindi aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Fornitori di dati. Viene visualizzata la pagina Fornitori di dati.
3. Scegli Crea un fornitore di dati. Nella tabella seguente vengono illustrate le impostazioni.

Opzione	Azione
Configurazione	Scegli se inserire le informazioni sul fornitore di dati manualmente o utilizzare l'istanza database Amazon RDS.

Opzione	Azione
Nome	Immetti un nome per il fornitore di dati. Assicurati di utilizzar e un nome univoco per il fornitore di dati in modo da poterlo identificare facilmente.
Tipo di motore	Scegli il tipo di motore di database per il fornitore di dati.
Server name (Nome del server)	Immetti il nome Domain Name Service (DNS) o l'indirizzo IP del server del database. Il nome del server per un fornitore di dati utilizzato per una replica omogenea deve iniziare con un carattere alfanumerico e può contenere solo caratteri alfanumerici, trattini (-), punti (.) o caratteri di sottolineatura (_).
Porta	Immetti la porta utilizzata per la connessione al server del database.
ID del servizio (SID) o nome del servizio	Immetti l'ID del sistema (SID) Oracle. Per individuare il SID Oracle, invia la seguenti query al database Oracle: <div style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; margin: 10px 0;"> <pre>SELECT sys_context('userenv', 'instance_name') AS SID FROM dual;</pre> </div>
Nome del database	Immetti il nome del database per questo fornitore di dati. Il nome del database di un fornitore di dati utilizzato per una replica omogenea può includere fino a 63 caratteri, ma non può contenere spazi.
Modalità Secure Socket Layer (SSL)	Scegli una modalità SSL se desideri attivare la crittografia della connessione per il fornitore di dati. A seconda della modalità selezionata, potresti dover fornire informazioni sul certificato e sul certificato server. Per ulteriori dettagli, consulta Usare SSL con AWS Database Migration Service .
Modalità di autenticazione	Per una fonte MongoDB, la modalità di autenticazione utilizzata per autenticare la AWS DMS connessione all'endpo int.

Opzione	Azione
Origine di autenticazione	Per una fonte MongoDB, il nome del database MongoDB da utilizzare per convalidare le credenziali per l'autenticazione.
Meccanismo di autenticazione	Per una fonte MongoDB, il metodo di autenticazione utilizzato da MongoDB per crittografare la password.

4. Scegli Crea un fornitore di dati.

Dopo aver creato un fornitore di dati, assicurati di aggiungere le credenziali di connessione al database in AWS Secrets Manager.

Creazione di progetti di migrazione in AWS Database Migration Service

Prima di creare un progetto di migrazione in AWS DMS, assicurati di creare le seguenti risorse:

- Fornitori di dati che descrivono i database di origine e di destinazione
- Segreti con credenziali del database archiviate in AWS Secrets Manager
- Il ruolo AWS Identity and Access Management (IAM) che fornisce l'accesso a Secrets Manager
- Un profilo dell'istanza che include le impostazioni di rete e sicurezza

Per creare un progetto di migrazione

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli Crea un progetto di migrazione. Nella tabella seguente vengono illustrate le impostazioni.

Opzione	Azione
Nome	Immetti un nome per il progetto di migrazione. Assicurati di utilizzare un nome univoco per il progetto di migrazione in modo da poterlo identificare facilmente.

Opzione	Azione
Profilo dell'istanza	Scegli il profilo dell'istanza da utilizzare per il progetto di migrazione.
Origine	Scegli Sfogliare, quindi seleziona il fornitore di dati di origine.
ID segreto	Scegli il nome della risorsa Amazon (ARN) del segreto in Secrets Manager che archivia le credenziali del database di origine.
Ruolo IAM	Scegli un ruolo IAM per fornire l'accesso alle credenziali del database di origine in Secrets Manager.
Target	Scegli Sfogliare, quindi seleziona il fornitore di dati di origine.
ID segreto	Scegli l'ARN del segreto in Secrets Manager che archivia le credenziali del database di destinazione.
Ruolo IAM	Scegli un ruolo IAM per fornire l'accesso alle credenziali del database di destinazione in Secrets Manager.
Regole di trasformazione	(Facoltativo) Se crei un progetto di migrazione per la conversione dello schema DMS, scegli Aggiungi regola di trasformazione per impostare le regole di trasformazione. Le regole di trasformazione consentono di modificare i nomi degli oggetti in base alla regola specificata. Per ulteriori informazioni, consulta Configurazione delle regole di trasformazione .

4. Scegli Crea un progetto di migrazione.

Dopo aver AWS DMS creato il progetto di migrazione, puoi utilizzare questo progetto nella conversione dello schema DMS o nelle migrazioni di dati omogenee. Per iniziare a utilizzare il progetto di migrazione, selezionalo nell'elenco nella pagina Progetti di migrazione.

Gestione dei progetti di migrazione in AWS Database Migration Service

Dopo aver creato il progetto di migrazione, è possibile modificarlo o eliminarlo. Ad esempio, puoi modificare il progetto di migrazione per cambiare il fornitore di dati di origine o di destinazione.

È possibile modificare o eliminare il progetto di migrazione solo dopo aver chiuso le operazioni di conversione dello schema o di migrazione dei dati. A tale scopo, scegli il progetto di migrazione dall'elenco e seleziona Conversione dello schema o Migrazioni dei dati. Quindi, seleziona Chiudi conversione dello schema per la conversione dello schema DMS e conferma la tua scelta. Per le migrazioni di dati omogenee, scegli la migrazione dei dati, quindi seleziona Interrompi dal menu Operazioni. Dopo aver modificato il progetto di migrazione, puoi avviare la conversione dello schema o ripetere la migrazione dei dati.

Per modificare un progetto di migrazione

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Modifica.
4. Aggiorna il nome del progetto, modifica il profilo dell'istanza o cambia i fornitori di dati di origine e di destinazione. Facoltativamente, aggiungi o modifica le regole di migrazione che cambiano i nomi degli oggetti durante la conversione.
5. Seleziona Salvataggio delle modifiche.

Per eliminare un progetto di migrazione

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Progetti di migrazione. Viene visualizzata la pagina Progetti di migrazione.
3. Scegli il progetto di migrazione, quindi seleziona Elimina.
4. Seleziona Elimina per confermare la scelta.

Best practice per AWS Database Migration Service

Per utilizzare AWS Database Migration Service (AWS DMS) in modo più efficiente, consulta i consigli in questa sezione sul modo più efficiente per migrare i dati.

Argomenti

- [Pianificazione della migrazione di AWS Database Migration Service](#)
- [Conversione dello schema](#)
- [Revisione della documentazione pubblica di AWS DMS](#)
- [Esecuzione di un proof of concept](#)
- [Miglioramento delle prestazioni di una migrazione AWS DMS](#)
- [Utilizzo del server dei nomi in locale](#)
- [Migrazione di oggetti binari di grandi dimensioni \(LOB\)](#)
- [Miglioramento delle prestazioni per la migrazione di tabelle di grandi dimensioni usando il filtro di riga](#)
- [La replica continua](#)
- [Riduzione del carico del database di origine](#)
- [Riduzione dei colli di bottiglia sul database di destinazione](#)
- [Utilizzo della convalida dei dati durante la migrazione](#)
- [Monitoraggio delle attività AWS DMS tramite i parametri](#)
- [Eventi e notifiche](#)
- [Utilizzo del log delle attività per risolvere i problemi relativi alla migrazione](#)
- [Risoluzione dei problemi delle attività di replica con Time Travel](#)
- [Modifica dell'utente e dello schema per una destinazione Oracle](#)
- [Modifica di spazi di tabella per tabelle e indici di una destinazione Oracle](#)
- [Aggiornamento della versione di un'istanza di replica](#)
- [Comprensione dei costi di migrazione](#)

Pianificazione della migrazione di AWS Database Migration Service

Durante la pianificazione della migrazione di un database tramite AWS Database Migration Service, considera quando segue:

- Dovrai configurare una rete per connettere i database di origine e di destinazione a un'istanza di replica AWS DMS. Per eseguire questa operazione, è sufficiente collegare due risorse AWS nello stesso cloud privato virtuale (VPC) dell'istanza di replica. Tuttavia puoi anche eseguire configurazioni più complesse, come la connessione di un database on-premise a un'istanza database Amazon RDS tramite una rete privata virtuale (VPN). Per ulteriori informazioni, consulta [Configurazioni di rete per la migrazione del database](#).
- Endpoint di origine e di destinazione: dovrai sapere quali informazioni e tabelle del database di origine devono essere migrate al database di destinazione. AWS DMS supporta la migrazione dello schema di base, inclusa la creazione di tabelle e chiavi primarie. Tuttavia, AWS DMS non crea automaticamente nel database di destinazione gli indici secondari, le chiavi esterne, gli account utente e così via. A seconda del motore di database di origine e di destinazione, può essere necessario configurare un log supplementare o modificare altre impostazioni per il database di origine o di destinazione. Per ulteriori informazioni, consultare [Origini per la migrazione dei dati](#) e [Destinazioni per la migrazione dei dati](#).
- Migrazione di schema e codice: AWS DMS non esegue la conversione dello schema o del codice. Puoi utilizzare strumenti quali Oracle SQL Developer, MySQL Workbench e pgAdmin III per convertire lo schema. Se desideri convertire uno schema esistente in un altro motore di database, puoi utilizzare AWS Schema Conversion Tool (AWS SCT). Questo strumento può creare e generare uno schema di destinazione per intero con tabelle, indici, viste e così via. Puoi inoltre utilizzare lo strumento per la conversione di PL/SQL o TSQL in PostgreSQL e altri formati. Per ulteriori informazioni su AWS SCT, consulta la [Guida per l'utente di AWS SCT](#).
- Tipi di dati non supportati: alcuni tipi di dati di origine devono essere convertiti nei tipi di dati equivalenti per il database di destinazione. Per ulteriori informazioni sui tipi di dati supportati, consulta la sezione relativa all'origine o alla destinazione del datastore.
- Risultati degli script di supporto diagnostico: quando pianifichi la migrazione, ti consigliamo di eseguire gli script di supporto diagnostico. Con i risultati di questi script, puoi individuare in anticipo informazioni sui potenziali errori di migrazione.

Se è disponibile uno script di supporto per il tuo database, scaricalo utilizzando il collegamento presente nell'argomento dello script corrispondente nella sezione seguente. Dopo aver verificato e esaminato lo script, è possibile eseguirlo secondo la procedura descritta nell'argomento dello script nel proprio ambiente locale. Al termine dell'esecuzione dello script, è possibile esaminare i risultati. Ti consigliamo di eseguire questi script come prima fase di qualsiasi operazione di risoluzione dei problemi. I risultati possono essere utili quando si lavora con il team AWS Support. Per ulteriori informazioni, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

- Valutazioni preliminari alla migrazione: una valutazione preliminare alla migrazione analizza i componenti specifici di un'attività di migrazione del database per identificare eventuali problemi che potrebbero impedire l'esecuzione dell'attività di migrazione come previsto. Utilizzando questa valutazione è possibile identificare potenziali problemi prima di eseguire un'attività nuova o modificata. Per ulteriori informazioni sull'utilizzo delle valutazioni preliminari alla migrazione, consulta [Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività](#).

Conversione dello schema

AWS DMS non esegue la conversione dello schema o del codice. Per convertire uno schema esistente in un motore di database diverso puoi utilizzare AWS SCT. AWS SCT converte gli oggetti di origine, la tabella, gli indici, le viste, i trigger e altri oggetti di sistema nel formato DDL (Data Definition Language) di destinazione. AWS SCT può essere usato anche per convertire la maggior parte del codice dell'applicazione, ad esempio PL/SQL o TSQL, nel linguaggio di destinazione equivalente.

AWS SCT si scarica gratuitamente da AWS. Per ulteriori informazioni su AWS SCT, consulta la [Guida per l'utente di AWS SCT](#).

Se gli endpoint di origine e di destinazione si trovano sullo stesso motore di database, puoi utilizzare strumenti come Oracle SQL Developer, MySQL Workbench PgAdmin o 4 per spostare lo schema.

Revisione della documentazione pubblica di AWS DMS

Ti consigliamo vivamente di consultare le pagine della documentazione pubblica di AWS DMS in relazione agli endpoint di origine e di destinazione prima di eseguire la prima migrazione. Questa documentazione può aiutarti a identificare i prerequisiti della migrazione e comprendere le limitazioni attuali prima di iniziare. Per ulteriori informazioni, consulta [Utilizzo degli endpoint AWS DMS](#).

Durante la migrazione, la documentazione pubblica può aiutarti a risolvere eventuali problemi relativi ad AWS DMS. Le pagine della risoluzione dei problemi della documentazione ti consentono di risolvere i problemi più comuni utilizzando AWS DMS e i database degli endpoint selezionati. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi alle attività di migrazione in AWS Database Migration Service](#).

Esecuzione di un proof of concept

Per facilitare l'individuazione dei problemi relativi all'ambiente nelle prime fasi della migrazione del database, ti consigliamo di eseguire una piccola migrazione di prova. In questo modo puoi anche

impostare una tempistica di migrazione più realistica. Inoltre, potrebbe essere necessario eseguire una migrazione di prova completa per valutare se AWS DMS gestisce la velocità di trasmissione effettiva del database sulla rete. Durante questa attività ti consigliamo di eseguire il benchmark e ottimizzare il pieno carico iniziale e la replica continua. In questo modo puoi comprendere la latenza della rete e valutare le prestazioni complessive.

Inoltre, hai anche l'opportunità di capire il tuo profilo di dati e le dimensioni del database, tra cui:

- quante tabelle sono di dimensioni grandi, medie e piccole;
- in che modo AWS DMS gestisce le conversioni dei tipi di dati e dei set di caratteri;
- quante tabelle hanno colonne di oggetti di grandi dimensioni (LOB);
- quanto tempo è necessario per eseguire una migrazione di prova.

Miglioramento delle prestazioni di una migrazione AWS DMS

Le prestazioni della migrazione AWS DMS sono influenzate da una serie di fattori:

- la disponibilità di risorse nell'origine;
- la velocità di trasmissione effettiva della rete disponibile;
- la capacità di risorse del server di replica;
- la possibilità della destinazione di acquisire le modifiche;
- il tipo e la distribuzione dei dati di origine;
- il numero di oggetti da migrare.

È possibile migliorare le prestazioni utilizzando alcune o tutte le best practice riportate di seguito. La possibilità di utilizzare una di queste procedure dipende dal caso d'uso specifico. Di seguito sono riportate alcune limitazioni.

Provisioning di un server di replica appropriato

AWS DMS è un servizio gestito che viene eseguito su un'istanza Amazon EC2. Il servizio si connette al database di origine, legge i dati di origine, formatta i dati per l'utilizzo da parte del database di destinazione e carica i dati nel database di destinazione.

La maggior parte di questo processo si verifica in memoria. Tuttavia, per le transazioni di grandi dimensioni potrebbe essere necessario il buffering su disco. Anche le transazioni e i file di

log memorizzati nella cache vengono scritti su disco. Nelle seguenti sezioni sono disponibili informazioni sui fattori da considerare nella scelta del server di replica.

CPU

AWS DMS è progettato per migrazioni eterogenee, ma supporta anche migrazioni omogenee. Per eseguire una migrazione omogenea, occorre innanzitutto convertire ogni tipo di dati di origine nel tipo di dati AWS DMS equivalente. Quindi, è necessario convertire ogni tipo di dati AWS DMS nel tipo di dati di destinazione. I riferimenti delle conversioni per ogni motore di database sono disponibili nella Guida per l'utente di AWS DMS.

AWS DMS esegue queste conversioni in modo ottimale quando la CPU è disponibile al momento delle conversioni. Il sovraccarico e la mancanza di risorse sufficienti della CPU possono causare migrazioni lente che possono anche provocare altri effetti collaterali.

Classe di istanza di replica

Alcune delle classi di istanze più piccole sono sufficienti per testare il servizio o per migrazioni di piccole dimensioni. Se la migrazione coinvolge un numero elevato di tabelle oppure se desideri eseguire diverse attività di replica simultaneamente, puoi valutare l'utilizzo di un'istanza di dimensioni maggiori. Un'istanza di dimensioni maggiori può essere l'ideale perché il servizio utilizza la giusta quantità di memoria e CPU.

Le istanze di tipo T2 sono progettate per offrire prestazioni di base moderate e garantire prestazioni notevolmente maggiori se il carico di lavoro lo richiede. Sono concepite per carichi di lavoro che non utilizzano completamente la CPU spesso o in maniera regolare, ma che occasionalmente necessitano di un incremento delle prestazioni. Le istanze T2 sono particolarmente adatte per carichi di lavoro a scopo generico, come server Web, ambienti di sviluppo e piccoli database. Se per risolvere i problemi relativi a una migrazione lenta utilizzi un tipo di istanza T2, controlla il parametro dell'host relativo all'utilizzo della CPU in quanto può indicarti se stai superando i valori di base per quel tipo di istanza.

Le classi di istanze C4 sono state concepite per fornire il livello più elevato di prestazioni del processore per i carichi di lavoro che richiedono un'elevata capacità di elaborazione. Raggiungono prestazioni significativamente più elevate in termini di pacchetti al secondo (PPS) e offrono minore instabilità di rete e minore latenza di rete. AWS DMS può richiedere un uso intensivo della CPU, soprattutto quando si eseguono migrazioni e repliche eterogenee, come la migrazione da Oracle a PostgreSQL. In questi casi, le istanze C4 possono rappresentare una scelta adeguata.

Le classi di istanze R4 sono ottimizzate per carichi di lavoro di database a memoria elevata. Le migrazioni o le repliche continue di sistemi di transazioni con velocità di trasmissione effettiva elevata che usano AWS DMS possono a volte utilizzare grandi quantità di CPU e memoria. Le istanze R4 includono una maggiore quantità di memoria per vCPU.

Supporto di AWS DMS per le classi di istanza R5 e C5

Le classi di istanza R5 includono istanze ottimizzate per la memoria che offrono prestazioni elevate per carichi di lavoro che elaborano in memoria set di dati di grandi dimensioni. Le migrazioni o le repliche continue di sistemi di transazioni con velocità di trasmissione effettiva elevata che usano AWS DMS possono a volte utilizzare grandi quantità di CPU e memoria. Le istanze R5 offrono il 5% di memoria aggiuntiva per vCPU rispetto alle istanze R4 e la dimensione più elevata fornisce 768 GiB di memoria. Inoltre, le istanze R5 consentono un miglioramento del prezzo per GiB del 10% e un aumento delle prestazioni della CPU di circa il 20% rispetto alle istanze R4.

Le classi di istanze C5 sono ottimizzate per carichi di lavoro ad alta intensità di calcolo e offrono prestazioni elevate a costi contenuti a un basso rapporto prezzo/elaborazione. Raggiungono prestazioni di rete notevolmente superiori. L'Adattatore elastico di rete (ENA) fornisce istanze C5 con un massimo di 25 Gbps di larghezza di banda della rete e fino a 14 Gbps di larghezza di banda dedicata ad Amazon EBS. AWS DMS può richiedere un uso intensivo della CPU, soprattutto quando si eseguono migrazioni e repliche eterogenee, come la migrazione da Oracle a PostgreSQL. In questi casi, le istanze C5 possono rappresentare una scelta adeguata.

Storage

In base alla classe di istanza, il server di replica dispone di 50 GB o 100 GB di archiviazione di dati. Questo spazio di archiviazione viene utilizzato per i file di log e per tutte le modifiche memorizzate nella cache raccolte durante il caricamento. Se il sistema di origine è occupato o richiede transazioni di grandi dimensioni, potrebbe essere necessario aumentare lo spazio di archiviazione. Anche se si eseguono più attività sul server di replica, potrebbe essere necessario aumentare lo spazio di archiviazione. Tuttavia, la quantità predefinita è generalmente sufficiente.

Tutti i volumi di archiviazione in AWS DMS sono GP2 o unità di memoria a stato solido (SSD) per uso generico. I volumi GP2 offrono prestazioni di base di tre operazioni di I/O al secondo (IOPS), con capacità di arrivare fino a 3.000 IOPS su una base di credito. Come regola generale, controlla i parametri `ReadIOPS` e `WriteIOPS` e per l'istanza di replica. Assicurati che la somma di questi valori non superi le prestazioni di base del volume.

Multi-AZ

La scelta di un'istanza Multi-AZ può proteggere la migrazione dagli errori di archiviazione. La maggior parte delle migrazioni sono transitorie e non sono destinate a durare per lunghi periodi di tempo. Se si utilizza AWS DMS per scopi di replica continua, la scelta di un'istanza Multi-AZ può migliorare la disponibilità in caso di problemi di archiviazione.

Quando si utilizza un'istanza di replica singola AZ o multi-AZ durante un FULL LOAD e si verifica un failover o la sostituzione dell'host, si prevede che l'attività di pieno carico abbia esito negativo. È possibile riavviare l'attività dal punto di errore per le tabelle rimanenti che non sono state completate o che si trovano in uno stato di errore.

Caricamento di più tabelle in parallelo

Per impostazione predefinita, AWS DMS carica otto tabelle alla volta. È possibile ottenere un miglioramento delle prestazioni aumentando leggermente tale numero quando si usa un server di replica di dimensioni molto grandi, ad esempio un'istanza `dms.c4.xlarge` o maggiore. Tuttavia, in un determinato momento, l'aumento di questo parallelismo riduce le prestazioni. Se il server di replica è relativamente piccolo, ad esempio un `dms.t2.medium`, ti consigliamo di ridurre il numero di tabelle caricate in parallelo.

Per modificare questo numero nella AWS Management Console, apri la console, seleziona Attività, scegli di creare o modificare un'attività, quindi seleziona Impostazioni avanzate. In Tuning Settings (Impostazioni di tuning), modifica l'opzione Maximum number of tables to load in parallel (Numero massimo di tabelle da caricare in parallelo).

Per cambiare questo numero utilizzando la AWS CLI, modifica il parametro `MaxFullLoadSubTasks` in `TaskSettings`.

Utilizzo del pieno carico parallelo

È possibile utilizzare il caricamento parallelo dalle origini Oracle, Microsoft SQL Server, MySQL, Sybase e IBM Db2 LUW in base a partizioni e sottopartizioni. In questo modo è possibile migliorare la durata complessiva del pieno carico. Inoltre, durante l'esecuzione di un'attività di migrazione AWS DMS, è possibile accelerare la migrazione delle tabelle di grandi dimensioni o partizionate. Per farlo, dividi la tabella in segmenti e carica i segmenti in parallelo nella stessa attività di migrazione.

Per utilizzare il caricamento in parallelo, è necessario creare una regola di mappatura della tabella di tipo `table-settings` con l'opzione `parallel-load`. Nella regola `table-settings`, è necessario specificare i criteri di selezione per la tabella o le tabelle che desideri caricare in

parallelo. Per specificare i criteri di selezione, imposta l'elemento `type` per `parallel-load` su una delle impostazioni seguenti:

- `partitions-auto`
- `subpartitions-auto`
- `partitions-list`
- `ranges`
- `none`

Per ulteriori informazioni su queste impostazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Utilizzo di indici, trigger e vincoli di integrità referenziale

Gli indici, i trigger e i vincoli di integrità referenziale possono influenzare le prestazioni di migrazione e impedirne il completamento. Il modo in cui ciò influenza la migrazione dipende dal fatto che l'attività di replica sia un'attività di pieno carico o un'attività di replica continua (acquisizione dei dati di modifica o CDC).

Per un'attività di caricamento completo, ti consigliamo di rimuovere gli indici delle chiavi primari, gli indici secondari, i vincoli di integrità referenziale e i trigger DML (Data Manipulation Language). In alternativa, è possibile ritardarne la creazione fino alla conclusione delle attività di pieno carico. Non sono necessari indici durante un'attività di pieno carico e, nel caso siano presenti, determinano costi di manutenzione. Poiché l'attività di caricamento completo carica gruppi di tabelle contemporaneamente, i vincoli di integrità referenziale sono violati. Analogamente, l'inserimento, l'aggiornamento e l'eliminazione di trigger può causare errori, ad esempio se l'inserimento di una riga viene attivato per una tabella precedentemente caricata in blocco. Anche altri tipi di trigger influenzano le prestazioni a causa di un'ulteriore elaborazione.

È possibile creare indici di chiavi primarie e secondarie prima di un'attività di pieno carico nel caso in cui i volumi di dati siano relativamente piccoli e il tempo di migrazione aggiuntivo non rappresenti un problema. I vincoli di integrità referenziale e i trigger devono essere sempre disattivati.

Per un'attività di pieno carico e CDC, ti consigliamo di aggiungere indici secondari prima della fase CDC. Poiché AWS DMS utilizza la replica logica, assicurati che gli indici secondari che supportano le operazioni DML siano presenti per evitare le scansioni dell'intera tabella. È possibile sospendere l'attività di replica prima della fase CDC per creare indici e vincoli di integrità referenziale prima di riavviare l'attività.

È necessario abilitare i trigger subito prima della conversione.

Disattivazione del log di backup e delle transazioni

Durante la migrazione a un database Amazon RDS, è consigliabile disattivare i backup e Multi-AZ sulla destinazione finché non sei pronto per la conversione. Analogamente, durante la migrazione a sistemi non Amazon RDS, è consigliabile disattivare qualsiasi log sulla destinazione fino alla conclusione della conversione.

Utilizzo di più attività

A volte l'utilizzo di più attività per una singola migrazione può migliorare le prestazioni. Se disponi di set di tabelle che non partecipano a transazioni comuni, puoi suddividere la migrazione in più attività. La coerenza transazionale viene mantenuta all'interno dell'attività, quindi è importante che le tabelle in attività separate non partecipino a transazioni comuni. Inoltre, ogni attività legge in modo indipendente il flusso di transazioni, quindi fai attenzione a non sovraccaricare il database di origine.

È possibile utilizzare più attività per creare flussi di replica separati. In questo modo, è possibile parallelizzare le letture sull'origine, i processi sull'istanza di replica e le scritture nel database di destinazione.

Ottimizzazione dell'elaborazione delle modifiche

Per impostazione predefinita, AWS DMS elabora le modifiche in una modalità transazionale, che conserva l'integrità delle transazioni. Se puoi permetterti vuoti temporanei nell'integrità delle transazioni, puoi utilizzare in alternativa l'opzione di applicazione ottimizzata in batch. Questa opzione raggruppa in modo efficiente le transazioni e le applica in batch per garantire l'efficienza. L'utilizzo dell'opzione di applicazione ottimizzata in batch viola quasi sempre i vincoli di integrità referenziale. Pertanto, ti consigliamo di disattivare questi vincoli durante il processo di migrazione e di riattivarli nel processo di conversione.

Utilizzo del server dei nomi in locale

Di solito, un'istanza di replica AWS DMS utilizza il risolutore del sistema dei nomi di dominio (DNS) in un'istanza Amazon EC2 per risolvere gli endpoint di dominio. Tuttavia, puoi utilizzare il server dei nomi on-premise per risolvere determinati endpoint se utilizzi il risolutore Amazon Route 53. Con questo strumento, puoi eseguire query tra dispositivi on-premise e AWS utilizzando gli endpoint in entrata e in uscita, le regole di inoltro e una connessione privata. I vantaggi dell'utilizzo di un server dei nomi on-premise includono una maggiore sicurezza e facilità d'uso con un firewall.

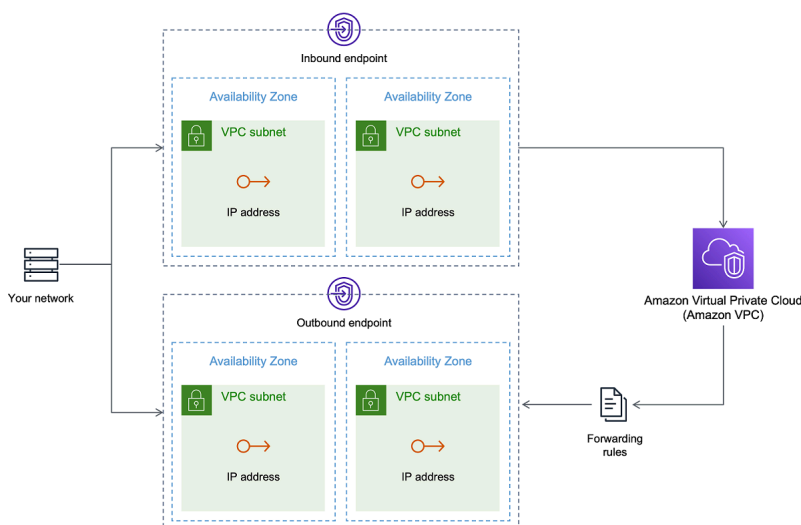
Se disponi di endpoint in entrata, puoi utilizzare le query DNS che hanno origine on-premise per risolvere i domini ospitati in AWS. Per configurare gli endpoint, assegna gli indirizzi IP in ogni sottorete a cui desideri fornire un risolutore. Per stabilire la connettività tra l'infrastruttura DNS on-premise e AWS, utilizza AWS Direct Connect o una rete privata virtuale (VPN).

Gli endpoint in uscita si connettono al server dei nomi on-premise. Il server dei nomi concede l'accesso solo agli indirizzi IP inclusi nell'elenco degli indirizzi consentiti e impostati in un endpoint in uscita. L'indirizzo IP del server dei nomi è l'indirizzo IP di destinazione. Quando scegli un gruppo di sicurezza per un endpoint in uscita, seleziona lo stesso gruppo di sicurezza utilizzato dall'istanza di replica.

Per selezionare i domini da inoltrare al server dei nomi, utilizza le regole di inoltro. Un endpoint in uscita può gestire più regole di inoltro. L'ambito della regola di inoltro è il cloud privato virtuale (VPC). Con una regola di inoltro associata a un VPC, puoi effettuare il provisioning di una sezione logicamente isolata del cloud AWS. Da questa sezione logicamente isolata, puoi avviare risorse AWS in una rete virtuale.

Puoi configurare i domini ospitati nell'infrastruttura DNS on-premise come regole di inoltro condizionale che impostano le query DNS in uscita. Quando viene effettuata una query a uno di questi domini, le regole attivano un tentativo di inoltro delle richieste DNS ai server configurati con le regole. Anche in questo caso, è necessaria una connessione privata tramite AWS Direct Connect o VPN.

Il diagramma seguente illustra l'architettura del risolutore Route 53.



Per ulteriori informazioni sul risolutore DNS Route 53, consulta [Nozioni di base su Route 53 Resolver](#) nella Guida per gli sviluppatori di Amazon Route 53.

Utilizzo del risolutore Amazon Route 53 con AWS DMS

Puoi creare un server dei nomi on-premise per AWS DMS per risolvere gli endpoint utilizzando [Amazon Route 53 Resolver](#).

Per creare un server dei nomi on-premise per AWS DMS basato su Route 53

1. Accedi alla AWS Management Console quindi apri la console Route 53 all'indirizzo <https://console.aws.amazon.com/route53/>.
2. Sulla console Route 53, scegli la Regione AWS in cui desideri configurare il risolutore Route 53. Il risolutore Route 53 è specifico per una regione.
3. Scegli la direzione della query: in entrata, in uscita o entrambe.
4. Fornisci la configurazione delle query in entrata:
 - a. Immetti un nome di endpoint e scegli un VPC.
 - b. Assegnare una o più sottoreti dal VPC (ad esempio, scegliere due per la disponibilità).
 - c. Assegna indirizzi IP specifici da utilizzare come endpoint o lascia che il risolutore Route 53 li assegni automaticamente.
5. Creare una regola per il dominio in locale in modo che i carichi di lavoro all'interno del VPC possano instradare le query DNS all'infrastruttura DNS.
6. Immetti uno o più indirizzi IP per i server DNS on-premise.
7. Invia la regola.

Al termine della creazione, il VPC è associato alle regole in entrata e in uscita e può iniziare a instradare il traffico.

Per ulteriori informazioni sul risolutore Route 53, consulta [Nozioni di base su Route 53 Resolver](#) nella Guida per gli sviluppatori di Amazon Route 53.

Migrazione di oggetti binari di grandi dimensioni (LOB)

In generale, AWS DMS esegue la migrazione di dati LOB in due fasi:

1. AWS DMS crea una nuova riga nella tabella di destinazione e la popola con tutti i dati eccetto il valore LOB associato.
2. AWS DMS aggiorna la riga nella tabella di destinazione con i dati LOB.

Questo processo di migrazione per i LOB richiede che, durante la migrazione, tutte le colonne LOB nella tabella di destinazione siano nullable. Ciò vale anche se le colonne LOB non sono nullable nella tabella di origine. Se AWS DMS crea le tabelle di destinazione, imposta le colonne LOB su nullable per impostazione predefinita. In alcuni casi, è possibile creare le tabelle di destinazione utilizzando altri meccanismi, come l'importazione o l'esportazione. In questi casi, assicurati che le colonne LOB siano annullabili prima di iniziare l'attività di migrazione.

Questo requisito ha un'eccezione. Supponi di eseguire una migrazione omogenea da un'origine Oracle a una destinazione Oracle e di scegliere Limited Lob mode (Modalità LOB limitata). In questo caso, l'intera riga viene popolata contemporaneamente, inclusi i valori LOB. Per questi casi, AWS DMS può creare le colonne LOB della tabella di destinazione con vincoli non nullable, se necessario.

Utilizzo della modalità LOB limitata

AWS DMS utilizza due metodi che bilanciano prestazioni e convenienza nel caso in cui la migrazione contenga valori LOB:

1. Limited LOB mode (Modalità LOB limitata) migra tutti i valori LOB fino a un limite di dimensioni specificato dall'utente (l'impostazione predefinita è 32 KB). I valori LOB di dimensioni superiori a questo limite devono essere migrati manualmente. Limited LOB mode (Modalità LOB limitata), l'impostazione predefinita per tutte le attività di migrazione, fornisce generalmente le prestazioni migliori. Tuttavia, accertati che l'impostazione del parametro Dimensione LOB massima sia corretta. Imposta questo parametro sulla dimensione LOB maggiore per tutte le tabelle.
2. Full LOB mode (Modalità LOB completa) migra tutti i dati LOB nelle tabelle, indipendentemente dalla dimensione. Full LOB mode (Modalità LOB completa) offre la praticità di spostare tutti i dati LOB nelle tabelle, ma il processo può avere un impatto significativo sulle prestazioni.

Per alcuni motori di database, come PostgreSQL, AWS DMS gestisce i tipi di dati JSON come LOB. Se hai scelto Modalità LOB limitata, assicurati che l'opzione Dimensione LOB massima sia impostata su un valore che non causa il troncamento dei dati JSON.

AWS DMS fornisce supporto completo per l'utilizzo di tipi di dati di oggetti di grandi dimensioni (BLOB, CLOB e NCLOB). I seguenti endpoint di origine hanno supporto LOB completo:

- Oracle
- Microsoft SQL Server
- ODBC

I seguenti endpoint di destinazione hanno supporto LOB completo:

- Oracle
- Microsoft SQL Server

Il seguente endpoint di destinazione ha supporto LOB limitato. Non è possibile utilizzare una dimensione LOB illimitata per questo endpoint di destinazione.

- Amazon Redshift
- Amazon S3

Per gli endpoint che hanno supporto LOB completo, è possibile impostare anche un limite di dimensione per i tipi di dati LOB.

Prestazioni LOB migliorate

Quando si migrano i dati LOB è possibile specificare le seguenti diverse impostazioni di ottimizzazione LOB.

Impostazioni LOB per tabella

Utilizzando le impostazioni LOB per tabella, è possibile sovrascrivere le impostazioni LOB a livello di attività per alcune o tutte le tabelle. Per farlo, definisci `lob-settings` nella regola `table-settings`. Di seguito è riportato un esempio di tabella che include valori LOB di grandi dimensioni.

```
SET SERVEROUTPUT ON
CREATE TABLE TEST_CLOB
(
  ID NUMBER,
  C1 CLOB,
  C2 VARCHAR2(4000)
);
DECLARE
bigtextstring CLOB := '123';
iINT;
BEGIN
WHILE Length(bigtextstring) <= 60000 LOOP
bigtextstring := bigtextstring || '00000000000000000000000000000000';
END LOOP;
INSERT INTO TEST_CLOB (ID, C1, C2) VALUES (0, bigtextstring, 'AnyValue');
```

```
END;  
/  
SELECT * FROM TEST_CLOB;  
COMMIT
```

Quindi, crea un'attività di migrazione e modifica la gestione LOB per la tabella utilizzando la nuova regola `lob-settings`. Il valore `bulk-max-size` determina la dimensione LOB massima (KB). I dati LOB vengono troncati se sono maggiori della dimensione specificata.

```
{  
  "rules": [{  
    "rule-type": "selection",  
    "rule-id": "1",  
    "rule-name": "1",  
    "object-locator": {  
      "schema-name": "HR",  
      "table-name": "TEST_CLOB"  
    },  
    "rule-action": "include"  
  },  
  {  
    "rule-type": "table-settings",  
    "rule-id": "2",  
    "rule-name": "2",  
    "object-locator": {  
      "schema-name": "HR",  
      "table-name": "TEST_CLOB"  
    },  
    "lob-settings": {  
      "mode": "limited",  
      "bulk-max-size": "16"  
    }  
  }  
]  
}
```

Anche se questa attività AWS DMS viene creata con `FullLobMode : true`, le impostazioni LOB per tabella indicano a AWS DMS di troncare i dati LOB in questa particolare tabella a 16.000. È possibile controllare i log delle attività per verificare.

```
721331968: 2018-09-11T19:48:46:979532 [SOURCE_UNLOAD] W: The value of column 'C' in  
table
```

```
'HR.TEST_CLOB' was truncated to length 16384
```

Impostazioni LOB in linea

Quando si crea un'attività AWS DMS, la modalità LOB determina come vengono gestiti i LOB.

È disponibile la modalità LOB completa e la modalità LOB limitata, ognuna con vantaggi e svantaggi. La modalità LOB in linea combina i vantaggi della modalità LOB completa e della modalità LOB limitata.

È possibile utilizzare la modalità LOB in linea quando è necessario replicare LOB di piccole e grandi dimensioni e la maggior parte dei LOB è di piccole dimensioni. Quando si sceglie questa opzione, durante il pieno carico l'attività AWS DMS trasferisce i LOB di piccole dimensioni in linea, ottenendo maggiore efficienza. L'attività AWS DMS trasferisce i LOB di grandi dimensioni eseguendo una ricerca nella tabella di origine.

Durante l'elaborazione delle modifiche, i LOB di piccole e grandi dimensioni vengono replicati eseguendo una ricerca nella tabella di origine.

Quando si utilizza la modalità LOB in linea, l'attività AWS DMS controlla tutte le dimensioni dei LOB per determinare quali trasferire in linea. I LOB più grandi della dimensione specificata vengono replicati utilizzando la modalità LOB completa. Pertanto, se la maggior parte dei LOB è più grande dell'impostazione specificata, è consigliabile non utilizzare questa opzione. Abilita invece la dimensione LOB illimitata.

Questa opzione viene configurata nelle impostazioni dell'attività utilizzando l'attributo `InlineLobMaxSize`, che è disponibile solo quando `FullLobMode` è impostato su `true`. Il valore predefinito per `InlineLobMaxSize` è 0 e l'intervallo è compreso tra 1 e 102400 kilobyte (100 MB).

Ad esempio, si potrebbero utilizzare le seguenti impostazioni dell'attività AWS DMS. In questo caso, impostando `InlineLobMaxSize` sul valore 5, tutti i LOB inferiori o uguali a 5 KiB (5.120 byte) vengono trasferiti in linea.

```
{
  "TargetMetadata": {
    "TargetSchema": "",
    "SupportLobs": true,
    "FullLobMode": true,
    "LobChunkSize": 64,
```

```
"LimitedSizeLobMode": false,  
"LobMaxSize": 32,  
"InlineLobMaxSize": 5,  
"LoadMaxFileSize": 0,  
"ParallelLoadThreads": 0,  
"ParallelLoadBufferSize":0,  
"BatchApplyEnabled": false,  
"TaskRecoveryTableEnabled": false},  
.  
.  
.  
}
```

Miglioramento delle prestazioni per la migrazione di tabelle di grandi dimensioni usando il filtro di riga

Per migliorare le prestazioni della migrazione di una tabella di grandi dimensioni, è possibile suddividere la migrazione in più attività. Per suddividere la migrazione in più attività utilizzando il filtro delle righe, utilizza una chiave o una chiave di partizione. Ad esempio, se hai un ID della chiave primaria intero da 1 a 8.000.000, puoi creare otto attività utilizzando il filtro delle righe per migrare 1 milione di record in ciascuna attività.

Per applicare il filtro di riga nella console:

1. Apri la AWS Management Console.
2. Scegli Attività e crea una nuova attività.
3. Scegli la scheda Mappature delle tabelle ed espandi Regole di selezione.
4. Scegli Aggiungi nuova regola di selezione. A questo punto puoi aggiungere un filtro di colonna con una condizione inferiore o uguale a, maggiore o uguale a, uguale a o di intervallo tra due valori. Per ulteriori informazioni sul filtro di colonna, consulta [Specifiche della selezione delle tabelle e delle regole di trasformazione dalla console](#).

Se hai una tabella di grandi dimensioni partizionata per data, puoi migrare i dati in base alla data. Ad esempio, supponi di disporre di una tabella partizionata per mese e solo i dati del mese corrente sono aggiornati. In questo caso, puoi creare un'attività di pieno carico per ogni partizione mensile statica e creare un'attività di pieno carico e CDC per la partizione attualmente aggiornata.

Se la tabella dispone di una chiave primaria a colonna singola o un indice univoco, puoi fare in modo che l'attività AWS DMS segmenti la tabella utilizzando un caricamento parallelo di tipo intervallo per

caricare i dati in parallelo. Per ulteriori informazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

La replica continua

AWS DMS fornisce la replica continua dei dati, mantenendo i database di origine e di destinazione sincronizzati. Replica solo una quantità limitata di istruzioni DDL (Data Definition Language). AWS DMS non propaga elementi come gli indici, gli utenti, i privilegi, le stored procedure e altre modifiche di database non direttamente correlate alla tabella dei dati.

Se prevedi di utilizzare la replica continua, imposta l'opzione Multi-AZ al momento della creazione dell'istanza di replica. Scegliendo Multi-AZ, ottieni elevata disponibilità e il supporto per il failover dell'istanza di replica. Tuttavia, questa opzione può avere un impatto sulle prestazioni e rallentare la replica durante l'applicazione delle modifiche al sistema di destinazione.

Prima di aggiornare i database di origine o di destinazione, si consiglia di interrompere tutte le attività AWS DMS in esecuzione su questi database. Riprendi le attività una volta completati gli aggiornamenti.

Durante la replica continua, è fondamentale identificare la larghezza di banda della rete tra il sistema di database di origine e l'istanza di replica AWS DMS. Assicurati che la rete non causi colli di bottiglia durante la replica continua.

È inoltre importante identificare la percentuale di modifica e la generazione dei log di archiviazione per ora sul sistema di database di origine. In questo modo è possibile comprendere la velocità di trasmissione effettiva che si può ottenere durante la replica continua.

Riduzione del carico del database di origine

AWS DMS utilizza alcune risorse del database di origine. Durante un'attività di caricamento completo, AWS DMS esegue la scansione completa della tabella di origine per ciascuna tabella elaborata in parallelo. Inoltre, ogni attività creata nell'ambito di una migrazione esegue sull'origine query relative alle modifiche come parte del processo della CDC. Affinché AWS DMS esegua il CDC per alcune origini, come Oracle, potrebbe essere necessario aumentare la quantità di dati scritti nel change log del database.

Se riscontri un sovraccarico del database di origine, riduci il numero di attività o tabelle per ogni attività per la migrazione. Ogni attività ottiene le modifiche dell'origine in modo indipendente, perciò il consolidamento delle attività può ridurre il carico di lavoro di acquisizione delle modifiche.

Riduzione dei colli di bottiglia sul database di destinazione

Durante la migrazione, prova a rimuovere tutti i processi relativi alle risorse di scrittura sul database di destinazione:

- Disattiva i trigger non necessari.
- Disattiva gli indici secondari durante il caricamento iniziale e riattivali in un secondo momento durante la replica continua.
- Con i database Amazon RDS è opportuno disattivare i backup e Multi-AZ fino al momento della conversione.
- Durante la migrazione in sistemi non RDS, è opportuno disattivare qualsiasi log sulla destinazione fino alla conversione.

Utilizzo della convalida dei dati durante la migrazione

Per garantire che i dati siano stati migrati in modo accurato dall'origine alla destinazione, ti consigliamo vivamente di utilizzare la convalida dei dati. Se attivi la convalida dei dati per un'attività, AWS DMS inizia a confrontare i dati di origine e di destinazione immediatamente dopo l'esecuzione di un pieno carico per una tabella.

La convalida dei dati funziona con i seguenti database se AWS DMS li supporta come endpoint di origine e di destinazione:

- Oracle
- PostgreSQL
- MySQL
- MariaDB
- Microsoft SQL Server
- Amazon Aurora edizione compatibile con MySQL
- Amazon Aurora PostgreSQL-Compatible Edition
- IBM Db2 LUW
- Amazon Redshift

Per ulteriori informazioni, consulta [Convalida dei dati in AWS DMS](#).

Monitoraggio delle attività AWS DMS tramite i parametri

Sono disponibili diverse opzioni per monitorare i parametri relativi alle attività tramite la console AWS DMS:

Parametri degli host

Puoi trovare le metriche degli host nella scheda Metriche per ogni particolare istanza di replica. CloudWatch Qui puoi controllare se l'istanza di replica è dimensionata in modo appropriato.

Parametri dell'attività di replica

Le metriche relative alle attività di replica, comprese le modifiche in entrata e confermate, e la latenza tra l'host di replica e i database di origine/destinazione sono disponibili nella scheda Metriche per ogni attività particolare. CloudWatch

Parametri della tabella

I parametri delle singole tabelle sono disponibili nella scheda Statistiche della tabella per ogni singola attività. I parametri includono i seguenti numeri:

- righe caricate durante il pieno carico;
- inserimenti, aggiornamenti ed eliminazioni dall'inizio dell'attività;
- operazioni DDL dall'inizio dell'attività.

Per ulteriori informazioni sul monitoraggio dei parametri, consulta [Monitoraggio delle attività AWS DMS](#).

Eventi e notifiche

AWS DMS utilizza Amazon SNS per inviare notifiche quando si verifica un evento di AWS DMS, ad esempio la creazione o l'eliminazione di un'istanza di replica. Puoi utilizzare queste notifiche in qualsiasi formato supportato da Amazon SNS per una regione AWS. Possono includere messaggi e-mail, messaggi di testo o chiamate a un endpoint HTTP.

Per ulteriori informazioni, consulta [Utilizzo degli eventi e delle notifiche Amazon SNS in AWS Database Migration Service](#).

Utilizzo del log delle attività per risolvere i problemi relativi alla migrazione

In alcuni casi, AWS DMS può riscontrare problemi per cui vengono visualizzati avvisi o messaggi di errore solo nel log delle attività. In particolare, i problemi di troncamento dei dati o rifiuti di righe a causa di violazioni delle chiavi esterne vengono scritti solo nel log delle attività. Pertanto, assicurati di esaminare il log delle attività durante la migrazione di un database. Per visualizzare il registro delle attività, configura Amazon CloudWatch come parte della creazione delle attività.

Per ulteriori informazioni, consulta [Monitoraggio delle attività di replica tramite Amazon CloudWatch](#).

Risoluzione dei problemi delle attività di replica con Time Travel

Per risolvere i problemi di migrazione di AWS DMS puoi utilizzare Time Travel. Per ulteriori informazioni su Time Travel, consulta [Impostazioni delle attività Time Travel](#).

Quando utilizzi Time Travel, tieni presente le seguenti considerazioni:

- Per evitare il sovraccarico su un'istanza di replica DMS, attiva Time Travel solo per le attività che richiedono il debug.
- Quando utilizzi Time Travel per risolvere i problemi relativi alle attività di replica che potrebbero durare diversi giorni, monitora i parametri delle istanze di replica per verificare il sovraccarico delle risorse. Questo approccio si applica soprattutto nei casi in cui carichi di transazioni elevati vengono eseguiti sui database di origine per lunghi periodi di tempo. Per ulteriori dettagli, consulta [Monitoraggio delle attività AWS DMS](#).
- Quando l'impostazione dell'attività Time Travel `EnableRawData` è impostata su `true`, l'utilizzo della memoria delle attività durante la replica DMS potrebbe essere maggiore rispetto a quando Time Travel non è attivato. Se attivi Time Travel per lunghi periodi di tempo, monitora l'attività.
- Attualmente puoi attivare Time Travel solo a livello di attività. Le modifiche a tutte le tabelle vengono registrate nei log di Time Travel. Se occorre risolvere problemi relativi a tabelle specifiche in un database con un volume di transazioni elevato, crea un'attività separata.

Modifica dell'utente e dello schema per una destinazione Oracle

Quando utilizzi Oracle come destinazione, AWS DMS esegue la migrazione dei dati allo schema di proprietà dell'utente dell'endpoint di destinazione.

Ad esempio, supponi di eseguire la migrazione di uno schema denominato PERFDATA a un endpoint di destinazione Oracle e che il nome utente dell'endpoint di destinazione sia MASTER. AWS DMS si collega alla destinazione Oracle come MASTER e popola lo schema MASTER con gli oggetti di database di PERFDATA.

Per sostituire questo comportamento, fornisci una trasformazione dello schema. Ad esempio, per migrare gli oggetti dello schema PERFDATA a uno schema PERFDATA nell'endpoint di destinazione, utilizza la seguente trasformazione.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "object-locator": {
    "schema-name": "PERFDATA"
  },
  "rule-target": "schema",
  "rule-action": "rename",
  "value": "PERFDATA"
}
```

Per ulteriori informazioni sulle trasformazioni, consulta [Specifiche della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).

Modifica di spazi di tabella per tabelle e indici di una destinazione Oracle

Quando si utilizza Oracle come destinazione, AWS DMS esegue la migrazione di tutte le tabelle e gli indici nello spazio di tabella predefinito nella destinazione. Ad esempio, supponi che l'origine sia un motore di database diverso da Oracle. Tutte le tabelle e gli indici della destinazione vengono migrati negli stessi spazi di tabella predefiniti.

Per sostituire questo comportamento, fornisci le corrispondenti trasformazioni degli spazi di tabella. Ad esempio, supponi di eseguire la migrazione di tabelle e indici negli spazi tabella delle tabelle e degli indici nella destinazione Oracle che sono denominati dopo lo schema nell'origine. In questo caso, puoi utilizzare trasformazioni simili alla seguente: Di seguito, lo schema nell'origine è denominato INVENTORY e gli spazi di tabella corrispondenti delle tabelle e degli indici nella destinazione sono denominati INVENTORYTBL e INVENTORYIDX.

```
{
  "rule-type": "transformation",
  "rule-id": "3",
  "rule-name": "3",
  "rule-action": "rename",
  "rule-target": "table-tablespace",
  "object-locator": {
    "schema-name": "INVENTORY",
    "table-name": "%",
    "table-tablespace-name": "%"
  },
  "value": "INVENTORYTBL"
},
{
  "rule-type": "transformation",
  "rule-id": "4",
  "rule-name": "4",
  "rule-action": "rename",
  "rule-target": "index-tablespace",
  "object-locator": {
    "schema-name": "INVENTORY",
    "table-name": "%",
    "index-tablespace-name": "%"
  },
  "value": "INVENTORYIDX"
}
```

Per ulteriori informazioni sulle trasformazioni, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).

Quando Oracle è sia origine che destinazione, è possibile mantenere le assegnazioni dello spazio di tabella per tabelle o indici esistenti impostando l'attributo aggiuntivo di connessione di origine Oracle `enableHomogenousTablespace=true`. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

Aggiornamento della versione di un'istanza di replica

AWS rilascia periodicamente nuove versioni del software del motore di replica AWS DMS, contenenti nuove funzionalità e miglioramenti in termini di prestazioni. Ogni versione del software del motore di replica dispone di un proprio numero di versione. È fondamentale testare la versione esistente dell'istanza di replica AWS DMS che esegue un carico di lavoro di produzione prima di aggiornare

l'istanza di replica a una versione successiva. Per ulteriori informazioni sugli aggiornamenti delle versioni disponibili, consulta [AWS Note di rilascio DMS](#).

Comprensione dei costi di migrazione

AWS Database Migration Service consente di migrare i database in AWS in modo semplice e sicuro. Paggi solo per le istanze di replica e l'eventuale archiviazione di log aggiuntiva. Ogni istanza di migrazione del database include un'archiviazione sufficiente per lo spazio di scambio, i log di replica e la cache dei dati per la maggior parte delle repliche e il trasferimento dei dati in entrata è gratuito.

Potrebbero essere necessarie più risorse durante il caricamento iniziale o durante i picchi di caricamento. Puoi monitorare attentamente l'utilizzo delle risorse delle istanze di replica con i parametri di CloudWatch. Quindi puoi aumentare e ridurre la dimensione dell'istanza di replica in base all'utilizzo.

Per ulteriori informazioni sulla stima dei costi di migrazione, consulta:

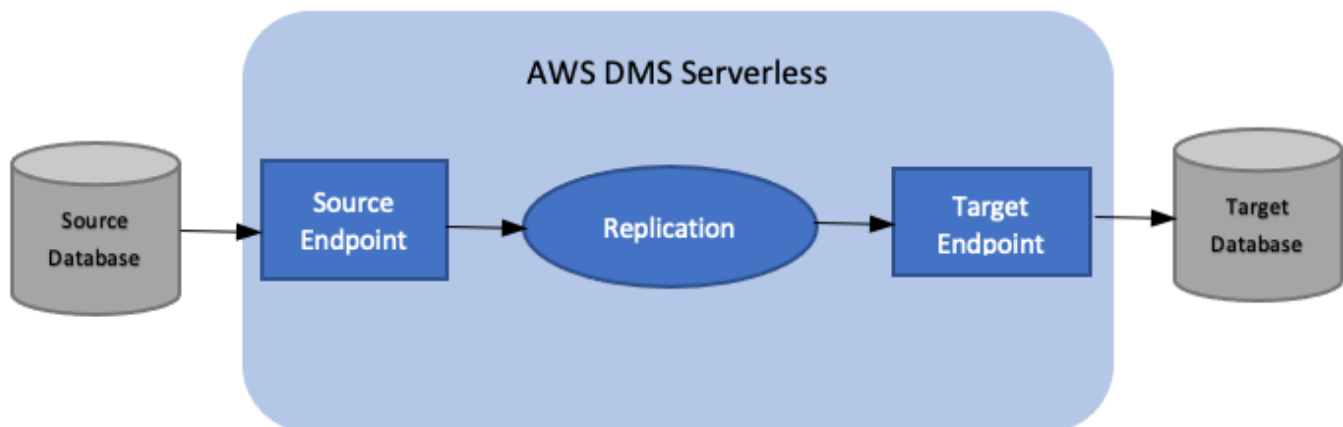
- [Prezzi di AWS Database Migration Service](#)
- [AWS Pricing Calculator](#)

Lavorare con AWS DMS Serverless

AWS DMS Serverless è una funzionalità che fornisce provisioning automatico, scalabilità, alta disponibilità integrata e un modello di pay-for-use fatturazione, per aumentare l'agilità delle operazioni e ottimizzare i costi. La funzionalità serverless elimina le attività di gestione delle istanze di replica come la stima della capacità, il provisioning, l'ottimizzazione dei costi e la gestione delle versioni e delle patch del motore di replica.

Con AWS DMS Serverless, simile alla funzionalità corrente di AWS DMS (denominata in questo documento come AWS DMS Standard), è possibile creare connessioni di origine e destinazione utilizzando gli endpoint. Dopo gli endpoint di origine e di destinazione, dovrai creare una configurazione della replica che includa le impostazioni di configurazione per la replica specificata. Puoi gestire le repliche avviandole, interrompendole, modificandole o eliminandole. Ogni replica dispone di impostazioni che puoi configurare in base alle esigenze della migrazione del database. È possibile specificare queste impostazioni utilizzando un file JSON o la AWS DMS sezione di AWS Management Console Per ulteriori informazioni sulle impostazioni di replica, vedere [Working with AWS DMS endpoints](#). Dopo aver avviato la replica, AWS DMS serverless si connette al database di origine e raccoglie i metadati del database per analizzare il carico di lavoro di replica. Utilizzando questi metadati, AWS DMS calcola e fornisce la capacità richiesta e avvia la replica dei dati.

Il diagramma seguente mostra il processo di replica serverless AWS DMS .



Note

AWS DMS Serverless utilizza la versione predefinita del motore. Per informazioni sulla versione del motore predefinita, consulta [Note di rilascio](#).

Visualizza i seguenti argomenti per scoprire maggiori dettagli su AWS DMS Serverless.

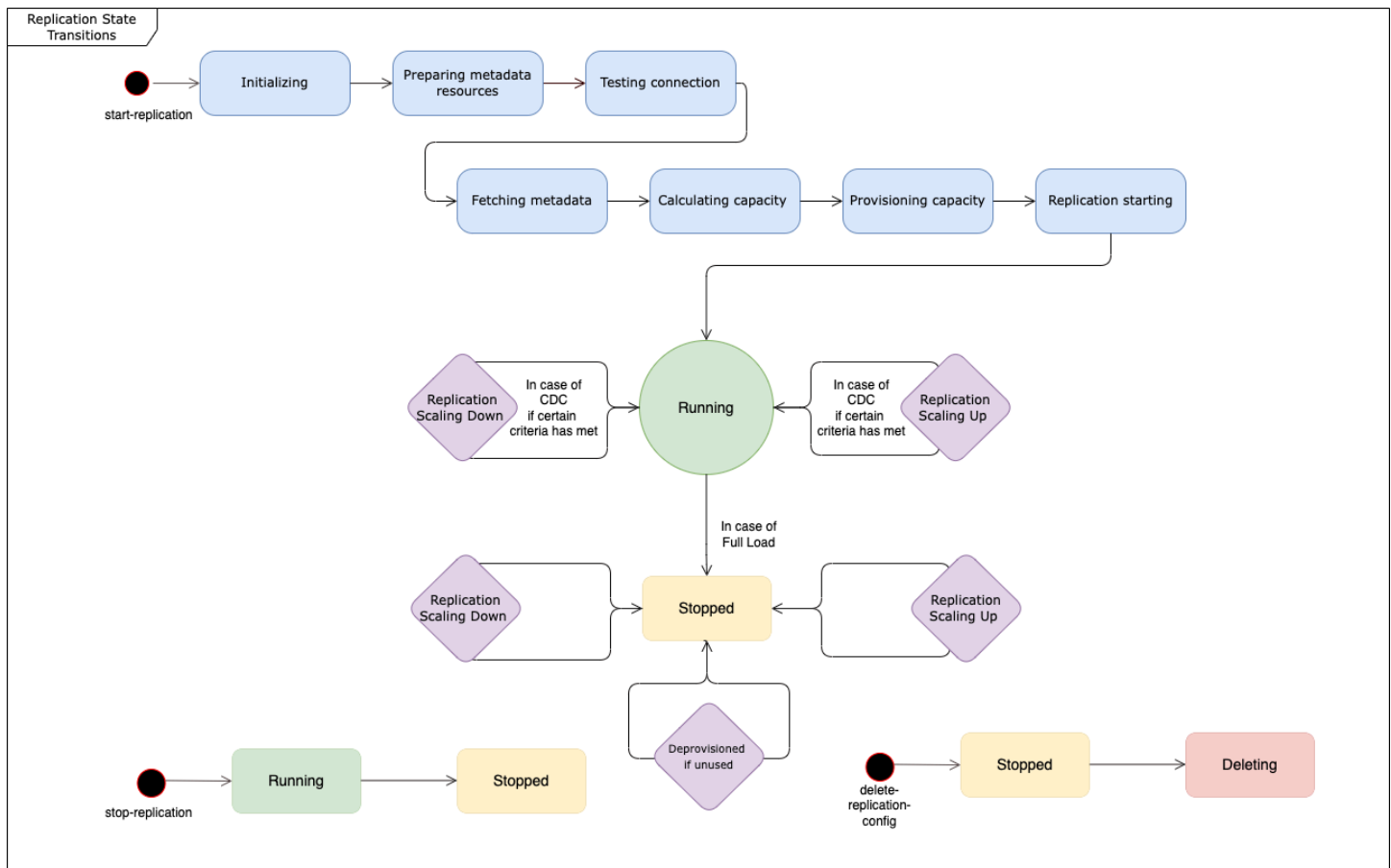
Argomenti

- [AWS DMS Componenti serverless](#)
- [AWS DMS Limitazioni serverless](#)

AWS DMS Componenti serverless

Per gestire le risorse necessarie per eseguire una replica, AWS DMS Serverless dispone di stati granulari che rivelano le diverse azioni interne intraprese dal servizio. Quando si avvia la replica, AWS DMS serverless calcola il carico della capacità, alloca la capacità calcolata e avvia la replica dei dati secondo i seguenti stati di replica.

Il diagramma seguente mostra le transizioni di stato per una replica serverless. AWS DMS



- Il primo stato dopo l'avvio della replica è Inizializzazione in corso. In questo stato vengono inizializzati tutti i parametri richiesti.
- Gli stati immediatamente successivi sono Preparazione delle risorse di metadati in corso, Verifica della connessione in corso e Recupero dei metadati in corso. In questi stati, AWS DMS Serverless si connette al database di origine per ottenere le informazioni necessarie a prevedere la capacità necessaria.
 - Quando lo stato di replica è Testing Connection, AWS DMS Serverless verifica che la connessione ai database di origine e di destinazione sia configurata correttamente.
 - Lo stato di replica dopo Verifica della connessione in corso è Recupero dei metadati in corso. Qui AWS DMS recupera le informazioni necessarie per calcolare la capacità.
 - Una volta AWS DMS recuperate le informazioni necessarie, lo stato successivo è Calcolo della capacità. In questo stato, il sistema calcola la dimensione delle risorse sottostanti necessarie per eseguire la replica.
- La transizione di stato successiva a Calcolo della capacità in corso è Capacità di allocazione. Quando la replica è in questo stato, AWS DMS serverless inizializza le risorse di elaborazione sottostanti.

- Lo stato di replica dopo che tutte le risorse sono state correttamente allocate è Avvio della replica. In questo stato, AWS DMS Serverless inizia la replica dei dati. Le fasi di una replica includono quanto segue:
 - Carico completo: in questa fase, DMS replica il data store di origine com'era all'inizio della replica.
 - CDC (iniziale): in questa fase, DMS replica le modifiche al data store di origine avvenute durante la fase di caricamento completo. DMS esegue questa fase solo se l'impostazione dell'attività è `StopTaskCachedChangesNotApplied`. `false`
 - CDC (in corso): dopo la fase CDC iniziale, DMS replica le modifiche nel database di origine non appena si verificano. DMS continua a eseguire la replica dopo la fase CDC iniziale solo se l'impostazione dell'attività è `StopTaskCachedChangesApplied` `false`
- Lo stato finale è In esecuzione. Lo stato In esecuzione indica che la replica dei dati è in corso.
- Una replica interrotta entra nello stato Interrotto. È possibile riavviare una replica interrotta nelle seguenti circostanze:
 - Non è possibile riavviare una replica di cui DMS ha eseguito il deprovisioning.
 - È possibile riavviare una replica interrotta solo CDC o a pieno carico e CDC utilizzando l'azione. [StartReplication](#) Non è possibile riavviare una replica interrotta utilizzando la console.
 - Non è possibile riavviare una replica interrotta che utilizza PostgreSQL come motore.

Questo argomento contiene le sezioni seguenti:

- [Versioni del motore supportate](#)
- [Creazione di una replica serverless](#)
- [Modifica delle repliche serverless AWS DMS](#)
- [Configurazione del calcolo](#)
- [Comprendere la scalabilità automatica in modalità serverless AWS DMS](#)
- [Monitoraggio delle repliche senza server AWS DMS](#)
- [Throughput migliorato per le migrazioni a pieno carico da Oracle ad Amazon Redshift](#)

Per AWS DMS Serverless, il pannello di navigazione a sinistra della AWS DMS console presenta una nuova opzione, le repliche Serverless. Per Repliche serverless è necessario specificare le repliche anziché i tipi o le attività dell'istanza di replica per definire una replica. Inoltre, è necessario specificare le unità di capacità DMS (DCU) massime e minime che DMS deve allocare per la replica. Una DCU è composta da 2 GB di RAM. AWS DMS fattura all'account ogni DCU attualmente utilizzata

dalla replica. Per informazioni sui AWS DMS prezzi, consulta la pagina dei [prezzi AWS del Database Migration Service](#).

AWS DMS quindi effettua automaticamente il provisioning delle risorse di replica in base alle mappature delle tabelle e alla dimensione prevista del carico di lavoro. Questa unità di capacità è un valore compreso nell'intervallo dei valori delle unità di capacità minime e massime specificati.

Versioni del motore supportate

Con AWS DMS Serverless, non è necessario scegliere e gestire le versioni del motore, poiché il servizio gestisce tale impostazione. AWS DMS Serverless supporta le seguenti fonti:

- Microsoft SQL Server
- Database compatibili con PostgreSQL
- Database compatibili con MySQL
- MariaDB
- Oracle
- IBM Db2

AWS DMS Serverless supporta i seguenti obiettivi:

- Microsoft SQL Server
- PostgreSQL
- Database compatibili con MySQL
- Oracle
- Amazon S3
- Amazon Redshift
- Amazon DynamoDB
- Flusso di dati Amazon Kinesis
- Amazon Managed Streaming per Apache Kafka
- OpenSearch Servizio Amazon
- Amazon DocumentDB (compatibile con MongoDB)
- Amazon Neptune

Come parte di AWS DMS Serverless, hai accesso ai comandi della console che ti consentono di creare, configurare, avviare e gestire repliche AWS DMS serverless. Per usare questi comandi con la sezione Repliche serverless della console, devi eseguire una delle seguenti operazioni:

- Imposta una nuova policy AWS Identity and Access Management (IAM) e un nuovo ruolo IAM a cui allegare quella policy.
- Utilizza un AWS CloudFormation modello per fornire l'accesso di cui hai bisogno.

AWS DMS Serverless richiede che nel tuo account esista un ruolo collegato al servizio (SLR). AWS DMS gestisce la creazione e l'utilizzo di questo ruolo. Per ulteriori informazioni su come verificare la disponibilità del ruolo collegato al servizio necessario, consulta [Ruolo collegato ai servizi per AWS DMS serverless](#).

Creazione di una replica serverless

Per creare una replica serverless tra due AWS DMS endpoint esistenti, procedi come segue. Per informazioni sulla creazione di AWS DMS endpoint, consulta [Creazione di endpoint di origine e destinazione](#)

Creazione di una replica serverless

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione scegli Repliche serverless, quindi seleziona Crea replica.
3. Nella pagina Crea replica specifica la configurazione della replica serverless:

Opzione	Azione
Nome	Immetti un nome per identificare la replica, ad esempio DMS-replication .
Nome della risorsa Amazon (ARN) descrittivo (facoltativo)	È possibile utilizzare questo parametro opzionale per fornire una descrizione della replica.
Endpoint del database di origine	Scegli gli endpoint esistenti nell'account. Tieni presente che AWS DMS Serverless supporta solo

Opzione	Azione
	un sottoinsieme dei tipi di endpoint supportati dallo standard. AWS DMS
Endpoint del database di destinazione	Scegli gli endpoint esistenti nell'account. Tieni presente che AWS DMS Serverless supporta solo un sottoinsieme dei tipi di endpoint supportati dallo standard. AWS DMS
Tipo di replica	<p>Scegli un tipo di replica in base alle esigenze:</p> <ul style="list-style-type: none"> • Caricamento completo: AWS DMS migra solo i dati esistenti. • Full Load and Change Data Capture (CDC): AWS DMS migra i dati esistenti e le modifiche che si verificano durante la replica. • Change Data Capture (CDC): migra AWS DMS solo le modifiche che si verificano dopo l'avvio della replica.

Nella sezione Impostazioni configura le impostazioni richieste dalla replica.

Nella sezione Mappature delle tabelle imposta la mappatura delle tabelle per definire le regole per selezionare e filtrare i dati che stai replicando. Prima di specificare la mappatura, consulta la sezione della documentazione sulla mappatura del tipo di dati per il database di origine e di destinazione. Per informazioni sulla mappatura dei tipi di dati per i database di origine e di destinazione, consulta la sezione sui tipi di dati per i tipi di endpoint di origine e di destinazione nell'argomento. [Utilizzo degli endpoint AWS DMS](#)

Nella sezione Impostazioni di calcolo configura le seguenti opzioni. Per informazioni sulle impostazioni di configurazione del calcolo, consulta [Configurazione del calcolo](#).

Opzione	Azione
VPC	Scegli un VPC esistente.

Opzione	Azione
Subnet group (Gruppo di sottoreti)	Scegli un gruppo di sottoreti esistente.
VPC security group(s) (Gruppi di sicurezza VPC)	Scegli Predefinito se non è già selezionato.
AWS Chiave KMS	Scegli una chiave KMS appropriata. Per informazioni sulle chiavi KMS, consulta Creazione di chiavi nell'AWS Key Management Service API Reference.
Distribuzione	Lascia il campo inalterato.
Zona di disponibilità	Lascia il campo inalterato.
Unità di capacità DMS minime (DCU) - (facoltativo)	Lascia il campo vuoto per utilizzare il valore predefinito di 1 DCU.
Unità di capacità DMS massime (DCU)	Scegli 16 DCU.

Lascia le impostazioni di Manutenzione invariate.

4. Scegli Crea replica.

AWS DMS crea una replica senza server per eseguire la migrazione.

Modifica delle repliche serverless AWS DMS

Per modificare la configurazione della replica, utilizza l'azione `modify-replication-config`. È possibile modificare solo una configurazione di AWS DMS replica che si trova negli stati `CREATED`, `STOPPED` o `FAILED`. Per informazioni sull'`modify-replication-config`, consulta [ModifyReplicationConfig](#) nell'AWS Database Migration Service API Reference.

Per modificare una configurazione di replica senza server utilizzando il AWS Management Console

1. [Accedere AWS Management Console e aprire la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/.](https://console.aws.amazon.com/dms/v2/)
2. Nel riquadro di navigazione scegli Repliche serverless.

3. Scegli la replica che desideri modificare. La tabella seguente descrive le modifiche che è possibile apportare in base allo stato corrente della replica.

Impostazione	Descrizione	Stati consentiti
Nome	Puoi modificare il nome della replica. Digita un nome per la replica che contenga da 8 a 16 caratteri ASCII stampabili (esclusi /, " e @). Il nome deve essere univoco all'interno dell'account nella regione AWS selezionata. Puoi scegliere di aggiungere alcuni dettagli al nome, ad esempio includere la AWS regione e l'attività che stai eseguendo, ad esempio: west2-mysql2mysql-config1 .	ReplicationState è CREATED, STOPPED o FAILED.
Endpoint del database di origine	Scegli un nuovo endpoint di origine esistente come origine della replica.	ReplicationState è CREATED oppure FAILED quando ProvisionState è null.
Endpoint del database di destinazione	Scegli un nuovo endpoint di destinazione esistente come destinazione della replica.	ReplicationState è CREATED oppure FAILED quando ProvisionState è null.
Tipo di replica	È possibile modificare il tipo di replica serverless.	ReplicationState è CREATED oppure FAILED quando ProvisionState è null.

Impostazione	Descrizione	Stati consentiti
Impostazioni di replica	È possibile modificare le impostazioni di replica, tra cui la modalità di preparazione della tabella di destinazione, l'inclusione delle colonne LOB nella replica, la dimensione massima dei LOB, la convalida e la registrazione. Per ulteriori informazioni, consulta Impostazioni delle attività .	ReplicationState è CREATED, STOPPED o FAILED.
Mappature delle tabelle	È possibile modificare le impostazioni di mappatura delle tabelle per una replica serverless, incluse le regole di selezione e trasformazione. Per ulteriori informazioni, consulta Mappatura delle tabelle .	ReplicationState è CREATED, STOPPED o FAILED.

Impostazione	Descrizione	Stati consentiti
Configurazione del calcolo	<p>È possibile modificare le impostazioni di configurazione del calcolo per una replica serverless, incluse le impostazioni di rete, dimensionamento e manutenzione. Per informazioni sulle impostazioni di configurazione del calcolo, consulta Configurazione del calcolo.</p>	<ul style="list-style-type: none"> • È possibile modificare e le seguenti impostazioni di dimensionamento, manutenzione e rete se <code>ReplicatedOnState</code> è <code>CREATED</code>, <code>STOPPED</code> o <code>FAILED</code>: <ul style="list-style-type: none"> • <code>MinCapacityUnits</code> • <code>MaxCapacityUnits</code> • <code>MultiAZ</code> • <code>PreferredMaintenanceWindow</code> • <code>VpcSecurityGroupIds</code> • È possibile modificare le seguenti impostazioni di rete e sicurezza se <code>ReplicatedOnState</code> è <code>CREATED</code> o <code>FAILED</code> quando <code>ProvisionState</code> è <code>null</code>: <ul style="list-style-type: none"> • <code>AvailabilityZone</code> • <code>DnsNameServers</code> • <code>KmsKeyId</code>

Impostazione	Descrizione	Stati consentiti
		<ul style="list-style-type: none"> Replicati onSubnetGroupId

Configurazione del calcolo

È possibile configurare il provisioning della replica utilizzando il parametro Configurazione del calcolo o la sezione della console. I campi dell'oggetto Configurazione del calcolo sono i seguenti:

Opzione	Descrizione
MinCapacityUnità	Questo è il numero minimo di unità di capacità DMS (DCU) che AWS DMS verranno fornite. È anche la DCU minima a cui il dimensionamento automatico può essere ridotto.
MaxCapacityUnità	È il numero massimo di unità di capacità DMS (DCU) che AWS DMS può allocare, in base alla previsione della capacità di replica. È anche la DCU massima a cui il dimensionamento automatico può essere aumentato.
KmsKeyId	La chiave di crittografia da utilizzare per crittografare le informazioni di connessione e archiviazione della replica. Se scegli (impostazione predefinita) aws/dms, AWS DMS utilizza la chiave KMS predefinita associata al tuo account e. Regione AWS Vengono mostrati una descrizione e il numero di account, insieme all'ARN della chiave. Per ulteriori informazioni sull'utilizzo della chiave di crittografia, consulta Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS . Per questo tutorial, lascia selezionato (Impostazione predefinita) aws/dms.
ReplicationSubnetGroupId	Il gruppo di sottoreti di replica nel VPC selezionato in cui desideri creare la replica. Se il database di origine è in un

Opzione	Descrizione
	VPC, scegli il gruppo di sottoreti che contiene il database di origine come posizione per la replica. Per ulteriori informazioni sui gruppi di sottoreti di replica, consulta Creazione di un gruppo di sottoreti di replica .
VpcSecurityGroupIds	L'istanza di replica viene creata in un VPC. Se il database di origine è in un VPC, seleziona il gruppo di sicurezza VPC che fornisce l'accesso all'istanza database in cui si trova il database.
PreferredMaintenanceFinestra	Questo parametro definisce un intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione del sistema. L'impostazione predefinita è una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per volta Regione AWS, che si verifica in un giorno casuale della settimana.
MultiAZ	Questo parametro facoltativo crea una replica di standby della replica in un'altra zona di disponibilità per il supporto del failover. Se desideri utilizzare l'acquisizione dei dati di modifica (CDC) o la replica continua, ti consigliamo di attivare questa opzione.

Comprendere la scalabilità automatica in modalità serverless AWS DMS

Dopo aver effettuato il provisioning di una replica che si trova RUNNING nello stato in cui si trova, il AWS DMS servizio gestisce la capacità delle risorse sottostanti di adattarsi ai carichi di lavoro in evoluzione. Questa gestione dimensiona le risorse di replica in base alle seguenti impostazioni di replica:

- MinCapacityUnits
- MaxCapacityUnits

Le repliche aumentano dopo il periodo di superamento della soglia di utilizzo massima e diminuiscono quando l'utilizzo della capacità è inferiore alla soglia di utilizzo minima della capacità per un lungo periodo.

Note

Le repliche serverless non possono essere ridimensionate automaticamente mentre è in corso un carico completo.

Ottimizzazione AWS DMS della scalabilità automatica in modalità serverless

Per ottimizzare i parametri di scalabilità automatica della replica, si consiglia di impostarli sul valore massimo e di lasciare che sia possibile `MaxCapacityUnits` gestire il provisioning delle risorse. AWS DMS Ti consigliamo di scegliere l'impostazione più ampia della capacità massima di DCU per sfruttare al massimo il dimensionamento automatico e far fronte ai picchi di volume delle transazioni. Il calcolatore dei prezzi mostra il costo mensile massimo se la replica utilizza continuamente la capacità massima di DCU. La capacità massima di DCU non rappresenta il costo effettivo, in quanto paghi solo per ciò che utilizzi.

Se la replica non utilizza le risorse a piena capacità, AWS DMS procederà gradualmente al rifornimento delle risorse per ridurre i costi. Tuttavia, poiché il provisioning e l'annullamento del provisioning delle risorse richiedono tempo, ti consigliamo di impostare `MinCapacityUnits` su un valore in grado di gestire eventuali picchi improvvisi previsti nel carico di lavoro di replica. In questo modo si eviterà che la replica venga sottoposta a un provisioning insufficiente e al contempo si riforniranno le risorse per un livello di carico di AWS DMS lavoro più elevato.

Se il provisioning della replica è insufficiente per l'impostazione della capacità massima troppo bassa per i requisiti dei dati o della capacità minima troppo bassa per gestire picchi improvvisi nel carico di lavoro di replica, è possibile che la metrica `CapacityUtilization` raggiunga costantemente il suo valore massimo, causando l'esito negativo della replica. Se la replica fallisce a causa di un approvvigionamento insufficiente delle risorse, crea un evento nei log di replica. AWS DMS out-of-memory Se la out-of-memory condizione si verifica a causa di un picco improvviso del carico di lavoro di replica, la replica verrà scalata e riavviata automaticamente.

Monitoraggio delle repliche senza server AWS DMS

AWS offre diversi strumenti per monitorare le repliche AWS DMS serverless e rispondere a potenziali incidenti:

- [AWS DMS metriche di replica senza server](#)
- [AWS DMS log di replica senza server](#)

AWS DMS metriche di replica senza server

Il monitoraggio della replica senza server include i CloudWatch parametri di Amazon per le seguenti statistiche. Queste statistiche sono raggruppate per ogni replica serverless.

Parametro	Unità	Descrizione
CapacityUtilization	Percentuale	Percentuale di memoria utilizzata dalla replica serverless
CDC IncomingChanges	Percentuale	Il numero totale di eventi di modifica in corso point-in-time che attendono di essere applicati all'obiettivo. Tieni presente che questo non equivale alla misura della frequenza di modifica della transazione dell'endpoint di origine. Un numero elevato per questa metrica di solito indica che non AWS DMS è in grado di applicare le modifiche acquisite in modo tempestivo, causando così un'elevata latenza target.
CDC LatencySource	Secondi	<p>Il divario, in secondi, tra l'ultimo evento acquisito dall'endpoint di origine e il timestamp di sistema corrente dell'istanza AWS DMS. CDC LatencySource rappresenta la latenza tra l'origine e l'istanza di replica. Un CDC elevato LatencySource significa che il processo di acquisizione delle modifiche dalla fonte viene ritardato. Per identificare la latenza in una replica in corso, puoi visualizzare questa metrica insieme a CDC. LatencyTarget. Se sia il CDC che il CDC LatencyTarget sono LatencySource elevati, esaminate prima il CDC. LatencySource</p> <p>CDC LatencySource può essere 0 quando non vi è alcun ritardo di replica tra l'origine e la replica. CDC LatencySource può inoltre diventare zero quando</p>

Parametro	Unità	Descrizione
		la replica tenta di leggere l'evento successivo nel registro delle transazioni dell'origine e non vengono rilevati nuovi eventi rispetto all'ultima lettura dall'origine. Quando ciò accade, la replica reimposta il CDC su 0. LatencySource
CDC LatencyTarget	Secondi	<p>Il divario, in secondi, tra il primo timestamp dell'evento in attesa di commit sulla destinazione e il timestamp corrente dell'istanza AWS DMS. La latenza della destinazione è la differenza tra l'ora del server dell'istanza di replica e l'ID dell'evento non confermato meno recente inoltrato a un componente di destinazione. In altre parole, la latenza della destinazione è la differenza di timestamp tra l'istanza di replica e l'evento meno recente applicato ma non confermato dall'endpoint di destinazione (99%). Quando il CDC LatencyTarget è alto, indica che il processo di applicazione degli eventi di modifica all'obiettivo è ritardato. Per identificare la latenza in una replica in corso, puoi visualizzare questa metrica insieme a CDC. LatencySource. Se il CDC LatencyTarget è elevato ma il CDC LatencySource non lo è, verifica se:</p> <ul style="list-style-type: none"> • mancano indici o chiavi primarie nella destinazione; • si verificano colli di bottiglia relativi alle risorse nella destinazione o nell'istanza di replica; • i problemi di rete risiedono tra la replica e la destinazione.
Obiettivo CDC ThroughputBandwidth	KB al secondo	Dati in uscita trasmessi per la destinazione in KB al secondo. Il CDC ThroughputBandwidth registra i dati in uscita trasmessi sui punti di campionamento. Se non viene rilevato traffico di rete, il valore è zero. CDC non emette transazioni di lunga durata, pertanto il traffico di rete potrebbe non essere registrato.

Parametro	Unità	Descrizione
ThroughputRowsFonte CDC	Righe al secondo	Modifiche in entrata dall'origine in righe al secondo.
Obiettivo CDC ThroughputRows	Righe al secondo	Modifiche in uscita per la destinazione in righe al secondo.
FullLoadThroughputBandwidthObiettivo	KB al secondo	Dati in uscita trasmessi da un pieno carico per la destinazione in KB al secondo.
FullLoadThroughputRowsObiettivo	Righe al secondo	Modifiche in uscita da un pieno carico per la destinazione in righe al secondo.

AWS DMS log di replica senza server

Puoi utilizzare Amazon CloudWatch per registrare le informazioni di replica durante un processo di AWS DMS migrazione. Puoi abilitare la registrazione quando selezioni le impostazioni di replica.

Le repliche serverless caricano i log di stato CloudWatch sul tuo account per fornire una maggiore visibilità sullo stato di avanzamento della replica e per facilitare la risoluzione dei problemi.

AWS DMS carica i log collegati senza server in un gruppo di log dedicato con il prefisso `dms-serverless-replication-<your replication config resource ID>`. All'interno di questo gruppo di log è presente un flusso di log denominato `dms-serverless-replication-orchestrator-<your replication config resource ID>`. Questo flusso di log riporta lo stato della replica e un messaggio associato che fornisce ulteriori dettagli sul lavoro svolto in questa fase. Per esempi di voci di log, consulta [Esempi di log della replica serverless](#) di seguito.

Note

AWS DMS non crea né il gruppo di log né lo stream finché non si esegue la replica. AWS DMS non crea il gruppo o lo stream di log se si crea solo la replica.

Per visualizzare i log di una replica eseguita, procedi come segue:

1. Apri la AWS DMS console e scegli Repliche senza server dal pannello di navigazione. Viene visualizzata la finestra di dialogo Repliche serverless.
2. Vai alla sezione Configurazione e scegli Visualizza i log serverless nella colonna Generale. Si apre il gruppo di CloudWatch log.
3. Individua la sezione Registri delle attività di migrazione e scegli Visualizza CloudWatch registri.

Se la replica non riesce, AWS DMS crea una voce di registro con uno stato di replica di `failed` e un messaggio che descrive il motivo dell'errore. È consigliabile controllare i CloudWatch log come primo passaggio per la risoluzione dei problemi di replica non riuscita.

Note

Come con AWS DMS Classic, è possibile abilitare una registrazione più granulare sullo stato di avanzamento della migrazione dei dati stessa, ovvero i log emessi dall'attività di replica sottostante. È possibile abilitare questi log nelle impostazioni di replica impostando `EnableLogging` su `true` nel campo `Logging`, come nel seguente esempio JSON:

```
{
  "Logging": {
    "EnableLogging": true
  }
}
```

Una volta abilitati, questi log sono disponibili solo durante la fase `running` della replica serverless. Sono presenti nello stesso gruppo di log del flusso di log precedente, ma dispongono del nuovo `dms-serverless-serv-res-id-{unique identifier}` del flusso di log. Per informazioni su come interpretare i log della replica serverless, consulta la sezione seguente.

Esempi di log della replica serverless

In questa sezione sono inclusi esempi di voci di log delle repliche serverless.

Esempio: avvio della replica

Quando si esegue una replica senza server, AWS DMS crea una voce di registro simile alla seguente:

```
{'replication_state':'initializing', 'message': 'Initializing the replication workflow.'}
```

Esempio: errore della replica

Se uno degli endpoint della replica non è configurato correttamente, AWS DMS crea una voce di registro simile alla seguente:

```
{'replication_state':'failed', 'message': 'Test connection failed for endpoint X.', 'failure_message': 'X'}
```

Se vedi questo messaggio nel log dopo un errore, assicurati che l'endpoint specificato sia integro e configurato correttamente.

Throughput migliorato per le migrazioni a pieno carico da Oracle ad Amazon Redshift

AWS DMS offre prestazioni di throughput notevolmente migliorate per le migrazioni a pieno carico da Oracle ad Amazon Redshift. DMS abilita automaticamente questa funzionalità per le tabelle senza l'custom `parallel-load` opzione nelle mappature delle tabelle. Per le tabelle con opzioni di caricamento parallelo personalizzate, DMS serverless distribuisce il carico della tabella in base alle configurazioni di mappatura delle tabelle fornite. Per utilizzare un throughput avanzato, procedi come segue:

- Fornite regole di selezione che non facciano riferimento a partizioni o limiti. Ad esempio, se le impostazioni della tabella nelle mappature delle tabelle lo contengono `parallel-load`, DMS Serverless non utilizzerà la funzionalità di throughput avanzato. Per ulteriori informazioni, consulta [Operazioni e regole di selezione](#).
- `MaxFileSize` imposta e su 64 MB. `WriteBufferSize` Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS](#).
- Si consiglia `CompressCsvFiles` di impostare su `true` per un data store con dati sparsi e `false` per un data store con dati densi.
- Imposta le seguenti impostazioni delle attività su: `0`

- `ParallelLoadThreads`
- `ParallelLoadQueuesPerThread`
- `ParallelApplyThreads`
- `ParallelApplyQueuesPerThread`
- `ParallelLoadBufferSize`
- Impostato `MaxFullLoadSubTasks` su 49 per supportare la migrazione parallela dei dati.
- Imposta `LOB mode` su `inline`. Per ulteriori informazioni, consulta [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#).

AWS DMS non fornisce prestazioni di throughput migliorate per le seguenti repliche:

- Repliche con tabelle che utilizzano il caricamento parallelo. Per ulteriori informazioni, consulta [Utilizzo del caricamento parallelo per le tabelle, le viste e le raccolte selezionate](#).
- Repliche con regole di trasformazione dei dati.
- Repliche con regole di filtro.
- Repliche con la regola di `change-data-type` trasformazione.

AWS DMS Limitazioni serverless

AWS DMS Serverless presenta le seguenti limitazioni:

- È possibile modificare solo una configurazione di AWS DMS replica che si trova negli stati `CREATEDSTOPPED`, o `FAILED`. Per informazioni dettagliate sulle impostazioni che è possibile modificare nelle varie condizioni, consulta [Modifica delle repliche serverless AWS DMS](#).
- È possibile eliminare solo una configurazione di AWS DMS replica che si trova negli stati `STOPPED`, o `FAILED`.
- Per la replica è disponibile uno spazio di archiviazione allocato statico di 100 GB. Se la replica utilizza più memoria, a causa di requisiti quali transazioni di lunga durata o memorizzazione nella cache, ti consigliamo di partizionare il carico di lavoro in repliche serverless separate. È possibile partizionare il carico di lavoro per tabella o per requisito, ad esempio inserendo tutte le repliche che coinvolgono i LOB in una replica serverless separata.
- A differenza delle istanze di replica, le repliche AWS DMS serverless non dispongono di un indirizzo IP pubblico per le attività di gestione. Le repliche serverless si gestiscono tramite la console.

- Questa versione di AWS DMS serverless non supporta tutti i tipi di endpoint di origine e di destinazione supportati dallo standard. AWS DMS Per l'elenco dei tipi di motore supportati, consulta [AWS DMS Componenti serverless](#).
- Le repliche serverless devono accedere alle dipendenze utilizzando endpoint VPC. È necessario utilizzare gli endpoint VPC per accedere ai seguenti tipi di endpoint:
 - Amazon S3
 - Amazon Kinesis
 - AWS Secrets Manager
 - Amazon DynamoDB
 - Amazon Redshift
 - OpenSearch Servizio Amazon

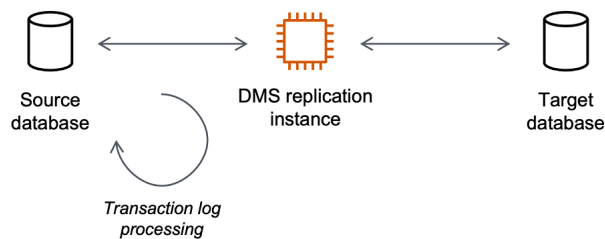
Per informazioni sull'impostazione degli endpoint VPC, consulta [Configurazione degli endpoint VPC come endpoint di origine e di destinazione AWS DMS](#).

- AWS DMS serverless non supporta le visualizzazioni con regole di selezione e trasformazione.
- AWS DMS serverless non supporta l'utilizzo di chiavi gestite AWS dal cliente. AWS DMS serverless supporta solo l'utilizzo della chiave DMS predefinita. Per ulteriori informazioni, consulta [Protezione dei dati in AWS Database Migration Service](#).
- DMS Serverless non supporta le connessioni SSL per gli endpoint DB2.

Utilizzo di un'istanza di AWS DMS replica

Quando crei un'istanza di AWS DMS replica, la AWS DMS crea su un'istanza Amazon EC2 in un cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Questa istanza di replica viene utilizzata per eseguire la migrazione del database. L'istanza di replica offre alta disponibilità e supporto per il failover con un'implementazione Multi-AZ se selezioni l'opzione Multi-AZ.

In una distribuzione Multi-AZ, effettua AWS DMS automaticamente il provisioning e mantiene una replica sincrona in standby dell'istanza di replica in una zona di disponibilità diversa. L'istanza di replica principale viene replicata in modo sincrono tra le zone di disponibilità in una replica di standby. Questo approccio fornisce ridondanza dei dati, elimina i blocchi I/O e riduce al minimo i picchi di latenza.



AWS DMS utilizza un'istanza di replica per connettersi al data store di origine, leggere i dati di origine e formattare i dati per l'utilizzo da parte del data store di destinazione. Un'istanza di replica, inoltre, carica i dati nel data store di destinazione. La maggior parte di questo processo si verifica in memoria. Tuttavia, per le transazioni di grandi dimensioni potrebbe essere necessario il buffering su disco. Anche le transazioni e i file di log memorizzati nella cache vengono scritti su disco.

È possibile creare un'istanza AWS DMS di replica nelle seguenti AWS regioni.

Nome della regione	Regione	Endpoint	Protocollo
US East (Ohio)	us-east-2	dms.us-east-2.amazonaws.com	HTTPS
		dms-fips.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	dms.us-east-1.amazonaws.com	HTTPS
		dms-fips.us-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Stati Uniti occidentali (California settentrionale)	us-west-1	dms.us-west-1.amazonaws.com	HTTPS
		dms-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	dms.us-west-2.amazonaws.com	HTTPS
		dms-fips.us-west-2.amazonaws.com	HTTPS
Africa (Città del Capo)	af-south-1	dms.af-south-1.amazonaws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	dms.ap-east-1.amazonaws.com	HTTPS
Asia Pacifico (Hyderabad)	ap-south-2	dms.ap-south-2.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	dms.ap-southeast-3.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Melbourne)	ap-southeast-4	dms.ap-southeast-4.amazonaws.com	HTTPS
Asia Pacifico (Mumbai)	ap-south-1	dms.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	dms.ap-northeast-3.amazonaws.com	HTTPS
Asia Pacifico (Seoul)	ap-northeast-2	dms.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacifico (Singapore)	ap-southeast-1	dms.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacifico (Sydney)	ap-southeast-2	dms.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	dms.ap-northeast-1.amazonaws.com	HTTPS
Canada (Centrale)	ca-central-1	dms.ca-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Canada occidentale (Calgary)	ca-west-1	dms.ca-west-1.amazonaws.com	HTTPS
Europa (Francoforte)	eu-central-1	dms.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	dms.eu-west-1.amazonaws.com	HTTPS
Europa (Londra)	eu-west-2	dms.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	dms.eu-south-1.amazonaws.com	HTTPS
Europa (Parigi)	eu-west-3	dms.eu-west-3.amazonaws.com	HTTPS
Europa (Spagna)	eu-south-2	dms.eu-south-2.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	dms.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	dms.eu-central-2.amazonaws.com	HTTPS
Israele (Tel Aviv)	il-central-1	dms.il-central-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Bahrein)	me-south-1	dms.me-south-1.amazonaws.com	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	dms.me-central-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	dms.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	dms.us-gov-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	dms.us-gov-west-1.amazonaws.com	HTTPS

AWS DMS supporta una AWS regione speciale AWS GovCloud (US) denominata progettata per consentire alle agenzie governative e ai clienti degli Stati Uniti di spostare carichi di lavoro sensibili nel cloud. AWS GovCloud (US) soddisfa i requisiti normativi e di conformità specifici del governo degli Stati Uniti. Per ulteriori informazioni su AWS GovCloud (US), consulta [What is AWS GovCloud \(US\)?](#)

Di seguito sono riportati ulteriori dettagli sulle istanze di replica.

Argomenti

- [Scelta dell'istanza di replica AWS DMS giusta per la migrazione](#)
- [Selezione della dimensione migliore per un'istanza di replica](#)
- [Utilizzo delle versioni del motore di replica](#)
- [Istanze di replica pubbliche e private](#)
- [Indirizzi IP e tipi di rete](#)
- [Configurazione di una rete per un'istanza di replica](#)
- [Impostazione di una chiave di crittografia per un'istanza di replica](#)
- [Creazione di un'istanza di replica](#)
- [Modifica di un'istanza di replica](#)
- [riavvio di un'istanza di replica.](#)
- [Eliminazione di un'istanza di replica.](#)
- [Utilizzo della finestra di manutenzione AWS DMS](#)

Scelta dell'istanza di replica AWS DMS giusta per la migrazione

AWS DMS crea l'istanza di replica su un'istanza Amazon EC2. AWS DMS attualmente supporta le classi di istanze Amazon EC2 T2, T3, C4, C5, C6i, R4, R5 e R6i per le istanze di replica:

- Le istanze T2 sono istanze a prestazioni espandibili che forniscono un livello di base di prestazioni della CPU e la possibilità di superarlo temporaneamente. Le prestazioni di base e la capacità di ottimizzazione sono governate dai crediti CPU. Le istanze T2 ricevono crediti CPU in modo continuo a una velocità prestabilita in base alla dimensione dell'istanza. Accumulano crediti CPU quando sono inattive e consumano crediti CPU quando sono attive.

Le istanze T2 sono una buona scelta per una varietà di carichi di lavoro generici. Includono microservizi, applicazioni interattive a bassa latenza, database di dimensioni medie e ridotte, desktop virtuali, ambienti di sviluppo, creazione e gestione temporanea, repository di codice e prototipi di prodotto.

- Le istanze T3 sono il tipo di istanza per uso generico espandibile di nuova generazione. Questo tipo fornisce un livello base di prestazioni della CPU con la possibilità di espandere l'utilizzo della CPU in qualsiasi momento per tutto il tempo necessario. Le istanze T3 offrono un rapporto equilibrato tra calcolo, memoria e risorse di rete e sono progettate per i carichi di lavoro con un

utilizzo moderato della CPU con picchi temporanei nell'uso. Le istanze T3 accumulano crediti CPU quando un carico di lavoro opera al di sotto della soglia di base. Ogni credito CPU guadagnato offre all'istanza T3 l'opportunità di sfruttare al massimo le prestazioni di un core CPU completo per un minuto, se necessario.

Le istanze T3 possono espandersi in qualsiasi momento per tutto il periodo necessario in modalità `unlimited`. Per ulteriori informazioni sulla modalità `unlimited`, consulta [Utilizzo della modalità illimitata per istanze a prestazioni espandibili](#).

- Le istanze C4 sono ottimizzate per carichi di lavoro con elevate esigenze di elaborazione e forniscono prestazioni elevate a costi ridotti, con un rapporto tra spese e potenza di calcolo ottimale. Garantiscono prestazioni PPS (packet per second) significativamente più elevate, minore jitter di rete e minore latenza di rete. AWS DMS può anche richiedere un uso intensivo della CPU, specialmente quando si eseguono migrazioni e repliche eterogenee come la migrazione da Oracle a PostgreSQL. In questi casi, le istanze C4 possono rappresentare una scelta adeguata.
- Le istanze C5 sono il tipo di istanza di nuova generazione che offre prestazioni elevate a costi contenuti a un basso rapporto tra spesa e potenza di calcolo per l'esecuzione di carichi di lavoro avanzati a uso intensivo delle capacità di calcolo. Sono inclusi i carichi di lavoro come server Web ad alte prestazioni, calcolo ad alte prestazioni (HPC), elaborazione in batch, pubblicazione di annunci, giochi multiplayer altamente dimensionabili e codifica video. Gli altri carichi di lavoro per cui sono adatte le istanze C5 includono la modellazione scientifica, l'analisi distribuita e l'inferenza di machine learning e deep learning. Le istanze C5 sono disponibili con una scelta di processori Intel e AMD.
- Le istanze C6i offrono prestazioni di calcolo superiori in termini di prezzo fino al 15% rispetto alle istanze Gen5 comparabili per un'ampia varietà di carichi di lavoro e la crittografia della memoria sempre attiva. Le istanze C6i sono adatte per carichi di lavoro a uso intensivo delle capacità di calcolo quali elaborazione in batch, analisi distribuita, calcolo ad alte prestazioni (HPC), pubblicazione di annunci, giochi multiplayer altamente dimensionabili e codifica video.
- Le istanze R4 sono ottimizzate per la memoria per carichi di lavoro con elevati requisiti di memoria. Le migrazioni o le repliche continue di sistemi di transazioni con elevata velocità di trasmissione effettiva che utilizzano AWS DMS possono a volte consumare grandi quantità di CPU e memoria. Le istanze R4 includono più memoria per vCPU rispetto ai tipi di istanze della generazione precedente.
- Le istanze R5 sono la nuova generazione di tipi di istanze ottimizzate per la memoria per Amazon EC2. Le istanze R5 sono adatte per applicazioni con elevati requisiti di memoria quali database ad alte prestazioni, cache in memoria distribuite su scala Web, database in memoria di medie dimensioni, analisi dei big data in tempo reale e altre applicazioni aziendali. Le migrazioni o le

repliche continue di sistemi di transazione ad alto throughput possono inoltre consumare grandi quantità di CPU e memoria. AWS DMS

- Le istanze R6i offrono prestazioni di calcolo superiori in termini di prezzo fino al 15% rispetto alle istanze Gen5 comparabili per un'ampia varietà di carichi di lavoro e la crittografia della memoria sempre attiva. Le istanze R6i sono certificate SAP e sono ideali per carichi di lavoro come database SQL e noSQL, cache in memoria distribuite su scala Web come Memcached e Redis, database in memoria come SAP HANA e analisi dei big data in tempo reale come i cluster Hadoop e Spark.

Ogni istanza di replica dispone di una specifica configurazione di memoria e di vCPU. La tabella seguente mostra la configurazione per ogni tipo di istanza di replica. Per informazioni sui prezzi, consulta la [pagina dei prezzi del servizio AWS Database Migration Service](#).

Tipi di istanze di replica per uso generico

Type	VPCU	Memoria (GiB)
dms.t2.micro	1	1
dms.t2.small	1	2
dms.t2.medium	2	4
dms.t2.large	2	8
dms.t3.micro	2	1
dms.t3.small	2	2
dms.t3.medium	2	4
dms.t3.large	2	8

Tipi di istanze di replica ottimizzate per il calcolo

Type	VPCU	Memoria (GiB)
dms.c4.large	2	3,75

Type	VPCU	Memoria (GiB)
dms.c4.xlarge	4	7.5
dms.c4.2xlarge	8	15
dms.c4.4xlarge	16	30
dms.c5.large	2	4
dms.c5.xlarge	4	8
dms.c5.2xlarge	8	16
dms.c5.4xlarge	16	32
dms.c5.9xlarge	36	72
dms.c5.12xlarge	48	96
dms.c5.18xlarge	72	144
dms.c5.24xlarge	96	192
dms.c6i.large	2	4
dms.c6i.xlarge	4	8
dms.c6i.2xlarge	8	16
dms.c6i.4xlarge	16	32
dms.c6i.8xlarge	32	64
dms.c6i.12xlarge	48	96
dms.c6i.16xlarge	64	128
dms.c6i.24xlarge	96	192
dms.c6i.32xlarge	128	256

Tipi di istanze di replica ottimizzate per la memoria

Type	VPCU	Memoria (GiB)
dms.r4.large	2	15,25
dms.r4.xlarge	4	30,5
dms.r4.2xlarge	8	61
dms.r4.4xlarge	16	122
dms.r4.8xlarge	32	244
dms.r5.large	2	16
dms.r5.xlarge	4	32
dms.r5.2xlarge	8	64
dms.r5.4xlarge	16	128
dms.r5.8xlarge	32	256
dms.r5.12xlarge	48	384
dms.r5.16xlarge	64	512
dms.r5.24xlarge	96	768
dms.r6i.large	2	16
dms.r6i.xlarge	4	32
dms.r6i.2xlarge	8	64
dms.r6i.4xlarge	16	128
dms.r6i.8xlarge	32	256
dms.r6i.12xlarge	48	384

Type	VPCU	Memoria (GiB)
dms.r6i.16xlarge	64	512
dms.r6i.24xlarge	96	768
dms.r6i.32xlarge	128	1.024

Le tabelle precedenti elencano tutti i tipi di istanze di AWS DMS replica, ma i tipi disponibili nell'area geografica potrebbero variare. Per visualizzare i tipi di istanze di replica disponibili nella propria regione, è possibile eseguire il comando [AWS CLI](#) seguente:

```
aws dms describe-orderable-replication-instances --region your_region_name
```

Argomenti

- [Decisione della classe di istanza da utilizzare](#)
- [Utilizzo della modalità illimitata per istanze a prestazioni espandibili](#)

Decisione della classe di istanza da utilizzare

Per aiutarti a determinare quale classe di istanza di replica potrebbe funzionare meglio per te, diamo un'occhiata al processo CDC (Change Data Capture) utilizzato. AWS DMS

Supponiamo che tu stia eseguendo un'attività di caricamento completo + CDC (caricamento in blocco + replica continua). In questo caso, l'attività dispone di un repository SQLite per archiviare i metadati e altre informazioni. Prima di AWS DMS iniziare un caricamento completo, vengono eseguiti i seguenti passaggi:

- AWS DMS inizia ad acquisire le modifiche per le tabelle che sta migrando dal registro delle transazioni del motore di origine (le chiamiamo modifiche memorizzate nella cache). Una volta completato il caricamento completo, queste modifiche memorizzate nella cache vengono raccolte e applicate nella destinazione. In base al volume, queste modifiche memorizzate nelle cache possono essere applicate direttamente dalla memoria, dove vengono prima raccolte, fino a una soglia definita. In alternativa, possono essere applicate dal disco, dove le modifiche vengono scritte nel caso non possano essere conservate in memoria.

- Dopo l'applicazione delle modifiche memorizzate nella cache, per impostazione predefinita AWS DMS avvia un processo di applicazione transazionale sull'istanza di destinazione.

Durante la fase di applicazione delle modifiche memorizzate nella cache e la fase di replica in corso, AWS DMS utilizza due buffer di flusso, uno ciascuno per i dati in entrata e in uscita. AWS DMS utilizza anche un componente importante chiamato sorter, che è un altro buffer di memoria. Di seguito sono riportati due utilizzi importanti del componente ordinatore (ne sono disponibili altri):

- Monitora tutte le transazioni e verifica che al buffer in uscita vengano inoltrate solo le transazioni pertinenti.
- Verifica che le transazioni vengano inoltrate nello stesso ordine di commit dell'origine.

Come puoi notare, sono presenti tre importanti buffer di memoria in questa architettura per CDC in AWS DMS. Un utilizzo elevato della memoria in uno di questi buffer può causare problemi di prestazioni e compromettere potenzialmente il sistema.

La memoria supplementare fornita dalle istanze R5 e R6i può risultare utile quando in questa architettura vengono associati pesanti carichi di lavoro con un numero elevato di transazioni al secondo (TPS). Puoi utilizzare le istanze R5 e R6i per conservare un numero elevato di transazioni in memoria e prevenire problemi di utilizzo elevato della memoria durante le repliche continue.

Utilizzo della modalità illimitata per istanze a prestazioni espandibili

Un'istanza a prestazioni espandibili configurata come `unlimited`, ad esempio un'istanza T3, può sostenere un utilizzo elevato della CPU per tutto il tempo necessario in qualsiasi momento. Il prezzo orario dell'istanza può coprire automaticamente tutti i picchi di utilizzo della CPU se l'utilizzo medio della CPU dell'istanza corrisponde o è inferiore alla baseline per un periodo di 24 ore o la durata dell'istanza, a seconda di quale dei due è inferiore.

Per la grande maggioranza dei carichi di lavoro per scopi generici, le istanze configurate come `unlimited` offrono prestazioni elevate senza addebiti aggiuntivi. Se l'istanza viene eseguita a un utilizzo più elevato della CPU per un periodo di tempo prolungato, verrà applicata una tariffa fissa aggiuntiva all'ora vCPU. Per informazioni sui prezzi delle istanze T3, consulta "Crediti CPU T3" in [AWS Database Migration Service](#).

Per ulteriori informazioni sulla `unlimited` modalità per le istanze T3, consulta la sezione [Modalità illimitata per istanze con prestazioni espandibili nella Guida per l'utente di Amazon EC2](#).

⚠ Important

Se utilizzi un'istanza `dms.t3.micro` nell'ambito dell'offerta [Piano gratuito di AWS](#) in modalità `unlimited`, potrebbero essere applicati costi. In particolare, potrebbero essere applicati costi aggiuntivi se l'utilizzo medio in un periodo continuo di 24 ore supera l'utilizzo di base dell'istanza. Per ulteriori informazioni, consulta [l'utilizzo di base](#) nella Guida per l'utente di Amazon EC2.

Le istanze T3 si avviano come `unlimited` per impostazione predefinita. Se l'utilizzo medio della CPU per un periodo di 24 ore supera la baseline, vengono addebitati i costi per i crediti in eccedenza. In alcuni casi, è possibile avviare le istanze spot T3 come `unlimited` e pianificare di utilizzarle immediatamente e per un breve periodo. Se lo fai senza tempo di inattività per accumulare crediti CPU, vengono addebitati i costi per i crediti in eccedenza. Consigliamo di avviare le istanze spot T3 in modalità standard per evitare di sostenere costi maggiori. Per ulteriori informazioni, consulta la sezione [I crediti in eccesso possono incorrere in addebiti, le istanze Spot T3 e la modalità Standard per le istanze con prestazioni espandibili nella Guida per l'utente di Amazon EC2](#).

Selezione della dimensione migliore per un'istanza di replica

La scelta dell'istanza di replica appropriata dipende da diversi fattori associati al caso d'uso. Per aiutarti a comprendere il modo in cui vengono utilizzate le risorse delle istanze di replica, consulta la seguente discussione. Copre lo scenario comune di un'attività di caricamento completo + CDC.

Durante un'attività di caricamento completo, AWS DMS carica le tabelle singolarmente. Per impostazione predefinita, vengono caricate otto tabelle alla volta. AWS DMS acquisisce le modifiche in corso all'origine durante un'attività di caricamento completo in modo che le modifiche possano essere applicate successivamente sull'endpoint di destinazione. Le modifiche vengono memorizzate nella cache della memoria; quando la memoria disponibile è esaurita, le modifiche vengono memorizzate nella cache del disco. Quando viene completata un'attività di caricamento completo per una tabella, applica AWS DMS immediatamente le modifiche memorizzate nella cache alla tabella di destinazione.

Dopo l'applicazione di tutte le modifiche memorizzate nella cache in sospenso per una tabella, l'endpoint di destinazione è in uno stato coerente a livello di transazioni. A questo punto, la destinazione è sincronizzata con l'endpoint di origine rispetto alle ultime modifiche memorizzate nella cache. AWS DMS inizia quindi la replica continua tra l'origine e la destinazione. A tale

scopo, AWS DMS prende le operazioni di modifica dai log delle transazioni di origine e le applica alla destinazione in modo transazionale coerente. (Questo processo presuppone che l'opzione Applicazione ottimizzata in batch non sia selezionata). AWS DMS trasmette le modifiche in corso attraverso la memoria sull'istanza di replica, se possibile. Altrimenti, AWS DMS scrive le modifiche su disco sull'istanza di replica finché non possono essere applicate sulla destinazione.

È possibile controllare il modo in cui l'istanza di replica gestisce l'elaborazione delle modifiche e il modo in cui la memoria viene utilizzata in tale processo. Per ulteriori informazioni su come ottimizzare l'elaborazione delle modifiche, consulta [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).

Fattori da considerare

La memoria e lo spazio su disco sono fattori chiave nella scelta dell'istanza di replica appropriata per il tuo caso d'uso. Di seguito, è disponibile una descrizione delle caratteristiche dei casi d'uso da analizzare per scegliere l'istanza di replica.

- Dimensione di database e tabelle

Il volume di dati aiuta a determinare la configurazione dell'attività per ottimizzare le prestazioni del pieno carico. Ad esempio, per due schemi da 1 TB è possibile partizionare le tabelle in quattro attività da 500 GB ed eseguirle in parallelo. Il parallelismo dipende dalla risorsa CPU disponibile nell'istanza di replica. Ecco perché è una buona idea comprendere le dimensioni del database e delle tabelle per ottimizzare le prestazioni del pieno carico. Aiuta a determinare il numero di attività che è possibile svolgere.

- Oggetti di grandi dimensioni

I tipi di dati presenti nell'ambito della migrazione possono influire sulle prestazioni. In particolare, gli oggetti di grandi dimensioni (LOB) influiscono sulle prestazioni e sul consumo di memoria. Per migrare un valore LOB, AWS DMS esegue un processo in due fasi. Innanzitutto, AWS DMS inserisce la riga nella destinazione senza il valore LOB. In secondo luogo, AWS DMS aggiorna la riga con il valore LOB. Ciò ha un impatto sulla memoria, quindi è importante identificare le colonne LOB nell'origine e analizzarne le dimensioni.

- Frequenza di caricamento e dimensione della transazione

La frequenza di caricamento e le transazioni al secondo (TPS) influiscono sull'utilizzo della memoria. Un numero elevato di attività TPS o DML (Data Manipulation Language) comporta un elevato utilizzo della memoria. Ciò accade perché DMS memorizza nella cache le modifiche finché

non vengono applicate alla destinazione. Durante la CDC comporta lo swap (scrittura sul disco fisico a causa di un sovraccarico di memoria), che causa latenza.

- Chiavi della tabella e integrità referenziale

Le informazioni sulle chiavi della tabella determinano la modalità CDC (applicazione in batch o applicazione transazionale) utilizzata per migrare i dati. In generale, l'applicazione transazionale è più lenta dell'applicazione in batch. Per le transazioni di lunga durata, la migrazione può includere molte modifiche. Quando si utilizza l'applicazione transazionale, AWS DMS potrebbe essere necessaria più memoria per archiviare le modifiche rispetto all'applicazione in batch. Se si esegue la migrazione delle tabelle senza chiavi primarie, l'applicazione in batch ha esito negativo e l'attività DMS passa alla modalità di applicazione transazionale. Quando l'integrità referenziale è attiva tra le tabelle durante il CDC, AWS DMS utilizza l'applicazione transazionale per impostazione predefinita. Per ulteriori informazioni sull'applicazione in batch rispetto all'applicazione transazionale, vedi [Come posso utilizzare la funzione di applicazione batch di DMS per migliorare le prestazioni di replica CDC?](#)

Utilizza i parametri indicati per determinare se è necessario che l'istanza di replica sia ottimizzata per il calcolo o la memoria.

Problemi comuni

Durante la migrazione potrebbero verificarsi i seguenti problemi comuni che causano un conflitto di risorse sull'istanza di replica. Per informazioni sui parametri dell'istanza di replica, consulta [Parametri dell'istanza di replica](#).

- Se la memoria in un'istanza di replica diventa insufficiente, i dati vengono scritti sul disco. La lettura dal disco può causare latenza, che è possibile evitare dimensionando l'istanza di replica con memoria sufficiente.
- La dimensione del disco assegnata all'istanza di replica può essere inferiore a quella richiesta. La dimensione del disco viene utilizzata quando lo spazio per i dati in memoria si esaurisce e anche per archiviare i log delle attività. Anche il numero massimo di IOPS dipende da questo.
- L'esecuzione di più attività oppure di attività con elevato parallelismo influisce sul consumo di CPU dell'istanza di replica. Si rallenta l'elaborazione delle attività che si traduce in latenza.

Best practice

Considera queste due best practice comuni per il dimensionamento di un'istanza di replica. Per ulteriori informazioni, consulta [Best practice per AWS Database Migration Service](#).

1. Dimensiona il tuo carico di lavoro e determina se richiede un uso intensivo delle capacità di calcolo o elevati requisiti di memoria. In base a ciò, puoi determinare la classe e la dimensione dell'istanza di replica:
 - AWS DMS elabora i LOB in memoria. Questa operazione richiede una discreta quantità di memoria.
 - Il numero di attività e il numero di thread influiscono sul consumo della CPU. Evita di utilizzare più di otto `MaxFullLoadSubTasks` durante l'operazione di pieno carico.
2. Aumenta lo spazio su disco assegnato all'istanza di replica in caso di carico di lavoro elevato durante il pieno carico. In questo modo l'istanza di replica può utilizzare il numero massimo di IOPS ad essa assegnato.

Le linee guida precedenti non coprono tutti gli scenari possibili. È importante considerare le specifiche del tuo particolare caso d'uso quando stabilisci la dimensione dell'istanza di replica.

I test precedenti mostrano che CPU e memoria variano a seconda dei diversi carichi di lavoro. In particolare, i LOB influiscono sulla memoria e il numero delle attività o il parallelismo influiscono sulla CPU. Una volta che la migrazione è in esecuzione, monitora la CPU, la memoria liberabile, lo storage libero e gli IOPS dell'istanza di replica. In base ai dati raccolti, è possibile dimensionare l'istanza di replica in base alle esigenze.

Utilizzo delle versioni del motore di replica

Il motore di replica è il AWS DMS software principale che viene eseguito sull'istanza di replica ed esegue le attività di migrazione specificate dall'utente. AWS rilascia periodicamente nuove versioni del software del motore di AWS DMS replica, con nuove funzionalità e miglioramenti delle prestazioni. Ogni versione del software del motore di replica dispone di un proprio numero di versione per distinguerlo dalle altre versioni.

Quando si avvia una nuova istanza di replica, viene eseguita la versione più recente del AWS DMS motore, a meno che non venga specificato diversamente. Per ulteriori informazioni, consulta [Utilizzo di un'istanza di AWS DMS replica](#).

Se disponi di un'istanza di replica attualmente in esecuzione, puoi aggiornarla a una versione del motore più recente. (AWS DMS non supporta il downgrade della versione del motore). Per ulteriori informazioni sulle versioni del motore di replica, consulta [AWS Note di rilascio DMS](#).

Aggiornamento della versione del motore mediante la console

È possibile aggiornare un'istanza di AWS DMS replica utilizzando AWS Management Console.

Per aggiornare un'istanza di replica utilizzando la console:

1. Aprire la AWS DMS console all'indirizzo <https://console.aws.amazon.com/dms/v2/>.
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegli il motore di replica, quindi scegli Modify (Modifica).
4. Per Versione del motore scegli il numero di versione desiderato, quindi scegli Modifica.

Note

È consigliabile interrompere tutte le attività prima di aggiornare l'istanza di replica. Se non interrompi l'operazione, la AWS DMS interromperà automaticamente prima dell'aggiornamento. Se interrompi l'attività manualmente, sarà necessario avviarla manualmente dopo il completamento dell'aggiornamento. L'aggiornamento dell'istanza di replica richiede alcuni minuti. Quando l'istanza è pronta, il relativo stato diventa available (disponibile).

Aggiornamento della versione del motore utilizzando il AWS CLI

È possibile aggiornare un'istanza di AWS DMS replica utilizzando AWS CLI, come segue.

Per aggiornare un'istanza di replica utilizzando AWS CLI:

1. Determina l'Amazon Resource Name (ARN) dell'istanza di replica utilizzando il comando seguente.

```
aws dms describe-replication-instances \  
--query "ReplicationInstances[*].\  
[ReplicationInstanceIdentifier,ReplicationInstanceArn,ReplicationInstanceClass]"
```

Nell'output, prendi nota dell'ARN dell'istanza di replica che desideri aggiornare, ad esempio:

```
arn:aws:dms:us-east-1:123456789012:rep:6EFQQ06U6EDPRCPKLNPL2SCEEY
```

2. Determina quali versioni dell'istanza di replica sono disponibili utilizzando il comando seguente.

```
aws dms describe-orderable-replication-instances \  
--query "OrderableReplicationInstances[*].[ReplicationInstanceClass,EngineVersion]"
```

Nell'output, prendi nota del numero o dei numeri di versione del motore disponibili per la classe dell'istanza di replica. Queste informazioni dovrebbero apparire nell'output della fase 1.

3. Aggiorna l'istanza di replica utilizzando il comando seguente.

```
aws dms modify-replication-instance \  
--replication-instance-arn arn \  
--engine-version n.n.n
```

Sostituisci *arn* nella riga precedente con l'ARN effettivo dell'istanza di replica indicato nella fase precedente.

Sostituisci *n.n.n* con il numero di versione del motore desiderato, ad esempio: 3.4.5

Note

L'aggiornamento dell'istanza di replica richiede alcuni minuti. Puoi visualizzare lo stato dell'istanza di replica utilizzando il comando seguente.

```
aws dms describe-replication-instances \  
--query "ReplicationInstances[*].  
[ReplicationInstanceIdentifier,ReplicationInstanceStatus]"
```

Quando l'istanza di replica è pronta, il relativo stato diventa available (disponibile).

Istanze di replica pubbliche e private

Puoi specificare se un'istanza di replica dispone di un indirizzo IP pubblico o privato che utilizza per la connessione ai database di origine e di destinazione.

Un'istanza di replica privata dispone di un indirizzo IP privato a cui non è possibile accedere al di fuori della rete di replica. Si utilizza un'istanza privata quando entrambi i database di origine e di destinazione si trovano nella stessa rete connessa al cloud privato virtuale (VPC) dell'istanza di replica. La rete può essere connessa al VPC utilizzando una rete privata virtuale (VPN) o il peering AWS Direct Connect VPC.

Una connessione di peering VPC è una connessione di rete tra due VPC. Consente il routing utilizzando gli indirizzi IP privati di ciascun VPC come se si trovassero nella stessa rete. Per ulteriori informazioni sul peering di VPC, consulta [Peering di VPC](#) nella Guida per l'utente di Amazon VPC.

Un'istanza di replica pubblica può utilizzare il gruppo di sicurezza VPC dell'istanza di replica e l'indirizzo IP pubblico dell'istanza di replica o l'indirizzo IP pubblico del gateway NAT. Queste connessioni creano una rete che viene utilizzata per la migrazione dei dati.

Indirizzi IP e tipi di rete

AWS DMS crea sempre la tua istanza di replica in un Amazon Virtual Private Cloud (VPC). Quando crei il VPC, puoi determinare l'indirizzo IP da utilizzare: IPv4 o IPv6 o entrambi. Quindi, quando crei o modifichi un'istanza di replica, puoi specificare l'uso di un protocollo di indirizzi IPv4 o di un protocollo di indirizzi IPv6 utilizzando la modalità dual-stack.

Indirizzi IPv4

Quando crei un VPC, devi specificare un intervallo di indirizzi IPv4 per il VPC sotto forma di blocco di routing interdominio senza classi (CIDR), ad esempio 10.0.0.0/16. Un gruppo di sottoreti definisce l'intervallo di indirizzi IP in questo blocco CIDR. Questi indirizzi IP possono essere privati o pubblici.

Un indirizzo IPv4 privato è un indirizzo IP non raggiungibile tramite Internet. Puoi utilizzare indirizzi IPv4 privati per la comunicazione tra l'istanza di replica e altre risorse, ad esempio istanze Amazon EC2, nello stesso VPC. Ogni istanza di replica dispone di un indirizzo IP privato per la comunicazione nel VPC.

Un indirizzo IP pubblico è un indirizzo IPv4 raggiungibile tramite Internet. Puoi utilizzare gli indirizzi pubblici per la comunicazione tra l'istanza di replica e le risorse su Internet. Puoi controllare se le istanze di replica ricevono un indirizzo IP pubblico.

Modalità dual-stack e indirizzi IPv6

Se le risorse devono comunicare con l'istanza di replica su IPv6, utilizza la modalità dual-stack. Per utilizzare la modalità dual-stack, assicurati che ogni sottorete nel gruppo di sottoreti associato

all'istanza di replica abbia un blocco CIDR IPv6. Per soddisfare questo requisito, puoi creare un nuovo gruppo di sottoreti di replica o modificare un gruppo di sottoreti di replica esistente. Ogni indirizzo IPv6 è univoco a livello globale. Il blocco CIDR IPv6 per il VPC è assegnato automaticamente dal pool di indirizzi IPv6 di Amazon. Non è possibile scegliere l'intervallo in modo autonomo.

DMS disabilita l'accesso al gateway Internet per gli endpoint IPv6 di istanze di replica private in modalità dual-stack per garantire che gli endpoint IPv6 siano privati e accessibili solo dall'interno del VPC.

Puoi utilizzare la AWS DMS console per creare o modificare un'istanza di replica e specificare la modalità dual-stack nella sezione Tipo di rete. L'immagine seguente mostra la sezione Network type (Tipo di rete) nella console.

Connectivity and security

Network type - new [Info](#)

To use dual-stack mode, make sure that you associate an IPv6 CIDR block with a subnet in the VPC you specify.

IPv4

Replication instance with an IPv4 network type that supports IPv4 addressing.

Dual-stack mode

Replication instance with a dual network type that supports both IPv4 and IPv6 addressing.

Riferimenti

- Per ulteriori informazioni sugli indirizzi IPv4 e IPv6, consulta [Assegnazione degli indirizzi IP](#) nella Guida per l'utente di Amazon VPC.
- Per ulteriori informazioni sulla creazione di un'istanza di replica tramite la modalità dual-stack, consulta [Creazione di un'istanza di replica](#).
- Per ulteriori informazioni sulla modifica di un'istanza di replica, consulta [Modifica di un'istanza di replica](#).

Configurazione di una rete per un'istanza di replica

AWS DMS crea sempre l'istanza di replica in un VPC basato su Amazon VPC. Puoi specificare il VPC in cui è posizionata l'istanza di replica. Puoi usare il tuo VPC predefinito per il tuo account e la tua AWS regione oppure puoi creare un nuovo VPC.

Assicurati che l'interfaccia di rete elastica allocata per il VPC dell'istanza di replica sia associata a un gruppo di sicurezza. Inoltre, assicurati che le regole del gruppo di sicurezza consentano a tutto il traffico su tutte le porte di uscire dal VPC. Questo approccio consente la comunicazione dall'istanza di replica agli endpoint dei database di origine e di destinazione, purché su tali endpoint siano abilitate le regole di uscita corrette. È consigliabile utilizzare le impostazioni predefinite per gli endpoint, che consentono l'uscita su tutte le porte in tutti gli indirizzi.

Gli endpoint di origine e di destinazione accedono all'istanza di replica all'interno del VPC connettendosi al VPC o rimanendo all'interno del VPC. Gli endpoint del database devono includere le liste di controllo degli accessi di rete (ACL) e le regole dei gruppi di sicurezza (se applicabili) che consentono l'accesso in entrata dall'istanza di replica. La modalità di impostazione dipende dalla configurazione di rete utilizzata. Puoi utilizzare il gruppo di sicurezza VPC dell'istanza di replica, l'indirizzo IP privato o pubblico dell'istanza di replica o l'indirizzo IP pubblico del gateway NAT. Queste connessioni creano una rete che viene utilizzata per la migrazione dei dati.

Note

Poiché un indirizzo IP può cambiare a seguito di modifiche all'infrastruttura sottostante, ti consigliamo di utilizzare un intervallo CIDR VPC o di indirizzare il traffico in uscita dell'istanza di replica attraverso un IP elastico associato a un gateway NAT. Per ulteriori informazioni sulla creazione di un VPC, incluso un blocco CIDR, consulta [Utilizzo di VPC e sottoreti](#) nella Guida per l'utente di Amazon Virtual Private Cloud. Per ulteriori informazioni sugli indirizzi IP elastici, consulta [Indirizzi IP elastici](#) nella Guida per l'utente di Amazon Elastic Compute Cloud.

Configurazioni di rete per la migrazione del database

È possibile utilizzare diverse configurazioni di rete con AWS Database Migration Service. Di seguito sono riportate le configurazioni comuni per una rete utilizzata per la migrazione del database.

Argomenti

- [Configurazione con tutti i componenti di migrazione del database in un VPC](#)
- [Configurazione con più VPC](#)
- [Configurazione con VPC condivisi](#)
- [Configurazione per una rete verso un VPC utilizzando AWS Direct Connect o una VPN](#)
- [Configurazione di una rete per un VPC mediante Internet](#)

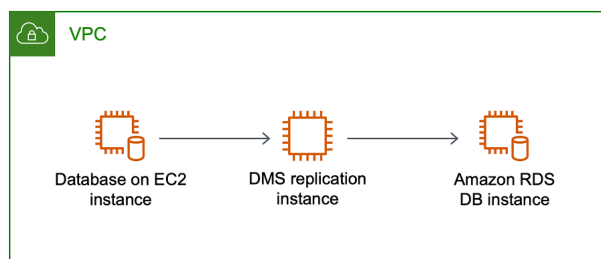
- [Configurazione con un'istanza DB RDS non in un VPC su un'istanza DB in un VPC utilizzando ClassicLink](#)

Se possibile, è consigliabile creare un'istanza di replica DMS nella stessa regione dell'endpoint di destinazione e nello stesso VPC o nella stessa sottorete dell'endpoint di destinazione.

Configurazione con tutti i componenti di migrazione del database in un VPC

La rete più semplice per la migrazione del database è quella in cui l'endpoint di origine, l'istanza di replica e l'endpoint di destinazione si trovano tutti nello stesso VPC. Questa configurazione è appropriata se gli endpoint di origine e di destinazione si trovano su un'istanza database Amazon RDS o su un'istanza Amazon EC2.

La figura seguente illustra una configurazione in cui un database su un'istanza Amazon EC2 si connette all'istanza di replica e i dati vengono migrati in un'istanza database Amazon RDS.



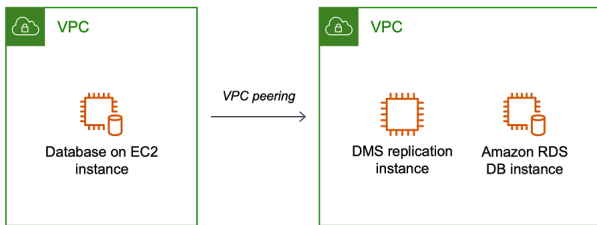
Il gruppo di sicurezza VPC utilizzato in questa configurazione deve consentire l'ingresso sulla porta del database dall'istanza di replica. Ci sono due modi per farlo. È possibile garantire che il gruppo di sicurezza utilizzato dall'istanza di replica abbia accesso agli endpoint. Oppure puoi consentire l'intervallo VPC CIDR, l'IP elastico del gateway NAT o l'indirizzo IP privato dell'istanza di replica, se ne stai utilizzando una. Tuttavia, non è consigliabile utilizzare l'indirizzo IP privato dell'istanza di replica, poiché potrebbe interrompere la replica se l'indirizzo IP di replica cambia.

Configurazione con più VPC

Se l'endpoint di origine e gli endpoint di destinazione si trovano in VPC differenti, puoi creare l'istanza di replica in uno dei VPC. È quindi possibile collegare i due VPC utilizzando il peering VPC.

Una connessione peering di VPC è una connessione di rete tra due VPC che consente di eseguire l'instradamento tramite gli indirizzi IP privati di ciascun VPC come se si trovassero sulla stessa rete. Puoi creare una connessione peering VPC tra i tuoi VPC, con un VPC in un altro account o con un VPC in un'altra AWS regione. AWS Per ulteriori informazioni sul peering di VPC, consulta [Peering di VPC](#) nella Guida per l'utente di Amazon VPC.

La figura seguente illustra una configurazione di esempio che utilizza il peering di VPC. Nella figura, il database di origine su un'istanza Amazon EC2 in un VPC viene collegato a un VPC mediante il peering di VPC. Questo VPC contiene l'istanza di replica e il database di destinazione su un'istanza database Amazon RDS.



Per implementare il peering VPC, segui le istruzioni riportate in [Utilizzo di connessioni peering VPC](#) nella documentazione Peering di VPC di Amazon Virtual Private Cloud. Assicurati che la tabella di routing di un VPC contenga il blocco CIDR dell'altro. Ad esempio, se il VPC A utilizza la destinazione 10.0.0.0/16 e il VPC B utilizza la destinazione 172.31.0.0, la tabella di routing del VPC A deve contenere 172.31.0.0 e la tabella di routing del VPC B deve contenere 10.0.0.0/16. Per informazioni più dettagliate, consulta [Aggiornamento delle tabelle di routing per una connessione peering VPC](#) nella documentazione Peering di VPC di Amazon Virtual Private Cloud.

I gruppi di sicurezza VPC utilizzati in questa configurazione devono consentire l'ingresso sulla porta del database dall'istanza di replica o sul blocco CIDR del VPC in peering.

Configurazione con VPC condivisi

AWS DMS tratta le sottoreti condivise con un account cliente partecipante in un'organizzazione come le normali sottoreti dello stesso account. Di seguito è riportata una descrizione di come AWS DMS gestisce i VPC e le sottoreti e di come è possibile utilizzare i VPC condivisi.

È possibile impostare la configurazione di rete per utilizzare sottoreti o VPC personalizzati creando oggetti `ReplicationSubnetGroup`. Quando crei un oggetto `ReplicationSubnetGroup`, puoi scegliere di specificare le sottoreti di un particolare VPC nel tuo account. L'elenco di sottoreti specificato deve includere almeno due sottoreti che si trovano in zone di disponibilità separate e tutte le sottoreti devono trovarsi nello stesso VPC. Durante la creazione di un `ReplicationSubnetGroup`, i clienti specificano solo le sottoreti. AWS DMS determinerà il VPC per tuo conto, poiché ogni sottorete è collegata esattamente a un VPC.

Quando si crea un `AWS DMS ReplicationInstance` o un `AWS DMS ReplicationConfig`, è possibile scegliere di specificare un gruppo di sicurezza VPC `ReplicationSubnetGroup` e/o un gruppo di sicurezza VPC in cui opera la `ReplicationInstance` o la replica serverless. Se non

specificato, AWS DMS sceglie l'impostazione predefinita del cliente `ReplicationSubnetGroup` (che AWS DMS viene creata per tuo conto se non è specificata per tutte le sottoreti nel VPC predefinito) e il gruppo di sicurezza VPC predefinito.

Puoi scegliere di eseguire le migrazioni in una zona di disponibilità che specifichi oppure in una qualsiasi delle zone di disponibilità del tuo `ReplicationSubnetGroup`. Quando AWS DMS tenta di creare un'istanza di replica o avviare una replica serverless, converte le zone di disponibilità delle sottoreti in zone di disponibilità nell'account di servizio principale, per garantire l'avvio delle istanze nella zona di disponibilità corretta anche se le mappature delle zone di disponibilità non sono identiche tra i due account.

Se utilizzi un VPC condiviso, dovrai assicurarti di creare gli oggetti `ReplicationSubnetGroup` mappati alle sottoreti che desideri utilizzare da un VPC condiviso. Quando crei un oggetto `ReplicationInstance` o `ReplicationConfig`, devi specificare un oggetto `ReplicationSubnetGroup` per il VPC condiviso e un gruppo di sicurezza VPC che hai creato per il VPC condiviso con la richiesta di creazione.

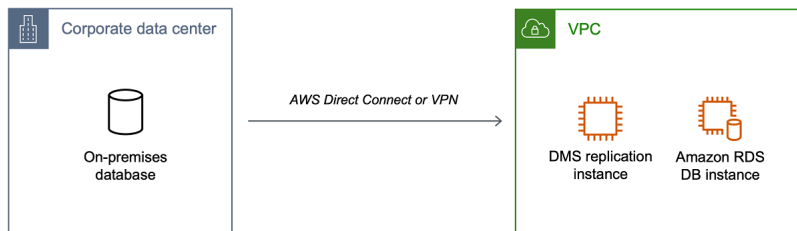
Nota quanto segue in relazione all'utilizzo di un VPC condiviso:

- Il proprietario del VPC non può condividere una risorsa con un partecipante, ma il partecipante può creare una risorsa di servizio nella sottorete del proprietario.
- Il proprietario del VPC non può accedere a una risorsa (come un'istanza di replica) creata dal partecipante perché tutte le risorse sono specifiche dell'account. Tuttavia, se si crea l'istanza di replica nel VPC condiviso, questa può accedere alle risorse nel VPC indipendentemente dall'account proprietario, purché l'endpoint o l'attività di replica disponga delle autorizzazioni corrette.
- Poiché le risorse sono specifiche dell'account, i partecipanti non possono accedere alle risorse di proprietà di altri account. Non ci sono autorizzazioni che puoi fornire ad altri account per consentire loro di accedere alle risorse create nel VPC condiviso con il tuo account.

Configurazione per una rete verso un VPC utilizzando AWS Direct Connect o una VPN

Le reti remote possono connettersi a un VPC utilizzando diverse opzioni come AWS Direct Connect o una connessione VPN software o hardware. Queste opzioni vengono spesso utilizzate per integrare servizi locali esistenti, ad esempio servizi di monitoraggio, autenticazione, sicurezza, dati o altri sistemi, estendendo una rete interna nel cloud AWS. Questo tipo di estensione di rete consente di connettersi senza problemi alle risorse ospitate su AWS, come un VPC.

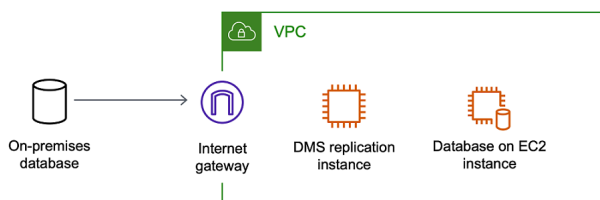
La figura seguente illustra una configurazione in cui l'endpoint di origine è un database locale in un data center aziendale. Mediante AWS Direct Connect o una VPN, il database si connette a un VPC contenente l'istanza di replica e un database di origine su un'istanza database Amazon RDS.



In questa configurazione, il gruppo di sicurezza VPC deve includere una regola di indirizzamento che invia a un host il traffico destinato a un intervallo CIDR del VPC o un indirizzo IP specifico. Questo host deve essere in grado di collegare il traffico del VPC nella VPN locale. In questo caso, l'host NAT include le proprie impostazioni del gruppo di sicurezza. Queste impostazioni devono consentire il traffico proveniente dall'intervallo CIDR del VPC, dall'indirizzo IP privato o dal gruppo di sicurezza dell'istanza di replica all'istanza NAT. Tuttavia, non è consigliabile utilizzare l'indirizzo IP privato dell'istanza di replica, poiché potrebbe interrompere la replica se l'indirizzo IP di replica cambia.

Configurazione di una rete per un VPC mediante Internet

Se non utilizzi una VPN o non ti connetti AWS Direct Connect alle AWS risorse, puoi utilizzare Internet per migrare il database. In questo caso, è possibile eseguire la migrazione a un'istanza Amazon EC2 o a un'istanza database Amazon RDS. Questa configurazione prevede un'istanza di replica pubblica in un VPC con un gateway Internet contenente l'endpoint di destinazione e l'istanza di replica.



Per aggiungere un gateway Internet al VPC, consulta [Collegamento di un gateway Internet](#) nella Guida per l'utente di Amazon VPC.

La tabella di routing VPC deve includere regole di instradamento che, per impostazione predefinita, inviano al gateway Internet il traffico non destinato al VPC. In questa configurazione, la connessione all'endpoint viene eseguita dall'indirizzo IP pubblico dell'istanza di replica e non dall'indirizzo IP privato. Per ulteriori informazioni, consulta [Tabelle di routing VPC](#) nella Guida per l'utente di Amazon VPC.

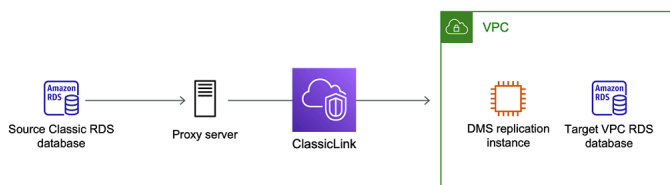
Configurazione con un'istanza DB RDS non in un VPC su un'istanza DB in un VPC utilizzando ClassicLink

Ritireremo EC2-Classic il 15 agosto 2022. Sugeriamo di effettuare la migrazione da EC2-Classic a un VPC. Per ulteriori informazioni, consulta [Eseguire la migrazione da EC2-Classic a un VPC](#) nella Guida per l'utente di Amazon EC2 e il blog [EC2-Classic Networking is Retiring – Here's How to Prepare](#) (Il networking EC2-Classic viene ritirato: ecco come prepararsi).

Per connettere un'istanza DB Amazon RDS non in un VPC a un server di replica DMS e un'istanza DB in un VPC, puoi utilizzarla con un server proxy. ClassicLink

ClassicLink ti consente di collegare un'istanza DB EC2-Classic a un VPC nel tuo account, all'interno della stessa regione. AWS Dopo aver creato il link, l'istanza database di origine può comunicare con l'istanza di replica all'interno del VPC mediante gli indirizzi IP privati.

Poiché l'istanza di replica nel VPC non può accedere direttamente all'istanza DB di origine sulla piattaforma EC2-Classic ClassicLink utilizzando, si utilizza un server proxy. Il server proxy connette l'istanza database di origine al VPC contenente l'istanza di replica e l'istanza database di destinazione. Il server proxy utilizza ClassicLink per connettersi al VPC. L'inoltro della porta sul server proxy consente la comunicazione tra l'istanza database di origine e l'istanza database di destinazione nel VPC.



Utilizzo ClassicLink con AWS Database Migration Service

Puoi connettere un'istanza DB Amazon RDS che non si trova in un VPC a un server di replica DMS e AWS un'istanza DB che si trovano in un VPC. A tale scopo, puoi utilizzare Amazon EC2 ClassicLink con un server proxy.

La procedura seguente mostra come utilizzarlo ClassicLink per questo scopo. Questa procedura collega un'istanza DB di origine Amazon RDS che non si trova in un VPC a un VPC contenente un'istanza di replica DMS e AWS un'istanza DB di destinazione.

- Crea un'istanza di replica AWS DMS in un VPC. Tutte le istanze di replica vengono create in VPC.

- Associa un gruppo di sicurezza VPC all'istanza di replica e all'istanza database di destinazione. Quando due istanze condividono un gruppo di sicurezza VPC, possono comunicare tra loro per impostazione predefinita.
- Configura un server proxy su un'istanza EC2 Classic.
- Crea una connessione ClassicLink tra il server proxy e il VPC.
- Crea endpoint AWS DMS per i database di origine e di destinazione.
- Crea un'attività AWS DMS.

Da utilizzare ClassicLink per migrare un database su un'istanza DB non in un VPC verso un database su un'istanza DB in un VPC

1. Crea un'istanza di replica AWS DMS e assegna un gruppo di sicurezza VPC:
 - a. [Accedi AWS Management Console e apri la console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/). [AWS DMS](#)

Se hai effettuato l'accesso come utente AWS Identity and Access Management (IAM), assicurati di disporre delle autorizzazioni di accesso AWS DMS appropriate. Per ulteriori informazioni sulle autorizzazioni necessarie per la migrazione del database, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).
 - b. Nella pagina Dashboard (Pannello di controllo), scegli Replication Instance (Istanza di replica). Per creare un'istanza di replica, segui le istruzioni riportate nella sezione [Fase 1: creazione di un'istanza di replica mediante la console AWS DMS](#).
 - c. Dopo aver creato l'istanza di replica AWS DMS, apri la console di servizio EC2. Seleziona Interfacce di rete nel riquadro di navigazione.
 - d. Scegli il DMS NetworkInterface, quindi scegli Cambia gruppi di sicurezza dal menu Azioni.
 - e. Scegli il gruppo di sicurezza che desideri utilizzare per l'istanza di replica e l'istanza database di destinazione.
2. Associa il gruppo di sicurezza dell'ultima fase all'istanza database di destinazione:
 - a. Apri la console del servizio Amazon RDS. Nel riquadro di navigazione, scegli Istanze.
 - b. Scegli l'istanza database di destinazione. Per Operazioni istanza scegli Modifica.
 - c. Per il parametro Gruppo di sicurezza seleziona il gruppo di sicurezza che hai usato nella fase precedente.
 - d. Scegli Continua, quindi seleziona Modifica istanza database.

3. Fase 3: configurazione di un server proxy su un'istanza EC2 Classic mediante NGINX. Utilizza un'AMI di tua scelta per avviare un'istanza EC2 Classic. L'esempio seguente si basa sull'AMI Ubuntu Server 14.04 LTS (HVM).

Per configurare un server proxy su un'istanza EC2 Classic

- a. Connettiti all'istanza EC2 Classic e installa NGINX utilizzando i comandi seguenti:

```
Prompt> sudo apt-get update
Prompt> sudo wget http://nginx.org/download/nginx-1.9.12.tar.gz
Prompt> sudo tar -xvzf nginx-1.9.12.tar.gz
Prompt> cd nginx-1.9.12
Prompt> sudo apt-get install build-essential
Prompt> sudo apt-get install libpcre3 libpcre3-dev
Prompt> sudo apt-get install zlib1g-dev
Prompt> sudo ./configure --with-stream
Prompt> sudo make
Prompt> sudo make install
```

- b. Modificare il file del daemon NGINX, `/etc/init/nginx.conf`, utilizzando il seguente codice:

```
# /etc/init/nginx.conf - Upstart file

description "nginx http daemon"
author "email"

start on (filesystem and net-device-up IFACE=lo)
stop on runlevel [!2345]

env DAEMON=/usr/local/nginx/sbin/nginx
env PID=/usr/local/nginx/logs/nginx.pid

expect fork
respawn
respawn limit 10 5

pre-start script
    $DAEMON -t
    if [ $? -ne 0 ]
```



```
        then exit $?
    fi
end script

exec $DAEMON
```

- c. Creare un file di configurazione NGINX in `/usr/local/nginx/conf/nginx.conf`. Nel file di configurazione aggiungi quanto segue:

```
# /usr/local/nginx/conf/nginx.conf - NGINX configuration file

worker_processes 1;

events {
    worker_connections 1024;
}

stream {
    server {
        listen DB instance port number;
        proxy_pass DB instance identifier:DB instance port number;
    }
}
```

- d. Dalla riga di comando, avvia NGINX utilizzando i comandi seguenti:

```
Prompt> sudo initctl reload-configuration
Prompt> sudo initctl list | grep nginx
Prompt> sudo initctl start nginx
```

4. Crea una ClassicLink connessione tra il server proxy e il VPC di destinazione che contiene l'istanza DB di destinazione e l'istanza di replica:
- Apri la console EC2 e scegli l'istanza EC2 Classic su cui è in esecuzione il server proxy.
 - Per Azioni, scegli ClassicLink, quindi scegli Collega a VPC.
 - Scegli il gruppo di sicurezza che hai usato in precedenza in questa procedura.

- d. Scegli Collegamento a VPC.
5. Passaggio 5: Creare endpoint AWS DMS utilizzando la procedura descritta in [Fase 2: specificazione degli endpoint di origine e di destinazione](#). Dovrai utilizzare il nome host DNS EC2 interno del proxy come nome del server quando specifichi l'endpoint di origine.
6. Creare un'attività AWS DMS utilizzando la procedura in [Fase 3: creazione di un'attività e migrazione dei dati](#)

Creazione di un gruppo di sottoreti di replica

Nella rete da utilizzare per la migrazione del database è necessario specificare le sottoreti del cloud privato virtuale (VPC) che intendi utilizzare. Il VPC si deve basare sul servizio Amazon VPC. Una sottorete è un intervallo di indirizzi IP nel VPC all'interno di una determinata zona di disponibilità. Queste sottoreti possono essere distribuite tra le zone di disponibilità della AWS regione in cui si trova il VPC.

Quando crei un'istanza di replica o un profilo di istanza nella console AWS DMS, puoi utilizzare la sottorete che preferisci.

Puoi creare un gruppo di sottoreti di replica per definire le sottoreti da utilizzare. È necessario specificare le sottoreti in almeno due zone di disponibilità.

Per creare un gruppo di sottoreti di replica

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni necessarie per la migrazione del database, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Nel pannello di navigazione selezionare Subnet groups (Gruppi di sottoreti).
3. Scegli Crea gruppo di sottoreti.
4. Nella pagina Crea gruppo di sottoreti di replica specifica le informazioni sul gruppo di sottoreti di replica. Nella tabella seguente vengono illustrate le impostazioni.

Opzione	Azione
Nome	Immetti un nome per il gruppo di sottoreti di replica contenente da 8 a 16 caratteri ASCII stampabili (esclusi /, " e @). Il nome deve essere univoco per il tuo account per la AWS regione selezionata. Puoi scegliere di aggiungere alcune informazioni al nome, ad esempio includere la AWS regione e l'attività che stai eseguendo DMS-default-VPC .
Descrizione	Immetti una breve descrizione del gruppo di sottoreti di replica.
VPC	Scegli il VPC che desideri utilizzare per la migrazione e del database. Tieni presente che il VPC deve disporre di almeno una sottorete in almeno due zone di disponibilità.
Aggiungi sottoreti	Scegli le sottoreti che desideri includere nel gruppo di sottoreti di replica. È necessario selezionare le sottoreti in almeno due zone di disponibilità.

5. Scegli Crea gruppo di sottoreti.

Risoluzione degli endpoint di dominio con DNS

Di solito, un'istanza di AWS DMS replica utilizza il resolver Domain Name System (DNS) in un'istanza Amazon EC2 per risolvere gli endpoint di dominio. Se devi eseguire la risoluzione DNS, puoi utilizzare il risolutore Amazon Route 53. Per ulteriori informazioni sull'utilizzo del risolutore DNS Route 53, consulta [Nozioni di base su Route 53 Resolver](#).

Per informazioni su come utilizzare il server dei nomi on-premise per risolvere determinati endpoint con il risolutore Amazon Route 53, consulta [Utilizzo del server dei nomi in locale](#).

Impostazione di una chiave di crittografia per un'istanza di replica

AWS DMS crittografa lo storage utilizzato da un'istanza di replica e le informazioni di connessione all'endpoint. Per crittografare lo storage utilizzato da un'istanza di replica, AWS DMS utilizza un AWS KMS key file univoco per l'account dell'utente. AWS È possibile visualizzare e gestire questa chiave KMS con (). AWS Key Management Service AWS KMS Puoi utilizzare la chiave KMS predefinita nel tuo account (aws/dms) o puoi creare una nuova chiave KMS. Se disponi di una chiave di AWS KMS crittografia esistente, puoi utilizzarla anche per la crittografia.

È possibile specificare la propria chiave di crittografia fornendo un identificatore di chiave KMS per crittografare le risorse DMS. AWS Quando specifichi una chiave di crittografia personalizzata, l'account utente utilizzato per eseguire la migrazione del database deve avere accesso a tale chiave. Per ulteriori informazioni sulla creazione delle chiavi di crittografia personalizzate e sull'assegnazione agli utenti dell'accesso a una chiave di crittografia, consulta la [Guida per gli sviluppatori di AWS KMS](#).

Se non specifichi un identificatore di chiave KMS, DMS utilizza la chiave di crittografia predefinita. AWS KMS crea la chiave di crittografia predefinita per AWS DMS per il tuo account. AWS Il tuo AWS account ha una chiave di crittografia predefinita diversa per ogni AWS regione.

Per gestire le chiavi utilizzate per crittografare le risorse AWS DMS, si utilizza. AWS KMS Puoi trovarlo cercando KMS AWS KMS nel pannello di navigazione. AWS Management Console

AWS KMS combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Utilizzando AWS KMS, è possibile creare chiavi di crittografia e definire le politiche che controllano il modo in cui tali chiavi possono essere utilizzate. AWS KMS supporta AWS CloudTrail, in modo da poter controllare l'utilizzo delle chiavi per verificare che vengano utilizzate in modo appropriato. AWS KMS Le chiavi possono essere utilizzate in combinazione con AWS DMS e altri servizi supportati AWS . I servizi AWS supportati sono Amazon RDS, Amazon S3, Amazon Elastic Block Store (Amazon EBS) e Amazon Redshift.

Dopo aver creato le risorse AWS DMS con una chiave di crittografia specifica, non è possibile modificare la chiave di crittografia per tali risorse. Assicurati di determinare i requisiti della chiave di crittografia prima di creare le tue risorse AWS DMS.

Creazione di un'istanza di replica

La prima attività della migrazione di un database è creare un'istanza di replica. L'istanza di replica deve disporre di storage e potenza di elaborazione sufficienti per eseguire le attività assegnate e

migrare i dati dal database di origine al database di destinazione. La dimensione richiesta di questa istanza varia a seconda della quantità di dati da migrare e delle attività che deve eseguire l'istanza. Per ulteriori informazioni sulle istanze di replica, consulta [Utilizzo di un'istanza di AWS DMS replica](#).

Per creare un'istanza di replica utilizzando la console AWS

1. Scegli Istanze di replica nel riquadro di navigazione della AWS DMS console, quindi scegli Crea istanza di replica.
2. Nella pagina Create replication instance (Crea istanza di replica), specifica le informazioni sull'istanza di replica. Nella tabella seguente vengono descritte le impostazioni che è possibile definire.

Opzione	Azione
Nome	Immetti un nome per l'istanza di replica, che contenga da 8 a 16 caratteri ASCII stampabili (esclusi /, " e @). Il nome deve essere univoco all'interno dell'account nella regione AWS selezionata. Puoi scegliere di aggiungere alcune informazioni al nome, ad esempio includendo la AWS regione e l'attività che stai eseguendo. west2-mysql12mysql1-instance1
Nome della risorsa Amazon (ARN) descrittivo: facoltativo	Un nome descrittivo per sovrascrivere l'ARN DMS predefinito. Non è possibile modificarlo dopo la creazione.
Descrizione	Immetti una breve descrizione dell'istanza di replica.
Instance class (Classe istanza)	Scegli una classe dell'istanza con la configurazione necessaria per la migrazione. Tieni presente che l'istanza deve disporre di storage, rete e potenza di elaborazione sufficienti per completare la migrazione. Per ulteriori informazioni su come stabilire la classe dell'istanza ideale per la migrazione, consulta Utilizzo di un'istanza di AWS DMS replica .
Versione del motore	Nella AWS DMS console, puoi scegliere qualsiasi versione del motore supportata che desideri. Da AWS

Opzione	Azione
	CLI, l'istanza di replica esegue l'ultima versione non beta del motore di AWS DMS replica, a meno che non si specifichi una versione diversa del motore in. AWS CLI
Elevata disponibilità	Utilizza questo parametro opzionale per creare una replica di standby dell'istanza di replica in un'altra zona di disponibilità per il supporto del failover. Se desideri utilizzare l'acquisizione dei dati di modifica (CDC) o la replica continua, dovrai attivare questa opzione.

Opzione	Azione
Storage allocato (GiB)	<p data-bbox="727 226 1507 550">Lo storage è principalmente consumato dai file di log e dalle transazioni memorizzate nella cache. Per le transazioni memorizzate nella cache, lo storage viene utilizzato solo quando le transazioni memorizzate nella cache devono essere scritte su disco. Pertanto, AWS DMS non utilizza una quantità significativa di storage. Di seguito sono riportate alcune eccezioni:</p> <ul data-bbox="727 592 1507 1507" style="list-style-type: none"><li data-bbox="727 592 1507 915">• Tabelle di grandissime dimensioni che sostengono o un notevole carico di transazioni. Il caricamento di una tabella di grandi dimensioni può richiedere del tempo, perciò le transazioni memorizzate nella cache hanno maggiori probabilità di essere scritte su disco durante il caricamento di una tabella di grandi dimensioni.<li data-bbox="727 936 1507 1306">• Le attività configurate per la sospensione prima del caricamento delle transazioni memorizzate nella cache. In questo caso, tutte le transazioni vengono memorizzate nella cache fino alla conclusione del caricamento completo per tutte le tabelle. Con questa configurazione, le transazioni memorizzate nella cache potrebbero consumare una buona quantità di storage.<li data-bbox="727 1327 1507 1507">• Attività configurate con tabelle in fase di caricamento in Amazon Redshift. Tuttavia, questa configurazione non rappresenta un problema quando Amazon Aurora è la destinazione. <p data-bbox="727 1579 1464 1852">Nella maggior parte dei casi, è sufficiente l'allocazione dello storage predefinita. Tuttavia, è sempre consigliabile prestare attenzione ai parametri relativi allo storage. Assicurati di aumentare lo spazio di storage se scopri che stai consumando più dell'allocazione predefinita.</p>

Opzione	Azione
Tipo di rete	DMS supporta il tipo di rete con protocollo di indirizzamento IPv4 e i tipi di rete con protocollo di indirizzamento IPv4 e IPv6 in modalità dual-stack. Utilizza la modalità dual-stack se le risorse devono comunicare con l'istanza database tramite il protocollo di indirizzamento IPv6. Per informazioni sulle limitazioni della modalità dual-stack, consulta Limitazioni per istanze database di rete dual-stack nella Guida per l'utente di Amazon Relational Database Service .
VPC	Scegli il VPC che vuoi utilizzare. Se il database di origine o di destinazione si trova in un VPC, scegli tale VPC. Se i database di origine e di destinazione sono in VPC diversi, assicurati che siano entrambi in sottoreti pubbliche e che siano accessibili pubblicamente, quindi scegli il VPC in cui deve essere posizionata l'istanza di replica. L'istanza di replica deve essere in grado di accedere ai dati nel VPC di origine. Se né il database di origine né quello di destinazione sono in un VPC, scegli un VPC in cui deve essere posizionata l'istanza di replica.
Replication Subnet Group (Gruppi di sottoreti di replica)	Scegli il gruppo di sottoreti di replica nel VPC selezionato in cui desideri creare l'istanza di replica. Se il database di origine è in un VPC, scegli il gruppo di sottoreti che contiene il database di origine come posizione per l'istanza di replica. Per ulteriori informazioni sui gruppi di sottoreti di replica, consulta Creazione di un gruppo di sottoreti di replica .
Accessibile pubblicamente	Scegli questa opzione se desideri che l'istanza di replica sia accessibile da Internet. L'impostazione predefinita è accessibile pubblicamente e, una volta scelta l'opzione, non è possibile modificarla dopo aver creato l'istanza di replica.

3. Scegliere la scheda Advanced per configurare i valori per le impostazioni di rete e crittografia, se necessari. Nella tabella seguente vengono illustrate le impostazioni.

Opzione	Azione
Availability zone (Zona di disponibilità)	Scegli la zona di disponibilità in cui si trova il database di origine.
VPC Security group(s) (Gruppi di sicurezza VPC)	L'istanza di replica viene creata in un VPC. Se il database di origine è in un VPC, scegli il gruppo di sicurezza VPC che fornisce accesso all'istanza database in cui risiede il database.
Chiave KMS	Scegli la chiave di crittografia da utilizzare per crittografare le informazioni sulla connessione e sullo storage di replica. Se scegli (Predefinito) aws/dms, viene utilizzata la chiave predefinita AWS Key Management Service (AWS KMS) associata al tuo account e AWS alla tua regione. Vengono mostrati una descrizione e il numero di account, insieme all'ARN della chiave. Per ulteriori informazioni sull'utilizzo della chiave di crittografia, consulta Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS .

4. Specifica le impostazioni di Maintenance (Manutenzione). Nella tabella seguente vengono illustrate le impostazioni. Per ulteriori informazioni sulle impostazioni di manutenzione, consulta [Utilizzo della finestra di manutenzione AWS DMS](#).

Opzione	Azione
Aggiornamento automatico della versione	AWS DMS non fa distinzione tra versioni principali e secondarie. Ad esempio, l'aggiornamento dalla versione 3.4.x alla 3.5.x non è considerato un aggiornamento di versione principale, quindi tutte le modifiche devono essere compatibili con le versioni precedenti.

Opzione	Azione
	<p>Quando l'aggiornamento automatico della versione è abilitato, DMS aggiorna automaticamente la versione dell'istanza di replica, se è obsoleta, durante la finestra di manutenzione.</p> <p>Quando <code>AutoMinorVersionUpgrade</code> è abilitato, DMS utilizza la versione corrente del motore predefinito quando si crea un'istanza di replica. Ad esempio, se si imposta <code>Versione del motore</code> su un numero di versione inferiore rispetto alla versione predefinita corrente, DMS utilizza la versione predefinita.</p> <p>Se <code>AutoMinorVersionUpgrade</code> non è abilitato quando si crea un'istanza di replica, DMS utilizza la versione del motore specificata dal parametro <code>Engine version</code>.</p>
Maintenance window (Finestra di manutenzione)	<p>Scegli un intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.</p> <p>Impostazione predefinita: una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per AWS regione, che si verifica in un giorno casuale della settimana.</p>

5. Scegli `Create replication instance` (Crea istanza di replica).

Modifica di un'istanza di replica

Puoi modificare le impostazioni di un'istanza di replica, ad esempio, per cambiare la classe dell'istanza o per aumentare lo storage.

Quando modifichi un'istanza di replica, puoi applicare le modifiche immediatamente. Per applicare le modifiche immediatamente, puoi scegliere l'opzione `Applica immediatamente le modifiche` nella AWS Management Console. Oppure usa il `--apply-immediately` parametro quando chiami o imposta AWS CLI il `ApplyImmediately` parametro su `true` quando usi l'API DMS.

Se non scegli di applicare le modifiche immediatamente, le modifiche vengono inserite nella coda delle modifiche in sospeso. Durante la finestra di manutenzione successiva, le eventuali modifiche in sospeso incluse nella coda vengono eseguite.

Note

Se scegli 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 dell'opzione Apply changes immediately (Applica immediatamente le modifiche) può determinare tempi di inattività imprevisti.

Per modificare un'istanza di replica utilizzando la console AWS

1. Accedere AWS Management Console e aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegli l'istanza di replica che desideri modificare. Nella tabella seguente vengono descritte le modifiche che è possibile apportare.

Opzione	Azione
Nome	Puoi modificare il nome dell'istanza di replica. Immetti un nome per l'istanza di replica, che contenga da 8 a 16 caratteri ASCII stampabili (esclusi /, " e @). Il nome deve essere univoco all'interno dell'account nella regione AWS selezionata. Puoi scegliere di aggiungere alcune informazioni al nome, ad esempio includendo la AWS regione e l'attività che stai eseguendo west2-mysql2mysql-instance1 .
Descrizione	Revisiona o immetti una breve descrizione dell'istanza di replica.
Instance class (Classe istanza)	Puoi modificare la classe dell'istanza. Scegli una classe dell'istanza con la configurazione necessaria per la migrazione. La modifica della classe dell'istanza

Opzione	Azione
	<p>causa il riavvio dell'istanza di replica. Questo riavvio si verifica durante la finestra di manutenzione successiva oppure può verificarsi immediatamente se scegli l'opzione Applica immediatamente le modifiche.</p> <p>Per ulteriori informazioni su come stabilire la classe dell'istanza ideale per la migrazione, consulta Utilizzo di un'istanza di AWS DMS replica.</p>
Versione del motore	<p>Puoi aggiornare la versione del motore utilizzata dall'istanza di replica. L'aggiornamento della versione del motore di replica causa l'arresto dell'istanza di replica mentre è in corso l'aggiornamento.</p>
Multi-AZ	<p>Puoi modificare questa opzione per creare una replica di standby dell'istanza di replica in un'altra zona di disponibilità per supportare il failover oppure puoi rimuovere questa opzione. Se intendi utilizzare la funzionalità CDC (Change Data Capture), la replica continua, devi abilitare questa opzione.</p>

Opzione	Azione
Storage allocato (GiB)	<p data-bbox="727 226 1507 594">Lo storage è principalmente consumato dai file di log e dalle transazioni memorizzate nella cache. Per le transazioni memorizzate nella cache, lo storage viene utilizzato solo quando le transazioni memorizzate nella cache devono essere scritte su disco. Pertanto, AWS DMS non utilizza una quantità significativa di spazio di archiviazione. Di seguito sono riportate alcune eccezioni:</p> <ul data-bbox="727 640 1507 1549" style="list-style-type: none"><li data-bbox="727 640 1507 961">• Tabelle di grandissime dimensioni che sostengono o un notevole carico di transazioni. Il caricamento di una tabella di grandi dimensioni può richiedere del tempo, perciò le transazioni memorizzate nella cache hanno maggiori probabilità di essere scritte su disco durante il caricamento di una tabella di grandi dimensioni.<li data-bbox="727 982 1507 1350">• Le attività configurate per la sospensione prima del caricamento delle transazioni memorizzate nella cache. In questo caso, tutte le transazioni vengono memorizzate nella cache fino alla conclusione del caricamento completo per tutte le tabelle. Con questa configurazione, le transazioni memorizzate nella cache potrebbero consumare una buona quantità di storage.<li data-bbox="727 1371 1507 1549">• Attività configurate con tabelle in fase di caricamento in Amazon Redshift. Tuttavia, questa configurazione non rappresenta un problema quando Amazon Aurora è la destinazione. <p data-bbox="727 1627 1469 1854">Nella maggior parte dei casi, è sufficiente l'allocazione dello storage predefinita. Tuttavia, è sempre consigliabile prestare attenzione ai parametri relativi allo storage e ampliare lo storage se si consuma più dell'allocazione predefinita.</p>

Opzione	Azione
Tipo di rete	DMS supporta il tipo di rete con protocollo di indirizzamento IPv4 e i tipi di rete con protocollo di indirizzamento IPv4 e IPv6 in modalità dual-stack. Scegli la modalità dual-stack se le risorse devono comunicare con l'istanza database tramite il protocollo di indirizzamento IPv6. Per informazioni sulle limitazioni della modalità dual-stack, consulta Limitazioni per istanze database di rete dual-stack nella Guida per l'utente di Amazon Relational Database Service .
Gruppi di sicurezza VPC	L'istanza di replica viene creata in un VPC. Se il database di origine è in un VPC, scegli il gruppo di sicurezza VPC che fornisce accesso all'istanza database in cui risiede il database.

Opzione	Azione
Aggiornamento automatico della versione	<p>AWS DMS non fa distinzione tra versioni principali e secondarie. Ad esempio, l'aggiornamento dalla versione 3.4.x alla 3.5.x non è considerato un aggiornamento di versione principale, quindi tutte le modifiche devono essere compatibili con le versioni precedenti. Quando l'aggiornamento automatico della versione è abilitato, DMS aggiorna automaticamente la versione dell'istanza di replica, se è obsoleta, durante la finestra di manutenzione.</p> <p>Quando l'aggiornamento automatico della versione è abilitato, DMS utilizza la versione corrente del motore predefinito quando si crea un'istanza di replica. Ad esempio, se si imposta Versione del motore su un numero di versione inferiore rispetto alla versione predefinita corrente, DMS utilizza la versione predefinita.</p> <p>Se l'aggiornamento automatico della versione non è abilitato quando si crea un'istanza di replica, DMS utilizza la versione del motore specificata dal parametro Versione del motore.</p>
Maintenance window (Finestra di manutenzione)	<p>Scegli un intervallo temporale settimanale nel fuso orario UTC (Universal Coordinated Time) durante il quale può verificarsi la manutenzione dei sistemi.</p> <p>Predefinito: una finestra di 30 minuti selezionata a caso da un intervallo di tempo di 8 ore per AWS regione, che si verifica in un giorno casuale della settimana.</p>

Opzione	Azione
Apply changes immediately (Applica immediatamente le modifiche)	<p>Scegli questa opzione per applicare immediatamente le modifiche apportate. A seconda delle impostazioni scelte, la selezione di questa opzione potrebbe causare il riavvio immediato dell'istanza di replica.</p> <p>Se scegli Testa la connessione mentre AWS DMS applica le modifiche, verrà visualizzato un messaggio di errore. Dopo aver applicato le modifiche all'istanza di replica, scegli nuovamente Testa connessione.</p>
Applica le modifiche durante la finestra di manutenzione successiva	Scegli questa opzione se desideri che DMS attenda fino alla successiva finestra di manutenzione programmata per applicare le modifiche.

riavvio di un'istanza di replica.

È possibile riavviare un'istanza di AWS DMS replica per riavviare il motore di replica. Il riavvio determina un'interruzione momentanea dell'istanza di replica, durante la quale lo stato dell'istanza viene impostato su Rebooting (Riavvio in corso). Se l'AWS DMS istanza è configurata per Multi-AZ, il riavvio può essere eseguito con un failover. Al termine del riavvio viene creato un AWS DMS evento.

Se l'AWS DMS istanza è una distribuzione Multi-AZ, è possibile forzare un failover pianificato da una zona di AWS disponibilità all'altra al riavvio. Quando si impone un failover pianificato dell'AWS DMS istanza, AWS DMS chiude le connessioni attive sull'istanza corrente prima di passare automaticamente a un'istanza di standby in un'altra zona di disponibilità. Il riavvio con un failover pianificato consente di simulare un evento di failover pianificato di un'istanza, ad esempio quando si ridimensiona la classe dell'AWS DMS istanza di replica.

Note

Dopo che un riavvio impone un failover da una zona di disponibilità a un'altra, la modifica della zona di disponibilità potrebbe non essere riflessa per alcuni minuti. Questo ritardo appare nelle e nelle chiamate all'API and AWS Management Console. AWS CLI AWS DMS

Se le attività di migrazione sono in esecuzione sull'istanza di replica quando avviene un riavvio, non si verifica alcuna perdita di dati, ma l'attività si interrompe e l'attività passa a uno stato di errore.

Se le tabelle dell'attività di migrazione vengono usate in un caricamento in blocco (fase di pieno carico) e non sono ancora state avviate, entrano in uno stato di errore. Tuttavia, le tabelle completate al momento rimangono in uno stato completato. Quando si verifica un riavvio durante la fase di pieno carico, si consiglia di eseguire uno dei passaggi seguenti.

- Rimuovi dall'attività le tabelle che si trovano nello stato completato e riavvia l'attività con le tabelle rimanenti.
- Crea una nuova attività con le tabelle in stato di errore e in sospeso.

Se le tabelle nell'attività di migrazione si trovano nella fase di replica continua, l'attività riprenderà al termine del riavvio.

Non è possibile riavviare l'istanza di AWS DMS replica se il relativo stato non è nello stato Disponibile. L' AWS DMS istanza può non essere disponibile per diversi motivi, ad esempio una modifica richiesta in precedenza o un'azione relativa alla finestra di manutenzione. Il tempo necessario per riavviare un'istanza di AWS DMS replica è in genere ridotto (meno di 5 minuti).

Riavvio di un'istanza di replica utilizzando la console AWS

Per riavviare un'istanza di replica, utilizzare la console. AWS

Per riavviare un'istanza di replica utilizzando la console AWS

1. [Accedere AWS Management Console e aprire la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/.](https://console.aws.amazon.com/dms/v2/)
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegli l'istanza di replica che desideri riavviare.
4. Scegliere Reboot (Riavvia). Viene visualizzata la finestra di dialogo Riavvia istanza di replica.
5. Seleziona la casella di controllo Riavvia con failover? se hai configurato l'istanza di replica per l'implementazione multi-AZ e desideri eseguire il failover su un'altra zona di disponibilità AWS .
6. Scegliere Reboot (Riavvia).

Riavvio di un'istanza di replica mediante l'interfaccia a riga di comando (CLI)

Per riavviare un'istanza di replica, utilizzate il AWS CLI [reboot-replication-instance](#) comando con il seguente parametro:

- `--replication-instance-arn`

Example Esempio di avvio semplice

L' AWS CLI esempio seguente riavvia un'istanza di replica.

```
aws dms reboot-replication-instance \  
--replication-instance-arn arn of my rep instance
```

Example Esempio di riavvio semplice con failover

L' AWS CLI esempio seguente riavvia un'istanza di replica con failover.

```
aws dms reboot-replication-instance \  
--replication-instance-arn arn of my rep instance \  
--force-planned-failover
```

Riavvio di un'istanza di replica mediante l'API

Per riavviare un'istanza di replica, utilizzate l'[RebootReplicationInstance](#) azione AWS DMS API con i seguenti parametri:

- `ReplicationInstanceArn` = *arn of my rep instance*

Example Esempio di avvio semplice

Il codice di esempio seguente riavvia un'istanza di replica.

```
https://dms.us-west-2.amazonaws.com/  
?Action=RebootReplicationInstance  
&DBInstanceArn=arn of my rep instance  
&SignatureMethod=HmacSHA256  
&SignatureVersion=4  
&Version=2014-09-01
```

```
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140425/us-east-1/dms/aws4_request
&X-Amz-Date=20140425T192732Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=1dc9dd716f4855e9bdf188c70f1cf9f6251b070b68b81103b59ec70c3e7854b3
```

Example Esempio di riavvio semplice con failover

Il seguente esempio di codice riavvia un'istanza di replica e esegue il failover in un'altra zona di disponibilità. AWS

```
https://dms.us-west-2.amazonaws.com/
?Action=RebootReplicationInstance
&DBInstanceArn=arn of my rep instance
&ForcePlannedFailover=true
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-09-01
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140425/us-east-1/dms/aws4_request
&X-Amz-Date=20140425T192732Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=1dc9dd716f4855e9bdf188c70f1cf9f6251b070b68b81103b59ec70c3e7854b3
```

Eliminazione di un'istanza di replica.

È possibile eliminare un'istanza AWS DMS di replica al termine dell'utilizzo. Se l'istanza di replica è utilizzata da attività di migrazione, è necessario arrestare ed eliminare tali attività prima di eliminare l'istanza di replica.

Se chiudi l' AWS account, tutte le AWS DMS risorse e le configurazioni associate all'account vengono eliminate dopo due giorni. Queste risorse includono tutte le istanze di replica, la configurazione degli endpoint di origine e di destinazione, le attività di replica e i certificati SSL. Se dopo due giorni decidi di AWS DMS riutilizzarlo, ricrei le risorse di cui hai bisogno.

Se l'istanza di replica soddisfa tutti i criteri per l'eliminazione e rimane nello stato DELETING per un periodo di tempo prolungato, contatta l'assistenza per risolvere il problema.

Eliminazione di un'istanza di replica tramite la console AWS

Per eliminare un'istanza di replica, utilizzare la console. AWS

Per eliminare un'istanza di replica utilizzando la console AWS

1. Accedere AWS Management Console e aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegli l'istanza di replica da eliminare.
4. Scegli Elimina.
5. Nella finestra di dialogo, scegli Delete (Elimina).

Eliminazione di un'istanza di replica mediante l'interfaccia a riga di comando (CLI)

Per eliminare un'istanza di replica, utilizzate il AWS CLI [delete-replication-instance](#) comando con il seguente parametro:

- `--replication-instance-arn`

Example Esempio di eliminazione

L' AWS CLI esempio seguente elimina un'istanza di replica.

```
aws dms delete-replication-instance \  
--replication-instance-arn arn of my rep instance
```

Eliminazione di un'istanza di replica mediante l'API

Per eliminare un'istanza di replica, utilizzate l'[DeleteReplicationInstance](#) azione AWS DMS API con i seguenti parametri:

- `ReplicationInstanceArn = arn of my rep instance`

Example Esempio di eliminazione

Il codice seguente elimina un'istanza di replica.

```
https://dms.us-west-2.amazonaws.com/  
?Action=DeleteReplicationInstance  
&DBInstanceArn=arn of my rep instance
```

```
&SignatureMethod=HmacSHA256
&SignatureVersion=4
&Version=2014-09-01
&X-Amz-Algorithm=AWS4-HMAC-SHA256
&X-Amz-Credential=AKIADQKE4SARGYLE/20140425/us-east-1/dms/aws4_request
&X-Amz-Date=20140425T192732Z
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date
&X-Amz-Signature=1dc9dd716f4855e9bdf188c70f1cf9f6251b070b68b81103b59ec70c3e7854b3
```

Utilizzo della finestra di manutenzione AWS DMS

Ogni istanza AWS DMS di replica ha una finestra di manutenzione settimanale durante la quale vengono applicate tutte le modifiche al sistema disponibili. La finestra di manutenzione può essere considerata come un'opportunità per controllare quando vengono applicate le modifiche e le patch software.

Se si AWS DMS determina che la manutenzione è necessaria durante una determinata settimana, la manutenzione viene eseguita durante la finestra di manutenzione di 30 minuti scelta al momento della creazione dell'istanza di replica. AWS DMS completa la maggior parte della manutenzione durante la finestra di manutenzione di 30 minuti. Tuttavia, potrebbe essere necessario un periodo di tempo più lungo per applicare modifiche di dimensioni maggiori.

Effetto della manutenzione sulle attività di migrazione esistenti

Quando un'attività di AWS DMS migrazione è in esecuzione su un'istanza, quando viene applicata una patch si verificano i seguenti eventi:

- Se le tabelle dell'attività di migrazione si trovano nella fase di replica delle modifiche in corso (CDC), AWS DMS arresta l'attività per un momento e quindi la riprende dopo l'applicazione della patch. La migrazione quindi prosegue dal punto in cui è stata interrotta quando è stata applicata la patch.
- Se AWS DMS si sta eseguendo la migrazione di una tabella come parte di un'attività di migrazione dei dati esistenti o di migrazione dei dati esistenti e replica delle modifiche in corso, DMS interrompe e riavvia la migrazione per tutte le tabelle in fase di pieno caricamento durante l'applicazione della patch. DMS inoltre arresta e riprende tutte le tabelle in fase CDC mentre viene applicata la patch.

Modifica dell'impostazione della finestra di manutenzione

È possibile modificare l'intervallo di tempo della finestra di manutenzione utilizzando l' AWS Management Console, l'API, AWS CLI o AWS DMS.

Modifica dell'impostazione della finestra di manutenzione mediante la console

Puoi utilizzare la AWS Management Console per modificare l'intervallo di tempo della finestra di manutenzione.

Per modificare la finestra di manutenzione preferita mediante la console

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione, scegli Replication instances (Istanze di replica).
3. Scegli l'istanza di replica che desideri modificare e scegli Modify (Modifica).
4. Espandi la scheda Maintenance (Manutenzione) e scegli una data e un'ora per la finestra di manutenzione.
5. Scegli Apply changes immediately (Applica immediatamente le modifiche).
6. Scegli Modifica.

Modifica dell'impostazione della finestra di manutenzione mediante l'interfaccia a riga di comando (CLI)

Per regolare la finestra di manutenzione preferita, utilizzate il AWS CLI [modify-replication-instance](#) comando con i seguenti parametri.

- `--replication-instance-identifier`
- `--preferred-maintenance-window`

Example

L' AWS CLI esempio seguente imposta la finestra di manutenzione sul martedì dalle 4:00 alle 4:30 UTC.

```
aws dms modify-replication-instance \  
--replication-instance-identifier myrepliance \  
--preferred-maintenance-window
```

```
--preferred-maintenance-window Tue:04:00-Tue:04:30
```

Modifica dell'impostazione della finestra di manutenzione mediante l'API

Per regolare la finestra di manutenzione preferita, utilizzate l'[ModifyReplicationInstance](#) azione AWS DMS API con i seguenti parametri.

- `ReplicationInstanceIdentifier` = *myrepiinstance*
- `PreferredMaintenanceWindow` = *Tue:04:00-Tue:04:30*

Example

Nell'esempio di codice seguente la finestra di manutenzione viene impostata su martedì dalle 4:00 alle 4:30. UTC.

```
https://dms.us-west-2.amazonaws.com/  
?Action=ModifyReplicationInstance  
&DBInstanceIdentifier=myrepiinstance  
&PreferredMaintenanceWindow=Tue:04:00-Tue:04:30  
&SignatureMethod=HmacSHA256  
&SignatureVersion=4  
&Version=2014-09-01  
&X-Amz-Algorithm=AWS4-HMAC-SHA256  
&X-Amz-Credential=AKIADQKE4SARGYLE/20140425/us-east-1/dms/aws4_request  
&X-Amz-Date=20140425T192732Z  
&X-Amz-SignedHeaders=content-type;host;user-agent;x-amz-content-sha256;x-amz-date  
&X-Amz-Signature=1dc9dd716f4855e9bdf188c70f1cf9f6251b070b68b81103b59ec70c3e7854b3
```

Utilizzo degli endpoint AWS DMS

Un endpoint fornisce informazioni sulla connessione, sul tipo di datastore e sulla posizione del tuo datastore. AWS Database Migration Service utilizza queste informazioni per connettersi a un datastore e migrare i dati da un endpoint di origine a un endpoint di destinazione. È possibile specificare gli attributi aggiuntivi di connessione per un endpoint utilizzando le impostazioni degli endpoint. Queste impostazioni possono controllare la registrazione, la dimensione dei file e altri parametri. Per ulteriori informazioni sulle impostazioni degli endpoint, consulta la sezione della documentazione relativa al tuo datastore.

Di seguito puoi trovare ulteriori informazioni sugli endpoint.

Argomenti

- [Creazione di endpoint di origine e destinazione](#)
- [Origini per la migrazione dei dati](#)
- [Destinazioni per la migrazione dei dati](#)
- [Configurazione degli endpoint VPC come endpoint di origine e di destinazione AWS DMS](#)
- [Istruzioni DDL supportate da AWS DMS](#)

Creazione di endpoint di origine e destinazione

Puoi creare endpoint di origine e destinazione durante la creazione dell'istanza di replica o una volta che l'istanza di replica è stata creata. I datastore di origine e destinazione possono trovarsi su un'istanza di Amazon Elastic Compute Cloud (Amazon EC2), un'istanza database di Amazon Relational Database Service (Amazon RDS) o un database locale. Tieni presente che uno dei tuoi endpoint deve utilizzare un servizio AWS. Non è possibile usare AWS DMS per migrare da un database on-premise a un altro database on-premise.

Nelle fasi seguenti si presuppone che tu abbia scelto la procedura guidata della console AWS. Ricorda che puoi eseguire questa operazione anche selezionando Endpoint dal riquadro di navigazione della console AWS DMS e quindi scegliendo Crea endpoint. Quando utilizzi la procedura guidata della console, crei entrambi gli endpoint di origine e destinazione nella stessa pagina. Quando non la utilizzi, crei ciascun endpoint separatamente.

Per specificare gli endpoint di origine e di destinazione del database tramite la console AWS

1. Nella pagina Connect source and target database endpoints (Collega gli endpoint di origine e di destinazione del database), specifica le informazioni di connessione per il database di origine o di destinazione. Nella tabella seguente vengono illustrate le impostazioni.

Per questa opzione	Eseguire questa operazione
Endpoint type (Tipo di endpoint)	Scegli se l'endpoint è di origine o di destinazione.
Select RDS DB Instance (Seleziona un'istanza database RDS)	Scegli questa opzione se l'endpoint è un'istanza database di Amazon RDS.
Endpoint identifier (Identificatore endpoint)	Digita il nome che desideri utilizzare per identificare l'endpoint. Potresti decidere di includere nel nome il tipo di endpoint, ad esempio oracle-source o PostgreSQL-target . Il nome deve essere univoco per tutte le istanze di replica.
Source engine (Motore di origine) e Target engine (Motore di destinazione)	Scegli il tipo di motore di database che rappresenta l'endpoint.
Accesso al database di endpoint	<p>Scegli l'opzione che desideri utilizzare per specificare le credenziali del database endpoint:</p> <ul style="list-style-type: none"> • Scegli AWS Secrets Manager: utilizza i segreti definiti in AWS Secrets Manager per fornire segretamente le tue credenziali come illustrato di seguito. Per ulteriori informazioni sulla creazione di questi segreti e sui ruoli di accesso segreto che consentono ad AWS DMS di accedere, consulta Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service. • Fornisci le informazioni di accesso manualmente: utilizza le credenziali in chiaro immesse direttamente, come illustrato di seguito.

Per questa opzione	Eeguire questa operazione
Scegli AWS Secrets Manager	Imposta le seguenti credenziali segrete.
ID segreto	Digita il nome della risorsa Amazon (ARN) completo, l'ARN parziale o il nome descrittivo di un segreto che hai creato in AWS Secrets Manager per l'accesso al database di endpoint.
Ruolo IAM	Digita l'ARN di un ruolo di accesso al segreto che hai creato in IAM per fornire ad AWS DMS l'accesso per tuo conto al segreto identificato da ID del segreto. Per informazioni sulla creazione di un ruolo di accesso al segreto, consulta Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service .
ID del segreto per Oracle Automatic Storage Management (ASM)	Solo per gli endpoint di origine Oracle che utilizzano Oracle ASM digita il nome della risorsa Amazon (ARN) completo, l'ARN parziale o il nome descrittivo di un segreto che hai creato in AWS Secrets Manager per l'accesso a Oracle ASM. Questo segreto viene in genere creato per accedere a Oracle ASM sullo stesso server del segreto identificato da ID del segreto.
Ruolo IAM per Oracle ASM	Solo per gli endpoint di origine Oracle che utilizzano Oracle ASM digita l'ARN di un ruolo di accesso al segreto che hai creato in IAM per fornire ad AWS DMS l'accesso per tuo conto al segreto identificato da ID del segreto per Oracle Automatic Storage Management (ASM).
Fornisci le informazioni di accesso manualmente	Imposta le seguenti credenziali in chiaro.

Per questa opzione	Eseguire questa operazione
Server name (Nome del server)	Digita il nome del server. Per un database locale, questo può essere l'indirizzo IP o il nome host pubblico. Per un'istanza database di Amazon RDS, questo può essere l'endpoint (chiamato anche nome DNS) per l'istanza database, ad esempio mysqlsrvinst.abcd12345678.us-west-2.rds.amazonaws.com .
Porta	Digita la porta utilizzata dal database.
Modalità Secure Socket Layer (SSL)	Scegli una modalità SSL se desideri abilitare la crittografia di connessione per questo endpoint. A seconda del modo selezionato, è possibile che ti venga richiesto di fornire le informazioni sul certificato e sul certificato server.
Nome utente	Digita il nome utente con le autorizzazioni richieste per consentire la migrazione dei dati. Per ulteriori informazioni sulle autorizzazioni richieste, consulta la sezione relativa alla sicurezza del motore di database di origine o di destinazione di questa Guida per l'utente.
Password	Digita la password dell'account con le autorizzazioni richieste. Le password per gli endpoint di origine e di destinazione AWS DMS prevedono restrizioni sui caratteri, a seconda del motore di database. Per ulteriori informazioni, consulta la tabella seguente.
Nome del database	Per alcuni motori di database, il nome del database che desideri utilizzare come database di endpoint.

La tabella seguente elenca i caratteri non supportati nelle password degli endpoint e nei segreti dei gestori segreti per i motori di database elencati. Se desideri utilizzare le virgole (,) nelle password degli endpoint, usa il supporto Secrets Manager fornito in AWS DMS per autenticare

l'accesso alle istanze AWS DMS. Per ulteriori informazioni, consulta [Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service](#).

Per questo motore di database	I seguenti caratteri non sono supportati nelle password di un endpoint e nei segreti del gestore segreto
Tutti	{ }
Microsoft Azure, solo come origine	;
Microsoft SQL Server	, ;
Compatibile con MySQL, inclusi MySQL, MariaDB e Amazon Aurora MySQL	;
Oracle	,
PostgreSQL, Amazon Aurora edizione compatibile con PostgreSQL e Amazon Aurora serverless come destinazione solo per Aurora edizione compatibile con PostgreSQL	; + %
Amazon Redshift, solo come destinazione	, ;

- Scegli Impostazioni endpoint e AWS KMS key se necessario. Puoi testare la connessione dell'endpoint scegliendo Run test (Esegui test). Nella tabella seguente vengono illustrate le impostazioni.

Per questa opzione	Eeguire questa operazione
Impostazioni endpoint	Seleziona qui i parametri di connessione aggiuntivi. Per ulteriori informazioni sulle impostazioni degli endpoint, consulta la sezione della documentazione

Per questa opzione	Eseguire questa operazione
	<p>relativa al motore di origine o al motore di destinazione (specificata nella fase 1).</p> <p>Per un endpoint di origine Oracle che utilizza Oracle ASM, se si sceglie Fornisci le informazioni di accesso manualmente nella fase 1, potrebbe essere necessari o digitare anche le impostazioni degli endpoint per specificare le credenziali utente di Oracle ASM. Per ulteriori informazioni su queste impostazioni degli endpoint per Oracle ASM, consulta Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC.</p>
AWS KMS key	<p>Scegli la chiave di crittografia da utilizzare per crittografare le informazioni sulla connessione e sullo storage di replica. Se scegli Impostazione predefinita aws/dms, viene utilizzata la chiave AWS Key Management Service (AWS KMS) predefinita associata al tuo account e alla tua regione AWS. Per ulteriori informazioni sull'utilizzo della chiave di crittografia, consulta Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS.</p>
Test endpoint connection (optional) (Testa la connessione dell'endpoint (facoltativo))	<p>Aggiungi il nome dell'istanza di replica e del VPC. Per testare la connessione, scegli Run test (Esegui test).</p>

Origini per la migrazione dei dati

AWS Database Migration Service (AWS DMS) può utilizzare molti dei più noti motori di dati come origine per la replica dei dati. L'origine del database può essere un motore autogestito in esecuzione su un'istanza Amazon EC2 o un database on-premise. In alternativa può essere un'origine dati su un servizio AWS, come Amazon RDS o Amazon S3.

Per l'elenco completo di origini valide, consulta [Origini per AWS DMS](#).

Argomenti

- [Utilizzo di un database Oracle come origine per AWS DMS](#)
- [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#)
- [Utilizzo di un database SQL di Azure di Microsoft come origine per AWS DMS](#)
- [Utilizzo di un'istanza gestita da Microsoft Azure SQL come origine per AWS DMS](#)
- [Utilizzo di un server flessibile Microsoft Azure Database per PostgreSQL come origine per AWS DMS](#)
- [Utilizzo di un server flessibile Microsoft Azure Database per MySQL come origine per AWS DMS](#)
- [Utilizzo di OCI MySQL Heatwave come origine per AWS DMS](#)
- [Utilizzo di Google Cloud per MySQL come origine per AWS DMS](#)
- [Utilizzo di Google Cloud per PostgreSQL come origine per AWS DMS](#)
- [Utilizzo di un database PostgreSQL come origine AWS DMS](#)
- [Utilizzo di un database compatibile con MySQL come origine per AWS DMS](#)
- [Utilizzo di un database SAP ASE come origine per AWS DMS](#)
- [Utilizzo di MongoDB come origine per AWS DMS](#)
- [Utilizzo di Amazon DocumentDB \(con compatibilità con MongoDB\) come fonte per AWS DMS](#)
- [Utilizzo di Amazon S3 come sorgente per AWS DMS](#)
- [Utilizzo di IBM Db2 per Linux, Unix, Windows e database Amazon RDS \(Db2 LUW\) come origine per AWS DMS](#)
- [Utilizzo dei database IBM Db2 for z/OS come origine per AWS DMS](#)

Utilizzo di un database Oracle come origine per AWS DMS

È possibile migrare i dati da uno o più database Oracle utilizzando AWS DMS. Con un database Oracle come origine, puoi eseguire la migrazione dei dati a una delle destinazioni supportate da AWS DMS.

AWS DMS supporta le seguenti edizioni del database Oracle:

- Oracle Enterprise Edition
- Oracle Standard Edition
- Oracle Express Edition
- Oracle Personal Edition

Per informazioni sulle versioni dei database Oracle AWS DMS supportate come origine, vedere [Fonti per AWS DMS](#).

Puoi utilizzare il protocollo Secure Sockets Layer (SSL) per crittografare le connessioni tra l'endpoint Oracle e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint Oracle, consulta [Supporto SSL per un endpoint Oracle](#).

AWS DMS supporta l'uso di Oracle Transparent Data Encryption (TDE) per crittografare i dati inattivi nel database di origine. Per ulteriori informazioni sull'utilizzo di Oracle TDE con un endpoint di origine Oracle, consulta [Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS](#).

AWS supporta l'uso di TLS versione 1.2 e successive con gli endpoint Oracle (e tutti gli altri tipi di endpoint) e consiglia l'utilizzo di TLS versione 1.3 o successiva.

Segui questi passaggi per configurare un database Oracle come endpoint di origine: AWS DMS

1. Crea un utente Oracle con le autorizzazioni appropriate per accedere AWS DMS al tuo database di origine Oracle.
2. Crea un endpoint di origine Oracle conforme alla configurazione del database Oracle scelta. Per creare un full-load-only task, non sono necessarie ulteriori configurazioni.
3. Per creare un'attività che gestisca l'acquisizione dei dati di modifica (un'attività solo CDC o a pieno carico e CDC), scegli Oracle LogMiner o AWS DMS Binary Reader per acquisire le modifiche ai dati. La scelta LogMiner di Binary Reader determina alcune delle autorizzazioni e delle opzioni di configurazione successive. Per un confronto tra Binary Reader, consultate la sezione seguente.
LogMiner

Note

Per ulteriori informazioni sulle attività di pieno carico, sola CDC e di pieno carico e CDC, consulta [Creazione di un'attività](#)

Per ulteriori dettagli sull'utilizzo dei database di origine Oracle e AWS DMS, vedere le seguenti sezioni.

Argomenti

- [Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC](#)

- [Flussi di lavoro per la configurazione di un database di origine Oracle autogestito o gestito per AWS](#)
- [AWS DMS Configurazione di un database di origine Oracle](#)
- [Utilizzo di un database Oracle autogestito come fonte per AWS DMS](#)
- [Utilizzo di un database Oracle AWS gestito come fonte per AWS DMS](#)
- [Limitazioni all'uso di Oracle come fonte per AWS DMS](#)
- [Supporto SSL per un endpoint Oracle](#)
- [Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS](#)
- [Metodi di compressione supportati per l'utilizzo di Oracle come fonte per AWS DMS](#)
- [Replica di tabelle annidate utilizzando Oracle come fonte per AWS DMS](#)
- [Memorizzazione di REDO su Oracle ASM quando si utilizza Oracle come origine per AWS DMS](#)
- [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#)
- [Tipi di dati di origine per Oracle](#)

Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC

In AWS DMS, esistono due metodi per leggere i redo log quando si esegue l'acquisizione dei dati di modifica (CDC) per Oracle come fonte: Oracle LogMiner e AWS DMS Binary Reader. LogMiner è un'API Oracle per leggere i redo log online e i redo log file archiviati. Binary Reader è un AWS DMS metodo che legge e analizza direttamente i redo log file non elaborati. Questi metodi hanno le seguenti funzionalità.

Funzionalità	LogMiner	Binary Reader
Facilità di configurazione	Sì	No
Impatto ridotto sull'I/O e sulla CPU del sistema di origine	No	Sì
Prestazioni CDC migliorate	No	Sì
Supporto per i cluster di tabelle Oracle	Sì	No
Supporto per tutti i tipi di Oracle Hybrid Columnar Compression (HCC)	Sì	Parzialmente Binary Reader non supporta QUERY LOW

Funzionalità	LogMiner	Binary Reader
		per le attività con CDC. Tutti gli altri tipi di HCC sono completamente supportati.
Supporto per colonne LOB solo in Oracle 12c	No (il supporto LOB non è disponibile con LogMiner Oracle 12c).	Sì
Supporto per le istruzioni UPDATE che riguardano solo le colonne LOB	No	Sì
Supporto per Oracle Transparent Data Encryption (TDE)	Parzialmente Quando si utilizza Oracle LogMiner, AWS DMS non supporta la crittografia TDE a livello di colonna per Amazon RDS for Oracle.	Parzialmente Binary Reader supporta la crittografia TDE solo per i database Oracle autogestiti.
Supporto per tutti i metodi di compressione Oracle	Sì	No
Supporto per transazioni XA	No	Sì

Funzionalità	LogMiner	Binary Reader
RAC	Sì	Sì
	Non consiglia to, per motivi di prestazioni e per alcune limitazioni interne del DMS.	Altamente consigliato

Note

Per impostazione predefinita, AWS DMS utilizza Oracle LogMiner for (CDC). AWS DMS supporta i metodi di crittografia trasparente dei dati (TDE) quando si lavora con un database di origine Oracle. Se le credenziali TDE specificate non sono corrette, l'attività di AWS DMS migrazione non ha esito negativo, il che può influire sulla replica continua delle tabelle crittografate. Per ulteriori informazioni sulla specifica delle credenziali TDE, consulta [Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS](#).

I principali vantaggi dell'utilizzo di LogMiner with AWS DMS includono quanto segue:

- LogMiner supporta la maggior parte delle opzioni Oracle, come le opzioni di crittografia e le opzioni di compressione. Binary Reader non supporta tutte le opzioni di Oracle, in particolare la compressione e la maggior parte delle opzioni di crittografia.
- LogMiner offre una configurazione più semplice, soprattutto rispetto alla configurazione ad accesso diretto di Binary Reader o quando i redo log vengono gestiti utilizzando Oracle Automatic Storage Management (ASM).
- LogMiner supporta cluster di tabelle utilizzabili da. AWS DMS Binary Reader no.

I principali vantaggi dell'utilizzo di Binary Reader con AWS DMS includono quanto segue:

- Per le migrazioni con un elevato volume di modifiche, LogMiner potrebbero avere un impatto sull'I/O o sulla CPU sul computer che ospita il database di origine Oracle. Binary Reader ha meno possibilità di avere impatto sull'I/O oppure sulla CPU perché i log vengono estratti direttamente anziché tramite più query sul database.

- Per le migrazioni con un elevato volume di modifiche, le prestazioni CDC sono in genere molto migliori quando si utilizza Binary Reader rispetto a Oracle LogMiner.
- Binary Reader supporta CDC per LOB nella versione Oracle 12c. LogMiner non lo fa.

In generale, utilizza Oracle LogMiner per la migrazione del database Oracle a meno che non si verifichi una delle seguenti situazioni:

- È necessario eseguire molte attività di migrazione sul database di origine Oracle.
- Il volume delle modifiche o dei log redo nel database Oracle di origine è elevato oppure si dispone delle modifiche e si utilizza anche Oracle ASM.

Note

Se passi dall'utilizzo di LogMiner Oracle a quello di AWS DMS Binary Reader, assicurati di riavviare l'attività CDC.

Configurazione dell'attività di CDC su un database di origine Oracle

Per consentire a un endpoint di origine Oracle di connettersi al database per un'attività di acquisizione dei dati di modifica (CDC), potrebbe essere necessario specificare gli attributi aggiuntivi di connessione. Questo è valido per un'attività di pieno carico e CDC o per un'attività di sola CDC. Gli attributi di connessione aggiuntivi specificati dipendono dal metodo utilizzato per accedere ai redo log: Oracle LogMiner o AWS DMS Binary Reader.

Gli attributi aggiuntivi di connessione si specificano al momento della creazione di un endpoint di origine. Se sono presenti più impostazioni di attributi di connessione, separale tra loro mediante punti e virgola senza inserire spazi vuoti (ad esempio `oneSetting;thenAnother`).

AWS DMS utilizza per impostazione LogMiner predefinita. Non è necessario specificare gli attributi aggiuntivi di connessione per utilizzarlo.

Per usare Binary Reader per accedere ai log redo, aggiungi i seguenti attributi aggiuntivi di connessione.

```
useLogMinerReader=N;useBfile=Y;
```

Usa il seguente formato per gli attributi di connessione aggiuntivi per accedere a un server che usa ASM con Binary Reader.

```
useLogMinerReader=N;useBfile=Y;asm_user=asm_username;asm_server=RAC_server_ip_address:port_number
+ASM;
```

Imposta il parametro di richiesta Password dell'endpoint sorgente sia per la password dell'utente Oracle sia per la password ASM, separate da una virgola come segue.

```
oracle_user_password,asm_user_password
```

Se l'origine Oracle utilizza ASM, è possibile utilizzare opzioni ad alte prestazioni in Binary Reader per l'elaborazione delle transazioni su larga scala. Queste opzioni includono attributi di connessione aggiuntivi per specificare il numero di thread paralleli (`parallelASMReadThreads`) e il numero di buffer read-ahead (`readAheadBlocks`). L'impostazione congiunta di questi attributi è in grado di migliorare sensibilmente le prestazioni dell'attività di CDC. Le seguenti impostazioni forniscono buoni risultati per la maggior parte delle configurazioni ASM.

```
useLogMinerReader=N;useBfile=Y;asm_user=asm_username;asm_server=RAC_server_ip_address:port_number
+ASM;
parallelASMReadThreads=6;readAheadBlocks=150000;
```

Per ulteriori informazioni sui valori supportati dagli attributi di connessione aggiuntivi, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

Inoltre, le prestazioni di un'attività di CDC con un'origine Oracle che utilizza ASM dipende da altre impostazioni scelte. Queste impostazioni includono gli attributi di connessione AWS DMS aggiuntivi e le impostazioni di configurazione di SQL dell'origine Oracle. Per ulteriori informazioni sugli attributi aggiuntivi di connessione per un'origine Oracle che utilizza ASM, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

È inoltre necessario scegliere un punto di partenza appropriato per l'attività di CDC. In genere, quando si esegue questa operazione, si desidera identificare il punto di elaborazione della transazione che acquisisce la prima transazione aperta da cui iniziare l'attività di CDC. In caso contrario, l'attività di CDC può perdere le transazioni aperte in precedenza. Per un database di origine Oracle, puoi scegliere per l'attività di CDC un punto di partenza nativo basato sul numero di modifica

del sistema (SCN) di Oracle per identificare la prima transazione aperta. Per ulteriori informazioni, consulta [Esecuzione della replica a partire da un punto di inizio CDC](#).

Per ulteriori informazioni sulla configurazione dell'attività di CDC per un database Oracle autogestito come origine, consulta [I privilegi dell'account sono richiesti quando si utilizza Oracle per accedere ai redo log LogMiner](#), [I privilegi dell'account sono necessari quando si utilizza AWS DMS Binary Reader per accedere ai redo log](#) e [Privilegi dell'account aggiuntivi necessari quando si utilizza Binary Reader con Oracle ASM](#).

Per ulteriori informazioni sulla configurazione di CDC per un database Oracle AWS gestito come origine, consulta e. [Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS Utilizzo di Amazon RDS Oracle Standby \(replica di lettura\) come origine con Binary Reader per l'attività di CDC in AWS DMS](#)

Flussi di lavoro per la configurazione di un database di origine Oracle autogestito o gestito per AWSAWS DMS

Flussi di lavoro per la configurazione di un database di origine Oracle autogestito o gestito per AWSAWS DMS

Per configurare un'istanza database di origine autogestito, utilizza le seguenti fasi del flusso di lavoro, a seconda di come esegui l'attività di CDC.

Per questa fase del flusso di lavoro	Se esegui CDC utilizzando CDC, esegui questa operazione e LogMiner	Se esegui l'attività di CDC usando Binary Reader
Concedi i privilegi dell'account Oracle.	Consulta Privilegi dell'account utente richiesti su una fonte Oracle autogestita per AWS DMS .	Per informazioni, consulta Privilegi dell'account utente richiesti su una fonte Oracle autogestita per AWS DMS .
Prepara il database di origine per la replica utilizzando l'attività di CDC.	Consulta Preparazione di un database di origine Oracle autogestito per CDC utilizzando AWS DMS .	Per informazioni, consulta Preparazione di un database di origine Oracle autogestito per CDC utilizzando AWS DMS .

Per questa fase del flusso di lavoro	Se esegui CDC utilizzando CDC, esegui questa operazione e LogMiner	Se esegui l'attività di CDC usando Binary Reader
Fornisci i privilegi dell'utente Oracle aggiuntivi necessari per l'attività di CDC.	Consulta I privilegi dell'account sono richiesti quando si utilizza Oracle per accedere ai redo log LogMiner .	Per informazioni, consulta I privilegi dell'account sono necessari quando si utilizza AWS DMS Binary Reader per accedere ai redo log .
Per un'istanza Oracle con ASM, fornisci i privilegi dell'account utente aggiuntivi, necessari per accedere ad ASM per l'attività di CDC.	Nessuna azione aggiuntiva. AWS DMS supporta Oracle ASM senza privilegi di account aggiuntivi.	Per informazioni, consulta Privilegi dell'account aggiuntivi necessari quando si utilizza Binary Reader con Oracle ASM .
Se non l'hai già fatto, configura l'attività per utilizzare LogMiner o Binary Reader for CDC.	Consulta Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC .	Per informazioni, consulta Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC .
Configura Oracle Standby come origine per l'attività di CDC.	AWS DMS non supporta Oracle Standby come fonte.	Per informazioni, consulta Utilizzo di Oracle Standby autogestito come origine con Binary Reader per l'attività di CDC in AWS DMS .

Utilizza i seguenti passaggi del flusso di lavoro per configurare un'istanza del database AWS di origine Oracle gestita.

Per questa fase del flusso di lavoro	Se esegui CDC utilizzando LogMiner, procedi nel seguente modo	Se esegui l'attività di CDC usando Binary Reader
Concedi i privilegi dell'account Oracle.	Per ulteriori informazioni, consulta Privilegi di account utente richiesti su una fonte	Per ulteriori informazioni, consultare Privilegi di account utente richiesti su una fonte

Per questa fase del flusso di lavoro	Se esegui CDC utilizzando LogMiner, procedi nel seguente modo	Se esegui l'attività di CDC usando Binary Reader
	Oracle gestita per AWSAWS DMS.	Oracle gestita per AWSAWS DMS.
Prepara il database di origine per la replica utilizzando l'attività di CDC.	Per ulteriori informazioni, consulta Configurazione di una fonte Oracle gestita per AWSAWS DMS.	Per ulteriori informazioni, consultare Configurazione di una fonte Oracle gestita per AWSAWS DMS.
Fornisci i privilegi dell'utente Oracle aggiuntivi necessari per l'attività di CDC.	Non sono necessari altri privilegi dell'account.	Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.
Se non l'hai già fatto, configura l'attività in modo che utilizzi LogMiner o Binary Reader for CDC.	Per ulteriori informazioni, consulta Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC.	Per ulteriori informazioni, consultare Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC.
Configura Oracle Standby come origine per l'attività di CDC.	AWS DMS non supporta Oracle Standby come fonte.	Per ulteriori informazioni, consulta Utilizzo di Amazon RDS Oracle Standby (replica di lettura) come origine con Binary Reader per l'attività di CDC in AWS DMS.

Utilizzo di un database Oracle autogestito come fonte per AWS DMS

Il database autogestito è quello puoi configurare e controllare e può trattarsi sia di un'istanza database on-premise che di un database in esecuzione su Amazon EC2. Di seguito, puoi scoprire i privilegi e le configurazioni necessari quando utilizzi un database Oracle autogestito con AWS DMS

Privilegi dell'account utente richiesti su una fonte Oracle autogestita per AWS DMS

Per utilizzare un database Oracle come origine in AWS DMS, concedi i seguenti privilegi all'utente Oracle specificato nelle impostazioni di connessione dell'endpoint Oracle.

Note

Durante la concessione dei privilegi, utilizza il nome effettivo degli oggetti e non i relativi sinonimi. Ad esempio, utilizza `V_$$OBJECT` includendo il carattere di sottolineatura, non `V $$OBJECT` senza il carattere di sottolineatura.

```
GRANT CREATE SESSION TO db_user;  
GRANT SELECT ANY TRANSACTION TO db_user;  
GRANT SELECT ON V_$$ARCHIVED_LOG TO db_user;  
GRANT SELECT ON V_$$LOG TO db_user;  
GRANT SELECT ON V_$$LOGFILE TO db_user;  
GRANT SELECT ON V_$$LOGMNR_LOGS TO db_user;  
GRANT SELECT ON V_$$LOGMNR_CONTENTS TO db_user;  
GRANT SELECT ON V_$$DATABASE TO db_user;  
GRANT SELECT ON V_$$THREAD TO db_user;  
GRANT SELECT ON V_$$PARAMETER TO db_user;  
GRANT SELECT ON V_$$NLS_PARAMETERS TO db_user;  
GRANT SELECT ON V_$$TIMEZONE_NAMES TO db_user;  
GRANT SELECT ON V_$$TRANSACTION TO db_user;  
GRANT SELECT ON V_$$CONTAINERS TO db_user;  
GRANT SELECT ON ALL_INDEXES TO db_user;  
GRANT SELECT ON ALL_OBJECTS TO db_user;  
GRANT SELECT ON ALL_TABLES TO db_user;  
GRANT SELECT ON ALL_USERS TO db_user;  
GRANT SELECT ON ALL_CATALOG TO db_user;  
GRANT SELECT ON ALL_CONSTRAINTS TO db_user;  
GRANT SELECT ON ALL_CONS_COLUMNS TO db_user;  
GRANT SELECT ON ALL_TAB_COLS TO db_user;  
GRANT SELECT ON ALL_IND_COLUMNS TO db_user;  
GRANT SELECT ON ALL_ENCRYPTED_COLUMNS TO db_user;  
GRANT SELECT ON ALL_LOG_GROUPS TO db_user;  
GRANT SELECT ON ALL_TAB_PARTITIONS TO db_user;  
GRANT SELECT ON SYS.DBA_REGISTRY TO db_user;  
GRANT SELECT ON SYS.OBJ$ TO db_user;  
GRANT SELECT ON DBA_TABLESPACES TO db_user;
```



```
GRANT SELECT ON DBA_OBJECTS TO db_user; -- Required if the Oracle version is earlier than 11.2.0.3.  
GRANT SELECT ON SYS.ENC$ TO db_user; -- Required if transparent data encryption (TDE) is enabled. For more information on using Oracle TDE with AWS DMS, see Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS.  
GRANT SELECT ON GV_$TRANSACTION TO db_user; -- Required if the source database is Oracle RAC in AWS DMS versions 3.4.6 and higher.  
GRANT SELECT ON V_$DATAGUARD_STATS TO db_user; -- Required if the source database is Oracle Data Guard and Oracle Standby is used in the latest release of DMS version 3.4.6, version 3.4.7, and higher.
```

Concedi il seguente privilegio aggiuntivo per ogni tabella replicata quando utilizzi un elenco di tabelle specifico.

```
GRANT SELECT on any-replicated-table to db_user;
```

Concedi il seguente privilegio aggiuntivo per convalidare le colonne LOB con la funzionalità di convalida.

```
GRANT EXECUTE ON SYS.DBMS_CCRYPTO TO db_user;
```

Concedi il seguente privilegio aggiuntivo se utilizzi il lettore binario anziché. LogMiner

```
GRANT SELECT ON SYS.DBA_DIRECTORIES TO db_user;
```

Concedi il seguente privilegio aggiuntivo per esporre le viste.

```
GRANT SELECT on ALL_VIEWS to dms_user;
```

Per esporre le viste, devi anche aggiungere l'attributo aggiuntivo di connessione `exposeViews=true` all'endpoint di origine.

Concedi il seguente privilegio aggiuntivo quando utilizzi le repliche serverless.

```
GRANT SELECT on dba_segments to db_user;
```

Per informazioni sulle repliche serverless, consulta [Lavorare con AWS DMS Serverless](#).

Concedi i seguenti privilegi aggiuntivi quando utilizzi le valutazioni di premigrazione specifiche di Oracle.

```
GRANT SELECT on gv_$parameter to dms_user;  
GRANT SELECT on v_$instance to dms_user;  
GRANT SELECT on v_$version to dms_user;  
GRANT SELECT on gv_$ASM_DISKGROUP to dms_user;  
GRANT SELECT on gv_$database to dms_user;  
GRANT SELECT on dba_db_links to dms_user;  
GRANT SELECT on gv_$log_History to dms_user;  
GRANT SELECT on gv_$log to dms_user;  
GRANT SELECT ON DBA_TYPES TO db_user;  
GRANT SELECT ON DBA_USERS to dms_user;  
GRANT SELECT ON DBA_DIRECTORIES to dms_user;
```

Per informazioni sulle valutazioni di premigrazione specifiche di Oracle, consulta [Valutazioni Oracle](#).

Prerequisiti per la gestione delle transazioni aperte per Oracle Standby

Quando si utilizzano AWS DMS le versioni 3.4.6 e successive, effettuare le seguenti operazioni per gestire le transazioni aperte per Oracle Standby.

1. Crea un collegamento di database denominato AWSDMS_DBLINK nel database primario. *DMS_USER* utilizzerà il collegamento per connettersi al database primario. Tieni presente che il collegamento di database viene eseguito dall'istanza di standby per eseguire query sulle transazioni aperte in esecuzione nel database primario. Guarda l'esempio seguente.

```
CREATE PUBLIC DATABASE LINK AWSDMS_DBLINK  
CONNECT TO DMS_USER IDENTIFIED BY DMS_USER_PASSWORD  
USING '(DESCRIPTION=  
    (ADDRESS=(PROTOCOL=TCP)(HOST=PRIMARY_HOST_NAME_OR_IP)(PORT=PORT))  
    (CONNECT_DATA=(SERVICE_NAME=SID))  
    )';
```

2. Verifica che sia stata stabilita la connessione al collegamento di database usando *DMS_USER*, come illustrato nell'esempio seguente.

```
select 1 from dual@AWSDMS_DBLINK
```

Preparazione di un database di origine Oracle autogestito per CDC utilizzando AWS DMS

Prepara il database Oracle autogestito come origine per eseguire un'attività di CDC effettuando le seguenti operazioni:

- [Verifica che AWS DMS supporti la versione del database di origine.](#)
- [Verifica che la modalità ARCHIVELOG sia attiva.](#)
- [Impostazione del log supplementare.](#)

Verifica che AWS DMS supporti la versione del database di origine

Esegui una query come la seguente per verificare che la versione corrente del database di origine Oracle sia supportata da AWS DMS.

```
SELECT name, value, description FROM v$parameter WHERE name = 'compatible';
```

Qui, `name`, `value` e `description` sono colonne presenti da qualche parte nel database che vengono interrogate in base al valore di `name`. Se questa query viene eseguita senza errori, AWS DMS supporta la versione corrente del database ed è possibile continuare con la migrazione. Se la query genera un errore, AWS DMS significa che non supporta la versione corrente del database. Per procedere con la migrazione, converti innanzitutto il database Oracle in una versione supportata da AWS DMS.

Verifica che la modalità ARCHIVELOG sia attiva

Puoi eseguire Oracle in due diverse modalità: la modalità ARCHIVELOG e la modalità NOARCHIVELOG. Per eseguire un'attività di CDC, esegui il database in modalità ARCHIVELOG. Per sapere se il database è in modalità ARCHIVELOG, esegui la seguente query.

```
SQL> SELECT log_mode FROM v$database;
```

Se viene restituita la modalità NOARCHIVELOG, imposta il database su ARCHIVELOG in base alle istruzioni di Oracle.

Impostazione del log supplementare

Per acquisire le modifiche in corso, è AWS DMS necessario abilitare una registrazione supplementare minima sul database di origine Oracle. Inoltre, è necessario abilitare il log supplementare per ogni tabella replicata nel database.

Per impostazione predefinita, AWS DMS aggiunge una registrazione PRIMARY KEY supplementare su tutte le tabelle replicate. AWS DMS Per consentire l'aggiunta di log PRIMARY KEY supplementari, concedi il seguente privilegio per ogni tabella replicata.

```
ALTER on any-replicated-table;
```

È possibile disabilitare la registrazione PRIMARY KEY supplementare predefinita aggiunta utilizzando AWS DMS l'attributo extra connection. `addSupplementalLogging` Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

Assicurati di attivare il log supplementare se l'attività di replica aggiorna una tabella utilizzando una clausola WHERE che non fa riferimento a una colonna di chiave primaria.

Per impostare manualmente il log supplementare

1. Esegui la seguente query per verificare che il log supplementare sia abilitato sul database.

```
SELECT supplemental_log_data_min FROM v$database;
```

Se il risultato restituito è YES o IMPLICIT, il log supplementare è abilitato sul database.

In caso contrario, abilita il log supplementare sul database eseguendo il seguente comando.

```
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA;
```

2. Assicurati che venga aggiunto il log supplementare richiesto per ogni tabella replicata.

Considera i seguenti aspetti:

- Se alla tabella viene aggiunto il log supplementare ALL COLUMNS, non è necessario aggiungere altri log.
- Se esiste una chiave primaria, aggiungi il log supplementare per la chiave primaria. Puoi eseguire questa operazione utilizzando il formato per aggiungere il log supplementare sulla

chiave primaria oppure aggiungendo il log supplementare sulle colonne della chiave primaria nel database.

```
ALTER TABLE TableName ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;  
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA (PRIMARY KEY) COLUMNS;
```

- Se non esiste una chiave primaria e la tabella dispone di un unico indice univoco, aggiungi tutte le colonne dell'indice univoco ai log supplementari.

```
ALTER TABLE TableName ADD SUPPLEMENTAL LOG GROUP LogGroupName  
(UniqueIndexColumn1 [, UniqueIndexColumn2] ...) ALWAYS;
```

L'utilizzo di SUPPLEMENTAL LOG DATA (UNIQUE INDEX) COLUMNS non aggiunge le colonne dell'indice univoco ai log.

- Se non esiste una chiave primaria e la tabella ha più indici univoci, AWS DMS seleziona il primo indice univoco in un elenco crescente in ordine alfabetico. È necessario aggiungere un log supplementare sulle colonne dell'indice selezionato come nell'elemento precedente.

L'utilizzo di SUPPLEMENTAL LOG DATA (UNIQUE INDEX) COLUMNS non aggiunge le colonne dell'indice univoco ai log.

- Se non esiste una chiave primaria e non esiste un indice univoco, aggiungere il log supplementare su tutte le colonne.

```
ALTER TABLE TableName ADD SUPPLEMENTAL LOG DATA (ALL) COLUMNS;
```

In alcuni casi, la chiave primaria o l'indice univoco della tabella di destinazione sono diversi da quelli della tabella di origine. In questi casi, aggiungi il log supplementare sulle colonne della tabella di origine che compongono la chiave primaria o l'indice univoco.

Se modifichi la chiave primaria della tabella di destinazione, è necessario aggiungere il log supplementare sulle colonne dell'indice selezionato invece che sulle colonne della chiave primaria o dell'indice univoco originali.

Se per una tabella sono definiti un filtro o una trasformazione, potrebbe essere necessario abilitare un logging aggiuntivo.

Considera i seguenti aspetti:

- Se alla tabella viene aggiunto il log supplementare ALL COLUMNS, non è necessario aggiungere altri log.
- Se una tabella dispone di un indice univoco o una chiave primaria, aggiungi un log supplementare a ciascuna colonna interessata da un filtro o da una trasformazione. Esegui questa operazione solo se le colonne sono diverse dalle colonne della chiave primaria o dell'indice univoco.
- Se una trasformazione include solo una colonna, non aggiungere questa colonna a un gruppo di log supplementare. Ad esempio, per una trasformazione A+B, aggiungi il log supplementare su entrambe le colonne A e B. Tuttavia, per una trasformazione `substring(A, 10)` non aggiungere il log supplementare alla colonna A.
- Per impostare il log supplementare sulle colonne della chiave primaria o dell'indice univoco e su altre colonne che vengono filtrate o trasformate, puoi impostare il log supplementare USER_LOG_GROUP. Aggiungi questo log sulle colonne della chiave primaria o dell'indice univoco e su altre colonne specifiche che vengono filtrate o trasformate.

Ad esempio, per replicare una tabella denominata TEST.LOGGING con chiave primaria ID e un filtro in base alla colonna NAME, puoi eseguire un comando simile a quello seguente per creare il log supplementare del gruppo di log.

```
ALTER TABLE TEST.LOGGING ADD SUPPLEMENTAL LOG GROUP TEST_LOG_GROUP (ID, NAME) ALWAYS;
```

I privilegi dell'account sono richiesti quando si utilizza Oracle per accedere ai redo log LogMiner

Per accedere ai redo log utilizzando Oracle LogMiner, concedi i seguenti privilegi all'utente Oracle specificato nelle impostazioni di connessione dell'endpoint Oracle.

```
GRANT EXECUTE on DBMS_LOGMNR to db_user;  
GRANT SELECT on V_$LOGMNR_LOGS to db_user;  
GRANT SELECT on V_$LOGMNR_CONTENTS to db_user;  
GRANT LOGMINING to db_user; -- Required only if the Oracle version is 12c or higher.
```

I privilegi dell'account sono necessari quando si utilizza AWS DMS Binary Reader per accedere ai redo log

Per accedere ai redo log utilizzando AWS DMS Binary Reader, concedi i seguenti privilegi all'utente Oracle specificato nelle impostazioni di connessione dell'endpoint Oracle.

```
GRANT SELECT on v_$transportable_platform to db_user; -- Grant this privilege if the
redo logs are stored in Oracle Automatic Storage Management (ASM) and AWS DMS accesses
them from ASM.
GRANT CREATE ANY DIRECTORY to db_user; -- Grant this privilege to
allow AWS DMS to use Oracle BFILE read file access in certain cases. This access is
required when the replication instance doesn't have file-level access to the redo logs
and the redo logs are on non-ASM storage.
GRANT EXECUTE on DBMS_FILE_TRANSFER to db_user; -- Grant this privilege to copy
the redo log files to a temporary folder using the CopyToTempFolder method.
GRANT EXECUTE on DBMS_FILE_GROUP to db_user;
```

Binary Reader utilizza le funzionalità di gestione file di Oracle che includono le directory Oracle. Ogni oggetto directory Oracle include il nome della cartella contenente i redo log da elaborare. Queste directory Oracle non sono rappresentate a livello di file system. Sono invece directory logiche che vengono create a livello di database Oracle. È possibile visualizzarle nella vista Oracle `ALL_DIRECTORIES`.

Se desideri AWS DMS creare queste directory Oracle, concedi il privilegio specificato in precedenza. `CREATE ANY DIRECTORY` AWS DMS crea i nomi delle directory con il prefisso `DMS_`. Se non concedi il privilegio `CREATE ANY DIRECTORY`, crea manualmente le directory corrispondenti. In alcuni casi, quando si creano manualmente le directory Oracle, l'utente Oracle specificato nell'endpoint di origine Oracle non è l'utente che ha creato tali directory. In questi casi, concedi anche il privilegio `READ` on `DIRECTORY`.

Se l'endpoint di origine Oracle è in modalità Active Dataguard Standby (ADG), consulta il post [How to use Binary Reader with ADG](#) sul Database Blog. AWS

Note

AWS DMS CDC non supporta Active Dataguard Standby che non è configurato per utilizzare il servizio di trasporto di ripristino automatico.

In alcuni casi i log potrebbero essere stati archiviati con Oracle Managed Files (OMF). In alternativa l'endpoint di origine è in modalità ADG e il privilegio `CREATE ANY DIRECTORY` non può essere concesso. In questi casi, crea manualmente le directory con tutte le possibili posizioni di registro prima di iniziare l'attività di replica. AWS DMS Se AWS DMS non trova una delle directory precedentemente create che si aspetta, l'attività si interrompe. Inoltre, AWS DMS non elimina le voci che ha creato nella `ALL_DIRECTORIES` vista, quindi devi eliminarle manualmente.

Privilegi dell'account aggiuntivi necessari quando si utilizza Binary Reader con Oracle ASM

Per accedere ai log redo in Automatic Storage Management (ASM) utilizzando Binary Reader, concedi i seguenti privilegi all'utente Oracle specificato nelle impostazioni di connessione dell'endpoint Oracle.

```
SELECT ON v_$transportable_platform
SYSASM -- To access the ASM account with Oracle 11g Release 2 (version 11.2.0.2) and
higher, grant the Oracle endpoint user the SYSASM privilege. For older supported
Oracle versions, it's typically sufficient to grant the Oracle endpoint user the
SYSDBA privilege.
```

È possibile verificare l'accesso all'account ASM aprendo un prompt dei comandi e richiamando una delle istruzioni seguenti, a seconda della versione di Oracle come specificato in precedenza.

Se è necessario il privilegio SYSDBA, utilizza quanto segue.

```
sqlplus asmuser/asmpassword@+asmserver as sysdba
```

Se è necessario il privilegio SYSASM, utilizza quanto segue.

```
sqlplus asmuser/asmpassword@+asmserver as sysasm
```

Utilizzo di Oracle Standby autogestito come origine con Binary Reader per l'attività di CDC in AWS DMS

Per configurare un'istanza Oracle Standby come origine quando si utilizza Binary Reader per l'attività di CDC, è necessario soddisfare i seguenti prerequisiti iniziali:

- AWS DMS attualmente supporta solo Oracle Active Data Guard Standby.
- Assicurati che la configurazione di Oracle Data Guard utilizzi:
 - Servizi di trasporto per la riesecuzione per trasferimenti automatici di dati di redo.
 - Servizi per applicare automaticamente la riesecuzione al database in standby.

Per verificare che tali requisiti siano soddisfatti, esegui la seguente query.

```
SQL> select open_mode, database_role from v$database;
```


Dall'output della query, verifica che il database in standby sia aperto in modalità READ ONLY e che la riesecuzione venga applicata automaticamente. Per esempio:

```
OPEN_MODE          DATABASE_ROLE
-----
READ ONLY WITH APPLY  PHYSICAL STANDBY
```

Per configurare un'istanza Oracle Standby come origine quando si utilizza Binary Reader per l'attività di CDC

1. Concedi i privilegi aggiuntivi necessari per accedere ai file di log in standby.

```
GRANT SELECT ON v_$standby_log TO db_user;
```

2. Crea un endpoint di origine per Oracle Standby utilizzando AWS Management Console o AWS CLI. Al momento della creazione dell'endpoint, specifica i seguenti attributi aggiuntivi di connessione.

```
useLogminerReader=N;useBfile=Y;
```

Note

In AWS DMS, è possibile utilizzare attributi di connessione aggiuntivi per specificare se si desidera migrare dai log di archivio anziché dai redo log. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

3. Configura la destinazione dei log archiviati.

DMS Binary Reader per l'origine Oracle senza ASM utilizza le directory Oracle per accedere ai log redo archiviati. Se il database è configurato per utilizzare la Fast Recovery Area (FRA) come destinazione dei log di archiviazione, la posizione dei file di archivio di riesecuzione non è costante. Ogni giorno in cui vengono generati i log redo archiviati, viene creata una nuova directory nella FRA, utilizzando il formato del nome di directory AAAA_MM_GG. Per esempio:

```
DB_RECOVERY_FILE_DEST/SID/archivelog/YYYY_MM_DD
```

Quando DMS deve accedere ai redo file archiviati nella directory FRA appena creata e il database primario di lettura/scrittura viene utilizzato come origine, DMS crea una nuova directory Oracle o sostituisce una directory Oracle esistente, come segue.

```
CREATE OR REPLACE DIRECTORY dmsrep_taskid AS 'DB_RECOVERY_FILE_DEST/SID/archivelog/YYYY_MM_DD';
```

Quando il database in standby viene utilizzato come origine, DMS non è in grado di creare o sostituire la directory Oracle perché il database è in modalità di sola lettura. Tuttavia, è possibile scegliere di eseguire una di queste fasi aggiuntive:

- a. Modifica `log_archive_dest_id_1` per utilizzare un percorso effettivo anziché l'area FRA in una configurazione tale che Oracle non crei giornalmente sottodirectory:

```
ALTER SYSTEM SET log_archive_dest_1='LOCATION=full directory path'
```

Quindi, crea un oggetto directory Oracle da utilizzare con DMS:

```
CREATE OR REPLACE DIRECTORY dms_archived_logs AS 'full directory path';
```

- b. Crea una destinazione aggiuntiva per il log di archiviazione e un oggetto directory Oracle che punti a tale destinazione. Per esempio:

```
ALTER SYSTEM SET log_archive_dest_3='LOCATION=full directory path';  
CREATE DIRECTORY dms_archived_log AS 'full directory path';
```

Quindi aggiungi un attributo aggiuntivo di connessione all'endpoint di origine dell'attività:

```
archivedLogDestId=3
```

- c. Crea manualmente in anticipo gli oggetti directory Oracle da utilizzare con DMS.

```
CREATE DIRECTORY dms_archived_log_20210301 AS 'DB_RECOVERY_FILE_DEST/SID/archivelog/2021_03_01';  
CREATE DIRECTORY dms_archived_log_20210302 AS 'DB_RECOVERY_FILE_DEST>/SID>/archivelog/2021_03_02';  
...
```

- d. Crea un processo di pianificazione Oracle che venga eseguito quotidianamente e crei la directory richiesta.

Utilizzo di un database gestito dall'utente su Oracle Cloud Infrastructure (OCI) come origine per l'attività di CDC in AWS DMS

Un database gestito dall'utente è quello che puoi configurare e controllare, ad esempio un database Oracle creato su una macchina virtuale (VM), un bare metal o un server Exadata. In alternativa, è il database che puoi configurare e controllare che viene eseguito su un'infrastruttura dedicata, come Oracle Cloud Infrastructure (OCI). Le seguenti informazioni descrivono i privilegi e le configurazioni necessari quando si utilizza un database Oracle gestito dall'utente su OCI come origine per l'acquisizione dei dati di modifica (CDC) in AWS DMS.

Per configurare un database Oracle gestito dall'utente ospitato da OCI come origine per l'acquisizione dei dati di modifica

1. Concedi i privilegi dell'account utente necessari per un database di origine Oracle gestito dall'utente su OCI. Per ulteriori informazioni, consulta [Privilegi dell'account per un endpoint di origine Oracle autogestito](#).
2. Concedi i privilegi dell'account necessari quando utilizzi Binary Reader per accedere ai log redo. Per ulteriori informazioni, consulta [Account privileges required when using Binary Reader](#).
3. Aggiungi i privilegi dell'account necessari quando utilizzi Binary Reader con Oracle Automatic Storage Management (ASM). Per ulteriori informazioni, consulta [Additional account privileges required when using Binary Reader with Oracle ASM](#).
4. Imposta il log supplementare. Per ulteriori informazioni, consulta [Setting up supplemental logging](#).
5. Configura la crittografia TDE. Per ulteriori informazioni, consulta [Encryption methods when using an Oracle database as a source endpoint](#).

Le seguenti limitazioni si applicano alla replica dei dati di un database di origine Oracle su Oracle Cloud Infrastructure (OCI).

Limitazioni

- DMS non supporta l'utilizzo di Oracle per accedere LogMiner ai redo log.
- DMS non supporta Autonomous DB.

Utilizzo di un database Oracle AWS gestito come fonte per AWS DMS

Un database AWS gestito è un database che si trova su un servizio Amazon come Amazon RDS, Amazon Aurora o Amazon S3. Di seguito, puoi trovare i privilegi e le configurazioni che devi configurare quando utilizzi un database Oracle gestito con. AWS AWS DMS

Privilegi di account utente richiesti su una fonte Oracle gestita per AWSAWS DMS

Concedi i seguenti privilegi all'account utente Oracle specificato nella definizione dell'endpoint di origine Oracle.

Important

Per tutti i valori dei parametri, ad esempio *db_user* e *any-replicated-table*, Oracle presuppone che il valore sia tutto in maiuscolo a meno che non si specifichi il valore con un identificatore con distinzione tra maiuscole e minuscole. Ad esempio, supponiamo di creare un valore *db_user* senza utilizzare le virgolette, come in `CREATE USER myuser` o `CREATE USER MYUSER`. In questo caso, Oracle identifica e memorizza il valore come tutto maiuscolo (MYUSER). Se si utilizzano le virgolette, come in `CREATE USER "MyUser"` o `CREATE USER 'MyUser'`, Oracle identifica e memorizza il valore con distinzione tra maiuscole e minuscole specificato (MyUser).

```
GRANT CREATE SESSION to db_user;
GRANT SELECT ANY TRANSACTION to db_user;
GRANT SELECT on DBA_TABLESPACES to db_user;
GRANT SELECT ON any-replicated-table to db_user;
GRANT EXECUTE on rdsadmin.rdsadmin_util to db_user;
-- For Oracle 12c or higher:
GRANT LOGMINING to db_user; - Required only if the Oracle version is 12c or higher.
```

Inoltre, concedi le autorizzazioni `SELECT` e `EXECUTE` sugli oggetti `SYS` utilizzando la procedura Amazon RDS `rdsadmin.rdsadmin_util.grant_sys_object`, come illustrato. Per ulteriori informazioni, consulta [Concessione di privilegi `SELECT` o `EXECUTE` su oggetti `SYS`](#).

```
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_VIEWS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_TAB_PARTITIONS', 'db_user',
'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_INDEXES', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_OBJECTS', 'db_user', 'SELECT');
```

```
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_TABLES', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_USERS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_CATALOG', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_CONSTRAINTS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_CONS_COLUMNS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_TAB_COLS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_IND_COLUMNS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_LOG_GROUPS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$ARCHIVED_LOG', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$LOG', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$LOGFILE', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$DATABASE', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$THREAD', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$PARAMETER', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$NLS_PARAMETERS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$TIMEZONE_NAMES', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$TRANSACTION', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$CONTAINERS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_REGISTRY', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('OBJ$', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('ALL_ENCRYPTED_COLUMNS', 'db_user',
'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$LOGMNR_LOGS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$LOGMNR_CONTENTS', 'db_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_LOGMNR', 'db_user', 'EXECUTE');

-- (as of Oracle versions 12.1 and higher)
exec rdsadmin.rdsadmin_util.grant_sys_object('REGISTRY$SQLPATCH', 'db_user', 'SELECT');

-- (for Amazon RDS Active Dataguard Standby (ADG))
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$STANDBY_LOG', 'db_user', 'SELECT');

-- (for transparent data encryption (TDE))

exec rdsadmin.rdsadmin_util.grant_sys_object('ENC$', 'db_user', 'SELECT');

-- (for validation with LOB columns)
exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_CCRYPTO', 'db_user', 'EXECUTE');

-- (for binary reader)
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_DIRECTORIES', 'db_user', 'SELECT');

-- Required when the source database is Oracle Data guard, and Oracle Standby is used
in the latest release of DMS version 3.4.6, version 3.4.7, and higher.
```

```
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$DATAGUARD_STATS', 'db_user',  
'SELECT');
```

Per ulteriori informazioni sull'uso di Amazon RDS Active Dataguard Standby (ADG) con AWS DMS , consulta [Utilizzo di Amazon RDS Oracle Standby \(replica di lettura\) come origine con Binary Reader per l'attività di CDC in AWS DMS](#).

Per ulteriori informazioni sull'utilizzo di Oracle TDE con AWS DMS, vedere. [Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS](#)

Prerequisiti per la gestione delle transazioni aperte per Oracle Standby

Se si utilizzano AWS DMS le versioni 3.4.6 e successive, effettuare le seguenti operazioni per gestire le transazioni aperte per Oracle Standby.

1. Crea un collegamento di database denominato AWSDMS_DBLINK nel database primario. **DMS_USER** utilizzerà il collegamento per connettersi al database primario. Tieni presente che il collegamento di database viene eseguito dall'istanza di standby per eseguire query sulle transazioni aperte in esecuzione nel database primario. Guarda l'esempio seguente.

```
CREATE PUBLIC DATABASE LINK AWSDMS_DBLINK  
CONNECT TO DMS_USER IDENTIFIED BY DMS_USER_PASSWORD  
USING '(DESCRIPTION=  
    (ADDRESS=(PROTOCOL=TCP)(HOST=PRIMARY_HOST_NAME_OR_IP)(PORT=PORT))  
    (CONNECT_DATA=(SERVICE_NAME=SID))  
)';
```

2. Verifica che sia stata stabilita la connessione al collegamento di database usando **DMS_USER**, come illustrato nell'esempio seguente.

```
select 1 from dual@AWSDMS_DBLINK
```

Configurazione di una fonte Oracle gestita per AWSAWS DMS

Prima di utilizzare un database Oracle AWS gestito come origine per AWS DMS, esegui le seguenti attività per il database Oracle:

- Abilita backup automatici. Per ulteriori informazioni sull'abilitazione dei backup automatici, consulta [Abilitazione dei backup automatici](#) nella Guida per l'utente di Amazon RDS.
- Imposta il log supplementare.
- Imposta l'archiviazione. L'archiviazione dei redo log per l'istanza DB di Amazon RDS for Oracle AWS DMS consente di recuperare le informazioni di registro utilizzando Oracle o Binary Reader. LogMiner

Per impostare l'archiviazione

1. Per impostare l'archiviazione eseguire il comando `rdsadmin.rdsadmin_util.set_configuration`.

Ad esempio, per mantenere i log redo archiviati per 24 ore, esegui il seguente comando.

```
exec rdsadmin.rdsadmin_util.set_configuration('archivelog retention hours',24);
commit;
```

Note

Il commit è necessario per rendere effettiva la modifica.

2. Assicurati che lo spazio di storage sia sufficiente per i log redo archiviati durante il periodo di conservazione specificato. Ad esempio, se il periodo di conservazione è 24 ore, calcola la dimensione totale dei log redo archiviati accumulati in un'ora di elaborazione tipica delle transazioni e moltiplica il totale per 24. Confronta il totale calcolato su 24 ore con lo spazio di storage disponibile e decidi se disponi di spazio di storage sufficiente per gestire un'intera elaborazione delle transazioni di 24 ore.

Per impostare il log supplementare

1. Per abilitare il log supplementare a livello di database, esegui il comando riportato di seguito.

```
exec rdsadmin.rdsadmin_util.alter_supplemental_logging('ADD');
```

2. Esegui il comando riportato di seguito per abilitare il log supplementare della chiave primaria.

```
exec rdsadmin.rdsadmin_util.alter_supplemental_logging('ADD','PRIMARY KEY');
```

3. (Facoltativo) Abilita il log supplementare della chiave a livello di tabella.

Nel database di origine si verificherà un leggero sovraccarico quando il log supplementare della chiave è abilitato. Pertanto, se esegui solo la migrazione di un sottoinsieme di tabelle, puoi abilitare il log supplementare della chiave a livello di tabella. Per abilitare il log supplementare della chiave a livello di tabella, esegui il comando riportato di seguito.

```
alter table table_name add supplemental log data (PRIMARY KEY) columns;
```

Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS

Puoi configurare l'accesso AWS DMS ai redo log di origine delle istanze Amazon RDS for Oracle utilizzando Binary Reader for CDC.

Note

Per utilizzare Oracle LogMiner, sono sufficienti i privilegi minimi richiesti per l'account utente. Per ulteriori informazioni, consulta [Privilegi di account utente richiesti su una fonte Oracle gestita per AWSAWS DMS](#).

Per utilizzare AWS DMS Binary Reader, specifica impostazioni aggiuntive e attributi di connessione aggiuntivi per l'endpoint di origine Oracle, a seconda della versione in uso. AWS DMS

Il supporto Binary Reader è disponibile nelle seguenti versioni di Amazon RDS per Oracle:

- Oracle 11.2, versione 11.2.0.4V11 e successive
- Oracle 12.1, versione 12.1.0.2.V7 e successive
- Oracle 12.2, tutte le versioni
- Oracle 18.0, tutte le versioni
- Oracle 19.0, tutte le versioni

Per configurare CDC utilizzando Binary Reader

1. Accedi al database di origine Amazon RDS per Oracle come utente master ed esegui le seguenti stored procedure per creare le directory a livello di server.


```
exec rdsadmin.rdsadmin_master_util.create_archivelog_dir;  
exec rdsadmin.rdsadmin_master_util.create_onlinelog_dir;
```

2. Concedi i seguenti privilegi all'account utente Oracle che viene utilizzato per accedere all'endpoint di origine Oracle.

```
GRANT READ ON DIRECTORY ONLINELOG_DIR TO db_user;  
GRANT READ ON DIRECTORY ARCHIVELOG_DIR TO db_user;
```

3. Imposta i seguenti attributi aggiuntivi di connessione sull'endpoint di origine Amazon RDS per Oracle.

- Per RDS per Oracle versioni 11.2 e 12.1, imposta quanto segue.

```
useLogminerReader=N;useBfile=Y;accessAlternateDirectly=false;useAlternateFolderForOnline=  
oraclePathPrefix=/rdsdbdata/db/[$DATABASE_NAME]_A/;usePathPrefix=/rdsdbdata/  
log/;replacePathPrefix=true;
```

- Per RDS per Oracle versioni 12.2, 18.0 e 19.0, imposta quanto segue.

```
useLogminerReader=N;useBfile=Y;
```

Note

Assicurati che non ci siano spazi bianchi dopo il separatore punto e virgola (;) per più impostazioni di attributi, ad esempio `oneSetting; thenAnother`.

Per ulteriori informazioni sulla configurazione di un'attività di CDC, consulta [Configurazione dell'attività di CDC su un database di origine Oracle](#).

Utilizzo di Amazon RDS Oracle Standby (replica di lettura) come origine con Binary Reader per l'attività di CDC in AWS DMS

Verifica i seguenti prerequisiti per l'utilizzo di Amazon RDS per Oracle Standby come origine quando usi Binary Reader per l'attività di CDC in AWS DMS:

- Utilizza l'utente master Oracle per configurare Binary Reader.
- Assicurati che AWS DMS attualmente supporti solo l'utilizzo di Oracle Active Data Guard Standby.

Una volta fatto, usa la procedura seguente per utilizzare RDS per Oracle Standby come origine con Binary Reader per l'attività di CDC.

Per configurare un'istanza RDS per Oracle Standby come origine quando si utilizza Binary Reader per l'attività di CDC

1. Accedi all'istanza primaria RDS per Oracle come utente master.
2. Esegui le seguenti stored procedure come documentato nella Guida per l'utente di Amazon RDS per creare le directory a livello di server.

```
exec rdsadmin.rdsadmin_master_util.create_archivelog_dir;
exec rdsadmin.rdsadmin_master_util.create_onlinelog_dir;
```

3. Identifica le directory create nella fase 2.

```
SELECT directory_name, directory_path FROM all_directories
WHERE directory_name LIKE ( 'ARCHIVELOG_DIR_%' )
      OR directory_name LIKE ( 'ONLINELOG_DIR_%' )
```

Ad esempio, il codice precedente visualizza un elenco di directory come il seguente.

DIRECTORY_NAME	DIRECTORY_PATH
ARCHIVELOG_DIR_A	/rdsdbdata/db/ORCL_A/arch
ARCHIVELOG_DIR_B	/rdsdbdata/db/ORCL_B/arch
ONLINELOG_DIR_A	/rdsdbdata/db/ORCL_A/onlinelog
ONLINELOG_DIR_B	/rdsdbdata/db/ORCL_B/onlinelog

4. Concedi il privilegio Read sulle directory precedenti all'account utente Oracle utilizzato per accedere a Oracle Standby.

```
GRANT READ ON DIRECTORY ARCHIVELOG_DIR_A TO db_user;
GRANT READ ON DIRECTORY ARCHIVELOG_DIR_B TO db_user;
GRANT READ ON DIRECTORY ONLINELOG_DIR_A TO db_user;
GRANT READ ON DIRECTORY ONLINELOG_DIR_B TO db_user;
```

5. Applica un'opzione del log di archiviazione all'istanza principale. In questo modo le modifiche a ALL_DIRECTORIES vengono trasferite anche in Oracle Standby.

6. Esegui una query `ALL_DIRECTORIES` su Oracle Standby per verificare che le modifiche siano state applicate.
7. Crea un endpoint di origine per Oracle Standby utilizzando la AWS DMS Management Console o AWS Command Line Interface ().AWS CLI Al momento della creazione dell'endpoint, specifica i seguenti attributi aggiuntivi di connessione.

```
useLogminerReader=N;useBfile=Y;archivedLogDestId=1;additionalArchivedLogDestId=2
```

8. Dopo aver creato l'endpoint, utilizzare Test endpoint connection nella pagina Crea endpoint della console o il AWS CLI `test-connection` comando per verificare che la connettività sia stabilita.

Limitazioni all'uso di Oracle come fonte per AWS DMS

Quando si utilizza un database Oracle come origine per AWS DMS, si applicano le seguenti limitazioni:

- AWS DMS supporta i tipi di dati Oracle Extended nella AWS DMS versione 3.5.0 e successive.
- AWS DMS non supporta nomi di oggetti lunghi (oltre 30 byte).
- AWS DMS non supporta indici basati su funzioni.
- Se gestisci il log supplementare ed esegui trasformazioni su una qualsiasi delle colonne, assicurati che il log supplementare sia attivato per tutti i campi e le colonne. Per ulteriori informazioni sull'impostazione del log supplementare, consulta i seguenti argomenti:
 - Per un database di origine Oracle autogestito, consulta [Impostazione del log supplementare](#).
 - Per un database di origine Oracle AWS gestito, vedere. [Configurazione di una fonte Oracle gestita per AWSAWS DMS](#)
- AWS DMS non supporta il database radice dei contenitori multi-tenant (CDB\$ROOT). Supporta un PDB utilizzando Binary Reader.
- AWS DMS non supporta i vincoli differiti.
- Nella AWS DMS versione 3.5.1 e successive, i LOB sicuri sono supportati solo eseguendo una ricerca LOB.
- AWS DMS supporta la `rename table table-name to new-table-name` sintassi per tutte le versioni Oracle 11 e successive supportate. Questa sintassi non è supportata per i database di origine Oracle versione 10.

- AWS DMS non replica i risultati dell'istruzione DDL. ALTER TABLE ADD *column data_type* DEFAULT *default_value* Invece di replicare *default_value* sulla destinazione, imposta la nuova colonna su NULL.
- Se utilizzate la AWS DMS versione 3.4.7 o successiva, per replicare le modifiche derivanti da operazioni di partizione o sottopartizione, effettuate le seguenti operazioni prima di avviare un'attività DMS.
 - Crea manualmente la struttura della tabella partizionata (DDL).
 - Assicurati che il DDL sia lo stesso per l'origine e la destinazione Oracle.
 - Imposta l'attributo aggiuntivo di connessione enableHomogenousPartitionOps=true.

Per ulteriori informazioni su enableHomogenousPartitionOps, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#). Inoltre, tieni presente che per il pieno carico e attività di CDC, DMS non replica le modifiche ai dati acquisite come parte delle modifiche memorizzate nella cache. In questo caso d'uso, ricrea la struttura della tabella sulla destinazione Oracle e ricarica le tabelle in questione.

Prima della AWS DMS versione 3.4.7:

DMS non replica le modifiche dei dati derivanti dalle operazioni di partizione o di sottopartizione (ADD, DROP, EXCHANGE e TRUNCATE). Tali aggiornamenti possono causare i seguenti errori durante la replica:

- Nel caso di operazioni ADD, aggiornamenti ed eliminazioni sui dati aggiunti potrebbero generare un avviso "0 righe interessate".
- Nel caso di operazioni DROP e TRUNCATE, nuovi inserimenti potrebbero generare errori di "duplicazione".
- Operazioni EXCHANGE potrebbero generare sia un avviso "0 righe interessate" che errori di "duplicazione".

Per replicare le modifiche derivanti da operazioni di partizione o di sottopartizione, ricaricare le tabelle in questione. Dopo aver aggiunto una nuova partizione vuota, le operazioni sulla partizione appena aggiunta vengono replicate nella destinazione come al solito.

- AWS DMS le versioni precedenti alla 3.4 non supportano le modifiche ai dati sulla destinazione derivanti dall'esecuzione dell'CREATE TABLE ASistruzione sull'origine. Tuttavia, nella destinazione viene creata la nuova tabella.
- AWS DMS non acquisisce le modifiche apportate dal DBMS_REDEFINITION pacchetto Oracle, ad esempio i metadati della tabella e il OBJECT_ID campo.

- AWS DMS mappa le colonne BLOB e CLOB vuote NULL sulla destinazione.
- Quando si acquisiscono le modifiche con Oracle 11 LogMiner, un aggiornamento su una colonna CLOB con una lunghezza di stringa superiore al 1982 viene perso e la destinazione non viene aggiornata.
- Durante l'acquisizione dei dati di modifica (CDC), AWS DMS non supporta gli aggiornamenti in batch alle colonne numeriche definite come chiave primaria.
- AWS DMS non supporta determinati UPDATE comandi. L'esempio seguente è un comando UPDATE non supportato.

```
UPDATE TEST_TABLE SET KEY=KEY+1;
```

Qui, TEST_TABLE è il nome della tabella e KEY è una colonna numerica definita come chiave primaria.

- AWS DMS non supporta la modalità LOB completa per il caricamento delle colonne LONG e LONG RAW. È invece possibile utilizzare la modalità LOB limitata per migrare questi tipi di dati in una destinazione Oracle. In modalità LOB limitata, AWS DMS tronca tutti i dati a 64 KB impostati su colonne LONG o LONG RAW più lunghe di 64 KB.
- AWS DMS non supporta la modalità LOB completa per il caricamento delle colonne XMLTYPE. È invece possibile utilizzare la modalità LOB limitata per migrare le colonne XMLTYPE in una destinazione Oracle. In modalità LOB limitata, DMS tronca tutti i dati più lunghi della variabile "Dimensione massima dei LOB" definita dall'utente. Il valore massimo consigliato per "Dimensione massima dei LOB" è 100 MB.
- AWS DMS non replica tabelle i cui nomi contengono apostrofi.
- AWS DMS supporta CDC da viste materializzate. Tuttavia DMS non supporta l'attività di CDC da nessun'altra vista.
- AWS DMS non supporta CDC per le tabelle organizzate a indice con un segmento di overflow.
- AWS DMS non supporta l'Drop Partition operazione per le tabelle partizionate per riferimento con set to. enableHomogenousPartitionOps true
- Quando si utilizza Oracle LogMiner per accedere ai redo log, AWS DMS presenta le seguenti limitazioni:
 - Solo per Oracle 12, AWS DMS non replica alcuna modifica alle colonne LOB.
 - Per tutte le versioni di Oracle, AWS DMS non replica il risultato delle UPDATE operazioni sulle colonne LOB XMLTYPE e sulle colonne LOB.
 - AWS DMS non supporta le transazioni XA in fase di replica durante l'utilizzo di Oracle. LogMiner

- Oracle LogMiner non supporta le connessioni a un database collegabile (PDB). Per connettersi a un PDB, accedere ai redo log utilizzando Binary Reader.
- Le operazioni SHRINK SPACE non sono supportate.
- Quando si utilizza Binary Reader, AWS DMS presenta le seguenti limitazioni:
 - Non supporta i cluster di tabelle.
 - Supporta solo le operazioni SHRINK SPACE a livello di tabella. Questo livello include la tabella completa, le partizioni e le sottopartizioni.
 - Non supporta le modifiche alle tabelle organizzate per indice con compressione delle chiavi.
 - Non supporta l'implementazione dei log redo online su dispositivi raw.
 - Binary Reader supporta la crittografia TDE solo per i database Oracle autogestiti perché RDS per Oracle non supporta il recupero delle password del wallet per le chiavi di crittografia TDE.
- AWS DMS non supporta connessioni a una sorgente Oracle Amazon RDS che utilizza un proxy Oracle Automatic Storage Management (ASM).
- AWS DMS non supporta colonne virtuali.
- AWS DMS non supporta il tipo di ROWID dati o le viste materializzate basate su una colonna ROWID.

AWS DMS supporta parzialmente Oracle Materialized Views. Per i caricamenti completi, DMS può eseguire la copia del pieno carico di una vista materializzata Oracle. DMS copia la vista materializzata come tabella di base nel sistema di destinazione e ignora tutte le colonne ROWID nella vista materializzata. Per la replica continua (CDC), DMS tenta di replicare le modifiche ai dati nella vista materializzata, ma i risultati potrebbero non essere ideali. In particolare, se la vista materializzata viene completamente aggiornata, DMS replica le singole eliminazioni per tutte le righe, seguite dai singoli inserimenti per tutte le righe. Si tratta di un esercizio che richiede molte risorse e potrebbe avere scarse prestazioni per le viste materializzate con un numero elevato di righe. Per una replica continua in cui le viste materializzate eseguono un aggiornamento rapido, DMS cerca di elaborare e replicare le modifiche ai dati con aggiornamento rapido. In entrambi i casi, DMS ignora qualsiasi colonna ROWID nella vista materializzata.

- AWS DMS non carica o acquisisce tabelle temporanee globali.
- Per le destinazioni S3 che utilizzano la replica, abilita il log supplementare su ogni colonna in modo che gli aggiornamenti delle righe di origine possano acquisire ogni valore di colonna. Di seguito è riportato un esempio: `alter table yourtablename add supplemental log data (all) columns;`

- Un aggiornamento per una riga con una chiave univoca composta che contiene null non può essere replicato sulla destinazione.
- AWS DMS non supporta l'uso di più chiavi di crittografia Oracle TDE sullo stesso endpoint di origine. Ogni endpoint può avere un solo attributo per il nome della chiave di crittografia TDE "securityDbEncryptionName" e una password TDE per questa chiave.
- Durante la replica da Amazon RDS for Oracle, TDE è supportato solo con tablespace crittografato e utilizzando Oracle. LogMiner
- AWS DMS non supporta più operazioni di ridenominazione di tabelle in rapida successione.
- Quando si utilizza Oracle 19.0 come sorgente, AWS DMS non supporta le seguenti funzionalità:
 - Reindirizzamento DML con protezione dei dati
 - Tabelle ibride partizionate
 - Account Oracle solo schema
- AWS DMS non supporta la migrazione di tabelle o viste di tipo BIN\$ oDR\$.
- A partire da Oracle 18.x, AWS DMS non supporta l'acquisizione dei dati di modifica (CDC) di Oracle Express Edition (Oracle Database XE).
- Al momento della migrazione dei dati da una colonna CHAR, DMS tronca gli spazi finali.
- AWS DMS non supporta la replica dai contenitori di applicazioni.
- AWS DMS non supporta l'esecuzione di Oracle Flashback Database e dei punti di ripristino, poiché queste operazioni influiscono sulla coerenza dei file Oracle Redo Log.
- La procedura INSERT di caricamento diretto con l'opzione di esecuzione parallela non è supportata nei seguenti casi:
 - Tabelle non compresse con più di 255 colonne
 - Dimensione delle righe superiore a 8K
 - Tabelle HCC Exadata
 - Database in esecuzione sulla piattaforma Big Endian
- Una tabella di origine senza chiave primaria né univoca richiede l'abilitazione del log supplementare ALL COLUMN. Crea più attività di log redo e può aumentare la latenza dell'attività di CDC di DMS.
- AWS DMS non migra i dati dalle colonne invisibili del database di origine. Per includere queste colonne nell'ambito della migrazione, utilizza l'istruzione ALTER TABLE per renderle visibili.

Supporto SSL per un endpoint Oracle

AWS DMS Gli endpoint Oracle supportano SSL V3 per le modalità e SSL. none verify-ca
Per utilizzare SSL con un endpoint Oracle, carica il wallet Oracle per l'endpoint anziché i file di certificato .pem.

Argomenti

- [Utilizzo di un certificato esistente per SSL Oracle](#)
- [Utilizzo di un certificato autofirmato per SSL Oracle](#)

Utilizzo di un certificato esistente per SSL Oracle

Per utilizzare un'installazione client Oracle esistente per creare il file wallet Oracle dal file di certificato CA, procedi come segue.

Per utilizzare un'installazione client Oracle esistente per SSL Oracle con AWS DMS

1. Impostare la variabile di sistema ORACLE_HOME sulla posizione della directory dbhome_1 eseguendo il comando seguente.

```
prompt>export ORACLE_HOME=/home/user/app/user/product/12.1.0/dbhome_1
```

2. Aggiungere \$ORACLE_HOME/lib alla variabile di sistema LD_LIBRARY_PATH.

```
prompt>export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib
```

3. Crea una directory per il wallet Oracle nel percorso \$ORACLE_HOME/ssl_wallet.

```
prompt>mkdir $ORACLE_HOME/ssl_wallet
```

4. Inserire il file .pem del certificato CA nella directory ssl_wallet. Se si utilizza Amazon RDS, è possibile scaricare il file del certificato CA root rds-ca-2015-root.pem ospitato da Amazon RDS. Per ulteriori informazioni sul download di questo file, consulta [Utilizzo di SSL/TLS per crittografare una connessione a un'istanza database](#) nella Guida per l'utente di Amazon RDS.
5. Esegui i comandi seguenti per creare il wallet Oracle.


```
prompt>orapki wallet create -wallet $ORACLE_HOME/ssl_wallet -auto_login_only
prompt>orapki wallet add -wallet $ORACLE_HOME/ssl_wallet -trusted_cert -cert
$ORACLE_HOME/ssl_wallet/ca-cert.pem -auto_login_only
```

Una volta completate le fasi precedenti, è possibile importare il file wallet con la chiamata API `ImportCertificate` specificando il parametro `certificate-wallet`. È quindi possibile utilizzare il certificato wallet importato quando si seleziona `verify-ca` come modalità SSL durante la creazione o la modifica dell'endpoint Oracle.

Note

I portafogli Oracle sono file binari. AWS DMS accetta questi file così come sono.

Utilizzo di un certificato autofirmato per SSL Oracle

Per utilizzare un certificato autofirmato per Oracle SSL, procedi nel seguente modo, presupponendo che la password del wallet Oracle sia `oracle123`.

Per utilizzare un certificato autofirmato per Oracle SSL con AWS DMS

1. Creare una directory da utilizzare con il certificato autofirmato.

```
mkdir -p /u01/app/oracle/self_signed_cert
```

2. Passare alla directory creata nella fase precedente.

```
cd /u01/app/oracle/self_signed_cert
```

3. Creare una chiave root.

```
openssl genrsa -out self-rootCA.key 2048
```

4. Autofirmare un certificato root utilizzando la chiave root creata nel passaggio precedente.

```
openssl req -x509 -new -nodes -key self-rootCA.key
-sha256 -days 3650 -out self-rootCA.pem
```

Utilizza i parametri di input, come i seguenti.

- Country Name (2 letter code) [XX], ad esempio: AU
- State or Province Name (full name) [], ad esempio: NSW
- Locality Name (e.g., city) [Default City], ad esempio: Sydney
- Organization Name (e.g., company) [Default Company Ltd], ad esempio: AmazonWebService
- Organizational Unit Name (e.g., section) [], ad esempio: DBeng
- Common Name (e.g., your name or your server's hostname) [], ad esempio: aws
- Email Address [], ad esempio: abcd.efgh@amazonwebservice.com

5. Creare una directory per il wallet Oracle per il database Oracle.

```
mkdir -p /u01/app/oracle/wallet
```

6. Creare un nuovo wallet Oracle.

```
orapki wallet create -wallet "/u01/app/oracle/wallet" -pwd oracle123 -  
auto_login_local
```

7. Aggiungere il certificato root al wallet Oracle.

```
orapki wallet add -wallet "/u01/app/oracle/wallet" -pwd oracle123 -trusted_cert  
-cert /u01/app/oracle/self_signed_cert/self-rootCA.pem
```

8. Elencare i contenuti del wallet Oracle. L'elenco deve includere il certificato root.

```
orapki wallet display -wallet /u01/app/oracle/wallet -pwd oracle123
```

Ad esempio, potrebbe essere visualizzato in modo simile a quanto segue.

```
Requested Certificates:  
User Certificates:  
Trusted Certificates:  
Subject:          CN=aws,OU=DBeng,O= AmazonWebService,L=Sydney,ST=NSW,C=AU
```

9. Generare la richiesta di firma del certificato (CSR) utilizzando l'utility ORAPKI.

```
orapki wallet add -wallet "/u01/app/oracle/wallet" -pwd oracle123  
-dn "CN=aws" -keysize 2048 -sign_alg sha256
```

10. Esegui il comando seguente.

```
openssl pkcs12 -in /u01/app/oracle/wallet/ewallet.p12 -nodes -out /u01/app/oracle/  
wallet/nonoracle_wallet.pem
```

Ciò produce un output simile al seguente.

```
Enter Import Password:  
MAC verified OK  
Warning unsupported bag type: secretBag
```

11. Utilizzare "dms" come nome comune.

```
openssl req -new -key /u01/app/oracle/wallet/nonoracle_wallet.pem -out certdms.csr
```

Utilizza i parametri di input, come i seguenti.

- Country Name (2 letter code) [XX], ad esempio: AU
- State or Province Name (full name) [], ad esempio: NSW
- Locality Name (e.g., city) [Default City], ad esempio: Sydney
- Organization Name (e.g., company) [Default Company Ltd], ad esempio: AmazonWebService
- Organizational Unit Name (e.g., section) [], ad esempio: aws
- Common Name (e.g., your name or your server's hostname) [], ad esempio: aws
- Email Address [], ad esempio: abcd.efgh@amazonwebservice.com

Assicurati che non siano uguali a quelli della fase 4. Puoi, ad esempio, modificare il nome dell'unità organizzativa usando un nome diverso, come illustrato.

Inserisci gli attributi aggiuntivi seguenti da inviare con la richiesta di certificato.

- A challenge password [], ad esempio: oracle123

- An optional company name [], ad esempio: aws

12. Ottenere la firma del certificato.

```
openssl req -noout -text -in certdms.csr | grep -i signature
```

La chiave di firma per questo post è sha256WithRSAEncryption.

13. Utilizza il comando seguente per generare il file di certificato (.crt).

```
openssl x509 -req -in certdms.csr -CA self-rootCA.pem -CAkey self-rootCA.key  
-CAcreateserial -out certdms.crt -days 365 -sha256
```

Ciò produce un output simile al seguente.

```
Signature ok  
subject=/C=AU/ST=NSW/L=Sydney/O=awsweb/OU=DBeng/CN=aws  
Getting CA Private Key
```

14. Aggiungere il certificato al wallet.

```
orapki wallet add -wallet /u01/app/oracle/wallet -pwd oracle123 -user_cert -cert  
certdms.crt
```

15. Visualizza il wallet. È composto da due voci. Consulta il seguente codice.

```
orapki wallet display -wallet /u01/app/oracle/wallet -pwd oracle123
```

16. Configurare il file sqlnet.ora (\$ORACLE_HOME/network/admin/sqlnet.ora).

```
WALLET_LOCATION =  
  (SOURCE =  
    (METHOD = FILE)  
    (METHOD_DATA =  
      (DIRECTORY = /u01/app/oracle/wallet/)  
    )  
  )  
  
SQLNET.AUTHENTICATION_SERVICES = (NONE)  
SSL_VERSION = 1.0  
SSL_CLIENT_AUTHENTICATION = FALSE  
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA)
```

17. Interrompere il listener Oracle.

```
lsnrctl stop
```

18. Aggiungere voci per SSL nel file listener.ora (\$ORACLE_HOME/network/admin/listener.ora).

```
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION =
  (SOURCE =
    (METHOD = FILE)
    (METHOD_DATA =
      (DIRECTORY = /u01/app/oracle/wallet/)
    )
  )

SID_LIST_LISTENER =
  (SID_LIST =
    (SID_DESC =
      (GLOBAL_DBNAME = SID)
      (ORACLE_HOME = ORACLE_HOME)
      (SID_NAME = SID)
    )
  )

LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = localhost.localdomain)(PORT = 1521))
      (ADDRESS = (PROTOCOL = TCPS)(HOST = localhost.localdomain)(PORT = 1522))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))
    )
  )
```

19. Configurare il file tnsnames.ora (\$ORACLE_HOME/network/admin/tnsnames.ora).

```
<SID>=
(DESCRIPTION=
  (ADDRESS_LIST =
    (ADDRESS=(PROTOCOL = TCP)(HOST = localhost.localdomain)(PORT =
1521))
  )
  (CONNECT_DATA =
```

```
                (SERVER = DEDICATED)
                (SERVICE_NAME = <SID>)
            )
        )
<SID>_ssl=
(DESCRIPTION=
    (ADDRESS_LIST =
        (ADDRESS=(PROTOCOL = TCPS)(HOST = localhost.localdomain)(PORT =
1522))
    )
    (CONNECT_DATA =
        (SERVER = DEDICATED)
        (SERVICE_NAME = <SID>)
    )
)
```

20. Riavviare il listener Oracle.

```
lsnrctl start
```

21. Mostrare lo stato del listener Oracle.

```
lsnrctl status
```

22. Verificare la connessione SSL al database da localhost utilizzando sqlplus e la voce SSL tnsnames.

```
sqlplus -L ORACLE_USER@SID_ssl
```

23. Verificare che la connessione sia stabilita utilizzando SSL.

```
SELECT SYS_CONTEXT('USERENV', 'network_protocol') FROM DUAL;

SYS_CONTEXT('USERENV', 'NETWORK_PROTOCOL')
-----
tcps
```

24. Modificare la directory nella directory con il certificato autofirmato.

```
cd /u01/app/oracle/self_signed_cert
```

25. Crea un nuovo portafoglio client Oracle AWS DMS da utilizzare.

```
orapki wallet create -wallet ./ -auto_login_only
```

26. Aggiungere il certificato root autofirmato al wallet Oracle.

```
orapki wallet add -wallet ./ -trusted_cert -cert self-rootCA.pem -auto_login_only
```

27. Elenca il contenuto del portafoglio Oracle AWS DMS da utilizzare. L'elenco deve includere il certificato root autofirmato.

```
orapki wallet display -wallet ./
```

Ciò produce un output simile al seguente.

```
Trusted Certificates:
Subject:          CN=aws,OU=DBeng,O=AmazonWebService,L=Sydney,ST=NSW,C=AU
```

28. Carica il portafoglio Oracle su cui hai appena creato AWS DMS.

Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS

Nella tabella seguente sono riportati i metodi TDE (Transparent Data Encryption) AWS DMS supportati quando si lavora con un database di origine Oracle.

Metodo di accesso ai redo log	Tablespace TDE	Colonna TDE
Oracle LogMiner	Sì	Sì
Binary Reader	Sì	Sì

AWS DMS supporta Oracle TDE quando si utilizza Binary Reader, sia a livello di colonna che a livello di tablespace. Per utilizzare la crittografia TDE con AWS DMS, è necessario innanzitutto identificare la posizione del wallet Oracle in cui sono archiviate la chiave di crittografia TDE e la password TDE. Identifica quindi la chiave di crittografia TDE e la password corrette per l'endpoint di origine Oracle.

Per identificare e specificare la chiave di crittografia e la password per la crittografia TDE

1. Esegui la seguente query per trovare il wallet di crittografia Oracle nell'host di database Oracle.

```
SQL> SELECT WRL_PARAMETER FROM V$ENCRYPTION_WALLET;
```

```
WRL_PARAMETER
```

```
-----  
/u01/oracle/product/12.2.0/dbhome_1/data/wallet/
```

Qui, /u01/oracle/product/12.2.0/dbhome_1/data/wallet/ è la posizione del wallet.

2. Ottieni l'ID della chiave master utilizzando una delle seguenti opzioni di crittografia, a seconda di quale restituisce questo valore.

- a. Per la crittografia a livello di tabella o colonna, esegui le seguenti query.

```
SQL> SELECT OBJECT_ID FROM ALL_OBJECTS  
WHERE OWNER='DMS_USER' AND OBJECT_NAME='TEST_TDE_COLUMN' AND  
OBJECT_TYPE='TABLE';
```

```
OBJECT_ID
```

```
-----
```

```
81046
```

```
SQL> SELECT MKEYID FROM SYS.ENC$ WHERE OBJ#=81046;
```

```
MKEYID
```

```
-----
```

```
AWGDC9g1Sk8Xv+3bVveiVSgAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

Qui, AWGDC9g1Sk8Xv+3bVveiVSg è l'ID della chiave master (MKEYID). Se ottieni un valore per MKEYID, puoi continuare con la fase 3. In caso contrario, passa alla fase 2.

Note

Il carattere 'A' della stringa finale (AAA...) non fa parte del valore.

- b. Per la crittografia a livello di spazio di tabella, esegui le seguenti query.

```
SQL> SELECT TABLESPACE_NAME, ENCRYPTED FROM dba_tablespaces;
```

```
TABLESPACE_NAME          ENC
```

```
-----
```

```
SYSTEM                   NO
```

```
SYSAUX                   NO
```

```
UNDOTBS1                 NO
```



```

TEMP                NO
USERS               NO
TEST_ENCRYPT        YES
SQL> SELECT name,utl_raw.cast_to_varchar2( utl_encode.base64_encode('01' ||
substr(mkeyid,1,4))) ||
  utl_raw.cast_to_varchar2( utl_encode.base64_encode(substr(mkeyid,5,length(mkeyid))))
  masterkeyid_base64
FROM (SELECT t.name, RAWTOHEX(x.mkid) mkeyid FROM v$tablespace t, x$kcbtek x
  WHERE t.ts#=x.ts#)
WHERE name = 'TEST_ENCRYPT';

NAME                MASTERKEYID_BASE64
-----
TEST_ENCRYPT        AWGDC9g1Sk8Xv+3bVveiVSg=

```

Qui, AWGDC9g1Sk8Xv+3bVveiVSg è l'ID della chiave master (TEST_ENCRYPT). Se entrambe le fasi 2.1 e 2.2 restituiscono un valore, sono sempre identici.

Il carattere '=' finale non fa parte del valore.

3. Dalla riga di comando, elenca le voci del wallet di crittografia sull'host di database Oracle di origine.

```

$ mkstore -wrl /u01/oracle/product/12.2.0/dbhome_1/data/wallet/ -list
Oracle Secret Store entries:
ORACLE.SECURITY.DB.ENCRYPTION.AWGDC9g1Sk8Xv+3bVveiVSgAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.AY1mRA80XU9Qvzo3idU40H4AAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.MASTERKEY
ORACLE.SECURITY.ID.ENCRYPTION.
ORACLE.SECURITY.KB.ENCRYPTION.
ORACLE.SECURITY.KM.ENCRYPTION.AY1mRA80XU9Qvzo3idU40H4AAAAAAAAAAAAAAAAAAAAAAAAAAAA

```

Trova la voce contenente l'ID della chiave master che hai trovato nella fase 2 (AWGDC9g1Sk8Xv+3bVveiVSg). Questa voce è il nome della chiave di crittografia TDE.

4. Visualizza i dettagli della voce trovata nella fase precedente.

```

$ mkstore -wrl /u01/oracle/product/12.2.0/dbhome_1/data/wallet/ -viewEntry
ORACLE.SECURITY.DB.ENCRYPTION.AWGDC9g1Sk8Xv+3bVveiVSgAAAAAAAAAAAAAAAAAAAAAAAAAAAA
Oracle Secret Store Tool : Version 12.2.0.1.0
Copyright (c) 2004, 2016, Oracle and/or its affiliates. All rights reserved.
Enter wallet password:

```

```
ORACLE.SECURITY.DB.ENCRYPTION.AWGDC9g1Sk8Xv+3bVveiVSgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
= AEMAASAASGYs0phWHfNt9J5mEMkkegGFid4LLfQszDojgDzbfoYDEACv0x3pJC+UGD/
PdtE2jLIcBQcAeHgJChQGLA==
```

Inserisci la password del wallet per vedere il risultato.

Qui, il valore a destra di '=' è la password TDE.

5. Specifica il nome della chiave di crittografia TDE per l'endpoint di origine Oracle impostando l'attributo aggiuntivo di connessione `securityDbEncryptionName`.

```
securityDbEncryptionName=ORACLE.SECURITY.DB.ENCRYPTION.AWGDC9g1Sk8Xv
+3bVveiVSgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

6. Fornisci la password TDE associata a questa chiave sulla console come parte del valore Password dell'origine Oracle. Utilizza l'ordine seguente per formattare i valori delle password separati da virgole, terminati dal valore della password TDE.

```
Oracle_db_password,ASM_Password,AEMAASAASGYs0phWHfNt9J5mEMkkegGFid4LLfQszDojgDzbfoYDEACv0x3
+UGD/PdtE2jLIcBQcAeHgJChQGLA==
```

Specificare i valori della password in questo ordine indipendentemente dalla configurazione del database Oracle. Ad esempio, se si utilizza TDE ma il database Oracle non utilizza ASM, specifica i valori delle password nel seguente ordine separato da virgole.

```
Oracle_db_password,,AEMAASAASGYs0phWHfNt9J5mEMkkegGFid4LLfQszDojgDzbfoYDEACv0x3pJC
+UGD/PdtE2jLIcBQcAeHgJChQGLA==
```

Se le credenziali TDE specificate non sono corrette, l'operazione di AWS DMS migrazione non ha esito negativo. Tuttavia, l'attività non legge né applica le modifiche di replica in corso al database di destinazione. Dopo aver avviato l'attività, monitora le Statistiche della tabella nella pagina dell'attività di migrazione della console per assicurarti che le modifiche vengano replicate.

Se un amministratore di database modifica i valori delle credenziali TDE per il database Oracle durante l'esecuzione, l'attività ha esito negativo. Il messaggio di errore contiene il nuovo nome della chiave di crittografia TDE. Per specificare nuovi valori e riavviare l'attività, utilizza la procedura precedente.

⚠ Important

Non è possibile manipolare un wallet TDE creato in una posizione Oracle Automatic Storage Management (ASM) perché i comandi a livello di sistema operativo, come `cp`, `mv`, `orapki` e `mkstore`, danneggiano i file del wallet archiviati in una posizione ASM. Questa restrizione è specifica solo per i file del wallet TDE archiviati in una posizione ASM, ma non per i file del wallet TDE archiviati in una directory del sistema operativo locale.

Per manipolare un wallet TDE archiviato in ASM con comandi a livello di sistema operativo, crea un keystore locale e unisci il keystore ASM nel keystore locale come segue:

1. Crea un keystore locale.

```
ADMINISTER KEY MANAGEMENT create keystore file system wallet location
identified by wallet password;
```

2. Unisci il keystore ASM nel keystore locale.

```
ADMINISTER KEY MANAGEMENT merge keystore ASM wallet location identified
by wallet password into existing keystore file system wallet location
identified by wallet password with backup;
```

Quindi, per elencare le voci del wallet di crittografia e la password TDE, esegui le fasi 3 e 4 sul keystore locale.

Metodi di compressione supportati per l'utilizzo di Oracle come fonte per AWS DMS

Nella tabella seguente, puoi trovare i metodi di compressione AWS DMS supportati quando si lavora con un database di origine Oracle. Come illustrato nella tabella, il supporto alla compressione dipende sia dalla versione del database Oracle in uso sia dal fatto che DMS sia configurato per utilizzare Oracle LogMiner per accedere ai redo log.

Versione	Base	OLTP	HCC (da Oracle 11g R2 o versione successiva)	Altri
Oracle 10	No	N/D	N/D	No
Oracle 11 o versione successiva: Oracle LogMiner	Sì	Sì	Sì	Sì: qualsiasi metodo di compressione supportato da Oracle LogMiner.
Oracle 11 o versione successiva, Binary Reader	Sì	Sì	Sì. Per ulteriori informazioni, consulta la seguente nota.	Sì

Note

Quando l'endpoint di origine Oracle è configurato per utilizzare Binary Reader, il livello Query Low del metodo di compressione HCC è supportato solo per le attività di caricamento completo.

Replica di tabelle annidate utilizzando Oracle come fonte per AWS DMS

AWS DMS supporta la replica di tabelle Oracle contenenti colonne che sono tabelle nidificate o tipi definiti. Per abilitare questa funzionalità, aggiungere la seguente impostazione dell'attributo aggiuntivo di connessione all'endpoint di origine Oracle.

```
allowSelectNestedTables=true;
```

AWS DMS crea le tabelle di destinazione dalle tabelle nidificate di Oracle come normali tabelle principali e secondarie sulla destinazione senza un vincolo univoco. Per accedere ai dati corretti sulla destinazione, eseguire il join tra le tabelle padre e figlio. A tale scopo, creare manualmente un indice non univoco sulla colonna NESTED_TABLE_ID nella tabella figlio di destinazione. È quindi possibile

utilizzare la colonna `NESTED_TABLE_ID` nella clausola di join `ON` insieme alla colonna padre che corrisponde al nome della tabella figlio. Inoltre, la creazione di un indice di questo tipo migliora le prestazioni quando i dati della tabella secondaria di destinazione vengono aggiornati o eliminati da AWS DMS. Per vedere un esempio, consulta [Esempio di join per le tabelle padre e figlio sulla destinazione](#).

Si consiglia di configurare l'arresto dell'attività dopo il completamento di un caricamento completo. Quindi, creare questi indici non univoci per tutte le tabelle figlio replicate nella destinazione e riprendere l'attività.

Se una tabella nidificata acquisita viene aggiunta a una tabella principale esistente (acquisita o non acquisita), la AWS DMS gestisce correttamente. Tuttavia, l'indice non univoco per la tabella di destinazione corrispondente non viene creato. In questo caso, se la tabella figlio di destinazione diventa estremamente grande, le prestazioni potrebbero risentirne. In tal caso, si consiglia di interrompere l'attività, creare l'indice, quindi riprendere l'attività.

Dopo che le tabelle nidificate vengono replicate nella destinazione, fare in modo che il DBA esegua un join sulle tabelle figlio padre e corrispondenti per appiattare i dati.

Prerequisiti per la replica di tabelle nidificate Oracle come origine

Assicurarsi di replicare le tabelle padre per tutte le tabelle nidificate replicate. Include sia le tabelle principali (le tabelle contenenti la colonna della tabella nidificata) che le tabelle secondarie (ovvero nidificate) nelle mappature delle AWS DMS tabelle.

Tipi di tabelle nidificate Oracle supportati come origine

AWS DMS supporta i seguenti tipi di tabelle nidificate Oracle come origine:

- Tipo di dati
- Oggetto definito dall'utente

Limitazioni del supporto di AWS DMS per le tabelle nidificate Oracle come origine

AWS DMS presenta le seguenti limitazioni nel supporto delle tabelle nidificate Oracle come origine:

- AWS DMS supporta solo un livello di nidificazione delle tabelle.
- AWS DMS la mappatura delle tabelle non verifica che sia la tabella o le tabelle principale che quelle secondarie siano selezionate per la replica. Cioè, è possibile selezionare una tabella padre senza una tabella figlio o una tabella figlio senza una tabella padre.

Come fa AWS DMS a replicare le tabelle nidificate di Oracle come origine

AWS DMS replica le tabelle principali e nidificate sulla destinazione come segue:

- AWS DMS crea la tabella principale identica a quella di origine. Definisce quindi la colonna nidificata nella tabella padre come RAW(16) e include un riferimento alle tabelle nidificate della tabella padre nella sua colonna NESTED_TABLE_ID.
- AWS DMS crea la tabella figlio identica alla sorgente nidificata, ma con una colonna aggiuntiva denominata NESTED_TABLE_ID. Questa colonna ha lo stesso tipo e valore della colonna nidificata nella tabella padre corrispondente e ha lo stesso significato.

Esempio di join per le tabelle padre e figlio sulla destinazione

Per appiattare la tabella padre, eseguire un join tra le tabelle padre e figlio, come illustrato nell'esempio seguente:

1. Creare la tabella Type.

```
CREATE OR REPLACE TYPE NESTED_TEST_T AS TABLE OF VARCHAR(50);
```

2. Creare la tabella padre con una colonna di tipo NESTED_TEST_T come definita precedentemente.

```
CREATE TABLE NESTED_PARENT_TEST (ID NUMBER(10,0) PRIMARY KEY, NAME NESTED_TEST_T)  
  NESTED TABLE NAME STORE AS NAME_KEY;
```

3. Appiattare la tabella NESTED_PARENT_TEST utilizzando un join con la tabella figlio NAME_KEY in cui CHILD.NESTED_TABLE_ID corrisponde a PARENT.NAME.

```
SELECT ... FROM NESTED_PARENT_TEST PARENT, NAME_KEY CHILD WHERE CHILD.NESTED_  
TABLE_ID = PARENT.NAME;
```

Memorizzazione di REDO su Oracle ASM quando si utilizza Oracle come origine per AWS DMS

Per le origini Oracle con un'elevata generazione di REDO, l'archiviazione di REDO su Oracle ASM può favorire le prestazioni, specialmente in una configurazione RAC perché è possibile configurare DMS per distribuire le letture REDO di ASM su tutti i nodi ASM.

Per utilizzare questa configurazione, usa l'attributo di connessione `asmServer`. Ad esempio, la seguente stringa di connessione distribuisce le letture REDO di DMS su 3 nodi ASM:

```
asmServer=(DESCRIPTION=(CONNECT_TIMEOUT=8)(ENABLE=BROKEN)(LOAD_BALANCE=ON)(FAILOVER=ON)
(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=tcp)(HOST=asm_node1_ip_address)(PORT=asm_node1_port_number))
(ADDRESS=(PROTOCOL=tcp)(HOST=asm_node2_ip_address)(PORT=asm_node2_port_number))
(ADDRESS=(PROTOCOL=tcp)(HOST=asm_node3_ip_address)(PORT=asm_node3_port_number)))
(CONNECT_DATA=(SERVICE_NAME=+ASM)))
```

Quando si utilizza NFS per archiviare i REDO Oracle, è importante assicurarsi che vengano applicate le patch del client DNFS (Direct NFS) applicabili, in particolare tutte le patch che risolvono il bug Oracle 25224242. Per ulteriori informazioni, consulta la seguente pubblicazione Oracle sulle patch relative al client Direct NFS, [Recommended Patches for Direct NFS Client](#).

Inoltre, per migliorare le prestazioni di lettura NFS, si consiglia di aumentare il valore di `rsize` e `wsiz` in `fstab` per il volume NFS, come mostrato nell'esempio seguente.

```
NAS_name_here:/ora_DATA1_archive /u09/oradata/DATA1 nfs
rw,bg,hard,nointr,tcp,nfsvers=3,_netdev,
timeo=600,rsize=262144,wsiz=262144
```

Inoltre, regola il valore `tcp-max-xfer-size` come segue:


```
vserver nfs modify -vserver vserver -tcp-max-xfer-size 262144
```

Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine Oracle in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in [AWS CLI](#), con la sintassi `--oracle-settings '{"EndpointSetting": "value", ...}'` JSON.

Nella tabella seguente sono riportate le impostazioni degli endpoint che è possibile utilizzare con Oracle come origine.


Nome	Descrizione
AccessAlternateDirectly	<p>Imposta questo attributo su false per utilizzare Binary Reader al fine di acquisire i dati di modifica per un Amazon RDS per Oracle come origine. In questo modo l'istanza DMS è configurata per non accedere ai log redo tramite qualsiasi sostituzione del prefisso del percorso specificato utilizzando l'accesso diretto ai file. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: true</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"AccessAlternateDirectly": false}'</code></p>
AdditionalArchivedLogDestId	<p>Imposta questo attributo con ArchivedLogDestId in una configurazione principale/in standby. Questo attributo è utile in caso di switchover quando si utilizza un database Oracle Data Guard come origine. In questo caso, AWS DMS deve sapere da quale destinazione recuperare i redo log dell'archivio per leggere le modifiche. Ciò è necessario perché dopo lo switchover l'istanza primaria precedente è diventata un'istanza di standby.</p> <p>Sebbene AWS DMS supporti l'uso dell'RESETLOGS opzione Oracle per aprire il database, non utilizzarla mai a RESETLOGS meno che non sia necessario. Per ulteriori informazioni su RESETLOGS, consulta RMAN Data Repair Concepts nella Guida per l'utente di Oracle® Database Backup and Recovery.</p> <p>Valori validi: ID di destinazione dell'archivio</p> <p>Esempio: <code>--oracle-settings '{"AdditionalArchivedLogDestId": 2}'</code></p>
AddSupplementalLogging	<p>Imposta questo attributo per configurare il log supplementare a livello di tabella per il database Oracle. Questo attributo abilita uno dei seguenti elementi in tutte le tabelle selezionate per un'attività di migrazione, a seconda dei metadati della tabella:</p>

Nome	Descrizione
	<ul style="list-style-type: none"> • Registrazione supplementare di PRIMARY KEY COLUMNS • Registrazione supplementare di UNIQUE KEY COLUMNS • Registrazione supplementare di ALL COLUMNS <p>Valore predefinito: false</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"AddSupplementalLogging": false}'</code></p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Se utilizzi questa opzione, è comunque necessario abilitare il log supplementare a livello di database come descritto in precedenza.</p> </div>
AllowSelectNestedTables	<p>Imposta questo attributo su true per abilitare la replica delle tabelle Oracle contenenti colonne che sono tabelle nidificate o tipi definiti. Per ulteriori informazioni, consulta Replica di tabelle annidate utilizzando Oracle come fonte per AWS DMS.</p> <p>Valore predefinito: false</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"AllowSelectNestedTables": true}'</code></p>


Nome	Descrizione
ArchivedLogDestId	<p>Specifica l'ID di destinazione per i registri di ripristino archiviati. Questo valore deve corrispondere a un numero nella colonna <code>dest_id</code> della visualizzazione <code>v\$archived_log</code>. Se utilizzi una destinazione aggiuntiva per i log redo, ti consigliamo di usare l'attributo <code>AdditionalArchivedLogDestId</code> per specificare l'ID della destinazione aggiuntiva. In questo modo è possibile migliorare le prestazioni garantendo l'accesso ai log corretti fin dal principio.</p> <p>Valore predefinito: 1</p> <p>Valori validi: numero</p> <p>Esempio: <code>--oracle-settings '{"ArchivedLogDestId": 1}'</code></p>
ArchivedLogsOnly	<p>Quando questo campo è impostato su Y, accede AWS DMS solo ai redo log archiviati. Se i redo log archiviati sono memorizzati solo su Oracle ASM, all'account AWS DMS utente devono essere concessi i privilegi ASM.</p> <p>Valore predefinito: N</p> <p>Valori validi: Y/N (S/N)</p> <p>Esempio: <code>--oracle-settings '{"ArchivedLogsOnly": Y}'</code></p>


Nome	Descrizione
asmUsePLSQLArray (solo ECA)	<p>Utilizza questo attributo di connessione aggiuntivo (ECA) per acquisire le modifiche all'origine con BinaryReader. Questa impostazione consente a DMS di memorizzare nel buffer 50 letture a livello di ASM per singolo thread di lettura controllando al contempo il numero di thread che utilizzano l'attributo <code>parallelASReadThread</code>. Quando impostate questo attributo, il lettore AWS DMS binario utilizza un blocco PL/SQL anonimo per acquisire i dati di ripristino e inviarli all'istanza di replica come buffer di grandi dimensioni. Ciò riduce il numero di round trip all'origine. Inoltre, può migliorare in modo significativo le prestazioni di acquisizione dell'origine, ma comporta un maggiore consumo di memoria PGA sull'istanza ASM. Potrebbero sorgere problemi di stabilità se la destinazione di memoria non è sufficiente. È possibile utilizzare la formula seguente per stimare l'utilizzo totale della memoria PGA dell'istanza ASM per una singola attività DMS: $\text{number_of_redo_threads} * \text{parallelASReadThreads} * 7 \text{ MB}$</p> <p>Valore predefinito: false</p> <p>Valori validi: true/false</p> <p>Esempio ECA: <code>asmUsePLSQLArray=true;</code></p>
ConvertTimestampWithZoneToUTC	<p>Imposta questo attributo su <code>true</code> per convertire in UTC il valore del timestamp delle colonne "TIMESTAMP WITH TIME ZONE" e "TIMESTAMP WITH LOCAL TIME ZONE". Per impostazione predefinita, il valore di questo attributo è "false" e i dati vengono replicati utilizzando il fuso orario del database di origine.</p> <p>Valore predefinito: false</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"ConvertTimestampWithZoneToUTC": true}'</code></p>

Nome	Descrizione
EnableHomogenousPartitionOps	<p>Imposta questo attributo su <code>true</code> per abilitare la replica delle operazioni DDL su partizioni e sottopartizioni Oracle per la migrazione omogenea di Oracle.</p> <p>Si noti che questa funzionalità e questo miglioramento sono stati introdotti nella versione 3.4.7. AWS DMS</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"EnableHomogenousPartitionOps": true}'</code></p>
EnableHomogenousTablespace	<p>Imposta questo attributo per consentire la replica omogenea degli spazi tabelle e la creazione di tabelle o indici esistenti negli stessi spazi tabelle sulla destinazione.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"EnableHomogenousTablespace": true}'</code></p>

Nome	Descrizione
EscapeCharacter	<p>Imposta questo attributo su un carattere di escape. Il carattere di escape consente che un singolo carattere jolly si comporti come un normale carattere nelle espressioni di mappatura delle tabelle. Per ulteriori informazioni, consulta Caratteri jolly nella mappatura delle tabelle.</p> <p>Valore predefinito: Null</p> <p>Valori validi: qualsiasi carattere diverso da un carattere jolly</p> <p>Esempio: <code>--oracle-settings '{"EscapeCharacter": "#"}'</code></p> <div data-bbox="461 684 1508 953" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Può essere utilizzato solo <code>escapeCharacter</code> per i nomi delle tabelle. Non imposta i caratteri di escape dei nomi degli schemi o dei nomi delle colonne.</p></div>
ExposeViews	<p>Utilizza questo attributo per estrarre i dati una volta da una vista. Non è possibile utilizzarlo per la replica continua. Quando estrai dati da una vista, quest'ultima viene mostrata come tabella sullo schema di destinazione.</p> <p>Valore predefinito: false</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"ExposeViews": true}'</code></p>

Nome	Descrizione
ExtraArchivedLogDestIds	<p>Specifica gli ID di un'altra destinazione per uno o più registri di ripristino o archiviati. Questi ID rappresentano i valori della colonna <code>dest_id</code> nella visualizzazione <code>v\$archived_log</code>. Utilizzate questa impostazione con l'attributo <code>ArchivedLogDestId</code> extra connection in una configurazione o in una <code>primary-to-single</code> configurazione. <code>primary-to-multiple-standby</code></p> <p>Questa impostazione è utile in caso di switchover quando si utilizza un database Oracle Data Guard come origine. In questo caso, sono AWS DMS necessarie informazioni sulla destinazione da cui recuperare i redo log dell'archivio per leggere le modifiche. AWS DMS ne ha bisogno perché dopo il passaggio l'istanza primaria precedente è un'istanza di standby.</p> <p>Valori validi: ID di destinazione dell'archivio</p> <p>Esempio: <code>--oracle-settings '{"ExtraArchivedLogDestIds": 1}'</code></p>
FailTasksOnLobTruncation	<p>Se è impostato su <code>true</code>, questo attributo non consentirà la riuscita di un'attività se le dimensioni attuali di una colonna LOB sono maggiori di quelle specificate in <code>LobMaxSize</code> .</p> <p>Se un'attività è impostata sulla modalità LOB limitata e questa opzione è impostata su <code>true</code>, l'operazione ha esito negativo invece di troncatura i dati LOB.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: booleani</p> <p>Esempio: <code>--oracle-settings '{"FailTasksOnLobTruncation": true}'</code></p>

Nome	Descrizione
<code>filterTransactionsOfUser</code> (solo ECA)	<p>Utilizza questo attributo di connessione aggiuntivo (ECA) per consentire a DMS di ignorare le transazioni di un utente specificato durante la replica dei dati da Oracle durante l'utilizzo. LogMiner È possibile passare i nomi utente separati da virgole, ma devono essere scritti solo in lettere MAIUSCOLE.</p> <p>Esempio ECA: <code>filterTransactionsOfUser= <i>USERNAME</i>;</code></p>
<code>NumberDataTypeScale</code>	<p>Specifica il fattore di dimensionamento. È possibile selezionare un aumento fino a 38 oppure è possibile selezionare -1 per FLOAT o -2 per VARCHAR. Per impostazione predefinita, il tipo di dati NUMBER è convertito alla precisione 38, dimensione 10.</p> <p>Valore predefinito: 10</p> <p>Valori validi: da -2 a 38 (-2 per VARCHAR, -1 per FLOAT)</p> <p>Esempio: <code>--oracle-settings '{"NumberDataTypeScale": 12}'</code></p> <div data-bbox="462 1087 1507 1543" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Seleziona una combinazione con scala di precisione, -1 (FLOAT) o -2 (VARCHAR). DMS supporta qualsiasi combinazione con scala di precisione prevista da Oracle. Se la precisione è pari o superiore a 39, seleziona -2 (VARCHAR). L' <code>NumberDataTypeScale</code> impostazione per il database Oracle viene utilizzata solo per il tipo di dati NUMBER (senza la precisione esplicita e la definizione della scala).</p> </div>

Nome	Descrizione
OpenTransactionWindow	<p>Fornisce l'intervallo di tempo in minuti per verificare la presenza di eventuali transazioni aperte per l'attività di sola CDC.</p> <div data-bbox="461 352 1507 760" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Quando è impostato su OpenTransactionWindow 1 o superiore, DMS converte i SCN_TO_TIMESTAMP valori SCN in valori di timestamp. A causa delle limitazioni del database Oracle, se si specifica un SCN troppo vecchio come punto di partenza CDC, SCN_TO_TIMESTAMP fallirà con un errore e non sarà possibile avviare attività solo CDC. ORA-08181</p> </div> <p>Valore predefinito: 0</p> <p>Valori validi: numero intero da 0 a 240</p> <p>Esempio: openTransactionWindow=15;</p>
OraclePathPrefix	<p>Imposta questo attributo stringa sul valore richiesto per utilizzare Binary Reader al fine di acquisire dati di modifica per un Amazon RDS per Oracle come origine. Questo valore specifica la radice Oracle predefinita utilizzata per accedere ai log redo. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: nessuno</p> <p>Valore valido: /rdsdbdata/db/ORCL_A/</p> <p>Esempio: <code>--oracle-settings '{"OraclePathPrefix": " /rdsdbdata/db/ORCL_A/ "'}</code></p>

Nome	Descrizione
ParallelASMReadThreads	<p>Imposta questo attributo per modificare il numero di thread configurati da DMS per eseguire l'acquisizione dei dati di modifica (CDC) utilizzando Oracle Automatic Storage Management (ASM). È possibile specificare un valore intero compreso tra 2 (impostazione predefinita) e 8 (massimo). Utilizzare questo attributo con l'attributo ReadAheadBlocks. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: 2</p> <p>Valori validi: numero intero da 2 a 8</p> <p>Esempio: <code>--oracle-settings '{"ParallelASMReadThreads": 6;}'</code></p>
ReadAheadBlocks	<p>Imposta questo attributo per modificare il numero di thread configurati da DMS per eseguire CDC utilizzando Oracle Automatic Storage Management (ASM) e lo storage NAS non ASM. È possibile specificare un valore intero compreso tra 1.000 (impostazione predefinita) e 200.000 (massimo). Utilizzare questo attributo con l'attributo ParallelASMReadThreads. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: 1000</p> <p>Valori validi: numero intero da 1.000 a 200.000</p> <p>Esempio: <code>--oracle-settings '{"ReadAheadBlocks": 150000}'</code></p>

Nome	Descrizione
ReadTableSpaceName	<p>Quando è impostato su <code>true</code>, questo attributo supporta la replica dello spazio tabella.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: booleani</p> <p>Esempio: <code>--oracle-settings '{"ReadTableSpaceName": true}'</code></p>
ReplacePathPrefix	<p>Imposta questo attributo su <code>true</code> per utilizzare Binary Reader al fine di acquisire i dati di modifica per un Amazon RDS per Oracle come origine. Questa impostazione indica all'istanza DMS di sostituire la radice Oracle predefinita con l'impostazione <code>UsePathPrefix</code> specificata per accedere ai log redo. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"ReplacePathPrefix": true}'</code></p>
RetryInterval	<p>Specifica il numero di secondi che il sistema attende prima di reinviare una query.</p> <p>Valore predefinito: <code>5</code></p> <p>Valori validi: numeri a partire da <code>1</code></p> <p>Esempio: <code>--oracle-settings '{"RetryInterval": 6}'</code></p>

Nome	Descrizione
SecurityDbEncryptionName	<p>Specifica il nome di una chiave utilizzata per la crittografia trasparente dei dati (TDE) delle colonne e dei tablespaces nel database di origine Oracle. Per ulteriori informazioni sull'impostazione di questo attributo e della relativa password associata nell'endpoint di origine Oracle, consulta Metodi di crittografia supportati per l'utilizzo di Oracle come fonte per AWS DMS.</p> <p>Valore predefinito: ""</p> <p>Valori validi: stringa</p> <p>Esempio: <code>--oracle-settings '{"SecurityDbEncryptionName": "ORACLE.SECURITY.DB.ENCRYPTION.Adg8m2dhkU/0v/m5QUaaNJEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"}'</code></p>
SpatialSdo2GeoJsonFunctionName	<p>Per le origini Oracle 12.1 o precedenti che migrano verso destinazioni PostgreSQL, utilizzare questo attributo per convertire SDO_GEOMETRY in formato GEOJSON.</p> <p>Per impostazione predefinita, AWS DMS richiama la funzione <code>SDO2GEOJSON</code> personalizzata che deve essere presente e accessibile all'utente. AWS DMS In alternativa, puoi creare una funzione personalizzata che imita l'operazione di <code>SDO2GEOJSON</code> e impostare <code>SpatialSdo2GeoJsonFunctionName</code> affinché la richiami.</p> <p>Valore predefinito: <code>SDO2GEOJSON</code></p> <p>Valori validi: stringa</p> <p>Esempio: <code>--oracle-settings '{"SpatialSdo2GeoJsonFunctionName": "myCustomSDO2GEOJSONFunction"}'</code></p>

Nome	Descrizione
StandbyDelayTime	<p>Utilizza questo attributo per specificare il tempo di ritardo in minuti della sincronizzazione in standby. Se l'origine è un database in standby Active Data Guard, utilizza questo attributo per specificare l'intervallo di tempo tra il database primario e quello in standby.</p> <p>In AWS DMS, puoi creare un task Oracle CDC che utilizza un'istanza di standby di Active Data Guard come fonte per replicare le modifiche in corso. Questa operazione elimina la necessità di connettersi a un database attivo che potrebbe essere in produzione.</p> <p>Valore predefinito: 0</p> <p>Valori validi: numero</p> <p>Esempio: <code>--oracle-settings '{"StandbyDelayTime": 1}'</code></p> <p>Nota: quando si utilizza DMS 3.4.6, 3.4.7 e versioni successive, l'uso di questa impostazione di connessione è facoltativo. Nell'ultima versione di DMS 3.4.6 e nella versione 3.4.7, <i>dms_user</i> deve avere l'autorizzazione <code>select</code> su <code>V_\$DATAGUARD_STATS</code>, che consente a DMS di calcolare il tempo di ritardo in standby.</p>
UseAlternateFolderForOnline	<p>Imposta questo attributo su <code>true</code> per utilizzare Binary Reader al fine di acquisire i dati di modifica per un Amazon RDS per Oracle come origine. In questo modo l'istanza DMS utilizza qualsiasi sostituzione prefisso specificata per accedere a tutti i log redo online. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"UseAlternateFolderForOnline": true}'</code></p>

Nome	Descrizione
UseBfile	<p>Imposta questo attributo su Y (Sì) per acquisire i dati utilizzando la utility Binary Reader. Imposta UseLogminerReader su N (No) per impostare questo attributo su Y (Sì). Per utilizzare Binary Reader con Amazon RDS per Oracle come origine, è necessario impostare attributi aggiuntivi. Per ulteriori informazioni su questa impostazione e sull'utilizzo di Oracle ASM, vedere Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC.</p> <p>Nota: quando si imposta questo valore come attributo aggiuntivo di connessione, i valori validi sono "Y" e "N". Quando si configura questo valore come impostazione dell'endpoint, i valori validi sono true e false.</p> <p>Valore predefinito: N</p> <p>Valori validi: Y/N (quando si imposta questo valore come attributo aggiuntivo di connessione), true/false (quando si imposta questo valore come impostazione dell'endpoint).</p> <p>Esempio: <code>--oracle-settings '{"UseBfile": Y}'</code></p>

Nome	Descrizione
UseLogminerReader	<p>Imposta questo attributo su Y per acquisire i dati di modifica utilizzando l' LogMiner utilità (impostazione predefinita). Imposta questa opzione su N se desideri che AWS DMS acceda ai redo log come file binario. Quando imposti questa opzione su N, aggiungi anche l'impostazione usebFile=y. Per ulteriori informazioni su questa impostazione e sull'utilizzo di Oracle Automatic Storage Management (ASM), consulta Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC.</p> <p>Nota: quando si imposta questo valore come attributo aggiuntivo di connessione, i valori validi sono "Y" e "N". Quando si configura questo valore come impostazione dell'endpoint, i valori validi sono true e false.</p> <p>Valore predefinito: Y</p> <p>Valori validi: Y/N (quando si imposta questo valore come attributo aggiuntivo di connessione), true/false (quando si imposta questo valore come impostazione dell'endpoint).</p> <p>Esempio: <code>--oracle-settings '{"UseLogminerReader": Y}'</code></p>
UsePathPrefix	<p>Imposta questo attributo stringa sul valore richiesto per utilizzare Binary Reader al fine di acquisire dati di modifica per un Amazon RDS per Oracle come origine. Questo valore specifica il prefisso del percorso utilizzato per sostituire la radice Oracle predefinita per accedere ai log redo. Per ulteriori informazioni, consulta Configurazione di un'attività CDC per l'utilizzo di Binary Reader con un codice sorgente RDS for Oracle per AWS DMS.</p> <p>Valore predefinito: nessuno</p> <p>Valore valido: <code>/rdsdbdata/log/</code></p> <p>Esempio: <code>--oracle-settings '{"UsePathPrefix": " /rdsdbdata/log/ "'}</code></p>

Tipi di dati di origine per Oracle

L'endpoint Oracle for AWS DMS supporta la maggior parte dei tipi di dati Oracle. La tabella seguente mostra i tipi di dati di origine Oracle supportati durante l'utilizzo AWS DMS e la mappatura predefinita ai tipi di AWS DMS dati.

Note

Ad eccezione dei tipi di dati LONG e LONG RAW, durante la replica da un'origine Oracle a una destinazione Oracle (replica omogenea), tutti i tipi di dati di origine e di destinazione saranno identici. Tuttavia, il tipo di dati LONG verrà mappato su CLOB e il tipo di dati LONG RAW verrà mappato su BLOB.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere [Tipi di dati per AWS Database Migration Service](#).

Tipo di dati Oracle	AWS DMS tipo di dati
BINARY_FLOAT	REAL4
BINARY_DOUBLE	REAL8
BINARY	BYTES
FLOAT (P)	Se la precisione è minore o uguale a 24, usa REAL4. Se la precisione è maggiore di 24, usa REAL8.
NUMBER (P,S)	Quando la dimensione è maggiore di 0, utilizza NUMERIC. Quando la dimensione è 0: <ul style="list-style-type: none"> e la precisione è minore o uguale a 2, usa INT1. e la precisione è maggiore di 2 e minore o uguale a 4, usa INT2. e la precisione è maggiore di 4 e minore o uguale a 9, usa INT4. e la precisione è maggiore a 9, usa NUMERIC.

Tipo di dati Oracle	AWS DMS tipo di dati
	<ul style="list-style-type: none"> e la precisione è maggiore o uguale alla dimensione, usa NUMERIC. <p>Quando la dimensione è minore di 0, usa REAL8.</p>
DATE	DATETIME
INTERVAL_YEAR TO MONTH	STRING (con indicazione interval year_to_month)
INTERVAL_DAY TO SECOND	STRING (con indicazione interval day_to_second)
TIMESTAMP	DATETIME
TIMESTAMP WITH TIME ZONE	STRING (con indicazione timestamp_with_timezone)
TIMESTAMP WITH LOCAL TIME ZONE	STRING (con indicazione timestamp_with_local_timezone)
CHAR	STRING
VARCHAR2	STRING
NCHAR	WSTRING
NVARCHAR2	WSTRING
RAW	BYTES
REAL	REAL8

Tipo di dati Oracle	AWS DMS tipo di dati
BLOB	<p data-bbox="542 222 630 256">BLOB</p> <p data-bbox="542 306 1455 483">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati BLOB per un'attività specifica. AWS DMS supporta i tipi di dati BLOB solo nelle tabelle che includono una chiave primaria.</p>
CLOB	<p data-bbox="542 527 630 560">CLOB</p> <p data-bbox="542 611 1481 787">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati CLOB per un'attività specifica. Durante CDC, AWS DMS supporta i tipi di dati CLOB solo nelle tabelle che includono una chiave primaria.</p>
NCLOB	<p data-bbox="542 831 646 865">NCLOB</p> <p data-bbox="542 915 1503 1092">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati NCLOB per un'attività specifica. Durante CDC, AWS DMS supporta i tipi di dati NCLOB solo nelle tabelle che includono una chiave primaria.</p>


Tipo di dati Oracle	AWS DMS tipo di dati
LONG	<p data-bbox="545 226 634 260">CLOB</p> <p data-bbox="545 306 1487 390">Il tipo di dati LONG non è supportato nella modalità di applicazione ottimizzata per batch (modalità CDC). TurboStream</p> <p data-bbox="545 436 1507 520">Per utilizzare questo tipo di dati con AWS DMS, abilita l'uso dei LOB per un'attività specifica.</p> <p data-bbox="545 567 1503 651">Durante CDC o a pieno carico, AWS DMS supporta i tipi di dati LOB solo nelle tabelle con una chiave primaria.</p> <p data-bbox="545 697 1503 1008">Inoltre, AWS DMS non supporta la modalità LOB completa per il caricamento di colonne LONG. È invece possibile utilizzare la modalità LOB limitata per migrare le colonne LONG in una destinazione Oracle. In modalità LOB limitata, AWS DMS tronca a 64 KB tutti i dati impostati su colonne LONG più lunghe di 64 KB. Per ulteriori informazioni sul supporto LOB in, vedere AWS DMS Impostazione del supporto LOB per i database di origine in un task AWS DMS</p>

Tipo di dati Oracle	AWS DMS tipo di dati
LONG RAW	<p>BLOB</p> <p>Il tipo di dati LONG RAW non è supportato nella modalità di applicazione ottimizzata per batch (modalità TurboStream CDC).</p> <p>Per utilizzare questo tipo di dati con AWS DMS, abilita l'uso dei LOB per un'attività specifica.</p> <p>Durante CDC o a pieno carico, AWS DMS supporta i tipi di dati LOB solo nelle tabelle con una chiave primaria.</p> <p>Inoltre, AWS DMS non supporta la modalità LOB completa per il caricamento di colonne LONG RAW. È invece possibile utilizzare la modalità LOB limitata per migrare le colonne LONG RAW in una destinazione Oracle. In modalità LOB limitata, AWS DMS tronca tutti i dati a 64 KB impostati su colonne LONG RAW più lunghe di 64 KB. Per ulteriori informazioni sul supporto LOB in, vedere AWS DMS Impostazione del supporto LOB per i database di origine in un task AWS DMS</p>
XMLTYPE	CLOB
SDO_GEOMETRY	<p>BLOB (in caso di migrazione da Oracle a Oracle)</p> <p>CLOB (in caso di migrazione da Oracle a PostgreSQL)</p>

Le tabelle di Oracle utilizzate come origine con colonne dei seguenti tipi di dati non sono supportate e non possono essere replicate. La replica di colonne con questi tipi di dati risulta in una colonna null.

- BFILE
- ROWID
- REF
- UROWID
- Tipi di dati definiti dall'utente
- ANYDATA

- VARRAY

 Note

Le colonne virtuali non sono supportate.

Migrazione dei tipi di dati spaziali di Oracle

I dati spaziali identificano le informazioni sulla geometria di un oggetto o di una posizione nello spazio. In un database Oracle, la descrizione geometrica di un oggetto spaziale viene memorizzata in un oggetto di tipo SDO_GEOMETRY. All'interno di questo oggetto, la descrizione geometrica viene memorizzata in una singola riga in una singola colonna di una tabella definita dall'utente.

AWS DMS supporta la migrazione del tipo Oracle SDO_GEOMETRY da una fonte Oracle a un target Oracle o PostgreSQL.

Quando esegui la migrazione dei tipi di dati spaziali Oracle utilizzando, tieni presente queste considerazioni: AWS DMS

- Quando si esegue la migrazione verso una destinazione Oracle, assicurarsi di trasferire manualmente le voci USER_SDO_GEOM_METADATA che includono informazioni sul tipo.
- Durante la migrazione da un endpoint di origine Oracle a un endpoint di destinazione PostgreSQL, crea colonne di destinazione. AWS DMS Queste colonne contengono informazioni predefinite sul tipo di geometria e di geografia con una dimensione 2D e un identificatore di riferimento spaziale (SRID) uguale a zero (0). Un esempio è GEOMETRY, 2, 0.
- Per le origini Oracle 12.1 o precedenti che migrano a destinazioni PostgreSQL, convertire gli oggetti SDO_GEOMETRY in formato GEOJSON utilizzando la funzione SD02GEOJSON o l'attributo di connessione aggiuntivo spatialSdo2GeoJsonFunctionName. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).
- AWS DMS supporta le migrazioni di Oracle Spatial Column solo per la modalità Full LOB. AWS DMS non supporta le modalità LOB limitata o LOB in linea. Per ulteriori informazioni sulla modalità LOB, consulta [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#).
- Poiché supporta AWS DMS solo la modalità Full LOB per la migrazione di Oracle Spatial Columns, la tabella delle colonne richiede una chiave primaria e una chiave univoca. Se la tabella non dispone di una chiave primaria e di una chiave univoca, la tabella viene ignorata dalla migrazione.

Utilizzo di un database Microsoft SQL Server come origine per AWS DMS

Esegui la migrazione dei dati da uno o più database di Microsoft SQL Server utilizzando AWS DMS. Con un database SQL Server come origine, è possibile migrare i dati verso un altro database SQL Server o verso uno degli altri database AWS DMS supportati.

Per informazioni sulle versioni di SQL Server AWS DMS supportate come origine, vedere [Fonti per AWS DMS](#).

È possibile installare il database SQL Server di origine su qualsiasi computer della rete. Per l'uso con AWS DMS è necessario anche un account di SQL Server con i privilegi di accesso appropriati per il database di origine e per il tipo di attività scelta. L'account deve avere le autorizzazioni `view definition` e `view server state`. È possibile aggiungere questa autorizzazione utilizzando il seguente comando:

```
grant view definition to [user]
grant view server state to [user]
```

AWS DMS supporta la migrazione di dati da istanze denominate di SQL Server. È possibile usare la seguente notazione nel nome del server al momento della creazione dell'endpoint di origine.

```
IPAddress\InstanceName
```

Ad esempio, il seguente è un nome corretto di server di endpoint di origine. Qui la prima parte del nome è l'indirizzo IP del server e la seconda parte è il nome dell'istanza di SQL Server (in questo esempio, SQLTest).

```
10.0.0.25\SQLTest
```

Inoltre, ottieni il numero di porta su cui è in ascolto l'istanza denominata di SQL Server e usalo per configurare AWS DMS l'endpoint di origine.

Note

L'impostazione predefinita per Microsoft SQL Server è la porta 1433. Tuttavia vengono spesso utilizzate porte dinamiche che cambiano ogni volta che viene avviato SQL Server e specifici numeri di porta statici utilizzati per connettersi a SQL Server tramite un firewall.

Quindi, vuoi conoscere il numero di porta effettivo dell'istanza denominata di SQL Server quando crei l'endpoint di AWS DMS origine.

Puoi utilizzare il protocollo SSL per crittografare le connessioni tra l'endpoint di SQL Server e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint di SQL Server, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Per ulteriori dettagli sull'utilizzo dei database di origine di SQL Server e AWS DMS, vedere quanto segue.

Argomenti

- [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#)
- [Autorizzazioni per attività solo pieno carico](#)
- [Prerequisiti per l'utilizzo della replica continua \(CDC\) da un'origine SQL Server](#)
- [Acquisizione delle modifiche ai dati per SQL Server autogestito on-premise o su Amazon EC2](#)
- [Configurazione della replica continua su un'istanza database di SQL Server nel cloud](#)
- [Impostazioni consigliate per l'utilizzo di Amazon RDS for SQL Server come origine per AWS DMS](#)
- [Metodi di compressione supportati per SQL Server](#)
- [Utilizzo di gruppi di disponibilità di SQL Server autogestiti AlwaysOn](#)
- [Requisiti di sicurezza quando si utilizza SQL Server come origine per AWS Database Migration Service](#)
- [Impostazioni degli endpoint quando si utilizza SQL Server come origine per AWS DMS](#)
- [Tipi di dati di origine per SQL Server](#)

Limitazioni all'utilizzo di SQL Server come origine per AWS DMS

Quando si utilizza un database SQL Server come origine per AWS DMS, si applicano le seguenti limitazioni:

- La proprietà di identità di una colonna non viene migrata a una colonna del database di destinazione.
- L'endpoint SQL Server non supporta l'uso di tabelle con colonne sparse.
- L'autenticazione Windows non è supportata.

- Le modifiche apportate ai campi calcolati in un SQL Server non vengono replicate.
- Le tabelle temporali non sono supportate.
- Il cambio delle partizioni di SQL Server non è supportato.
- Quando si utilizzano le utilità WRITETEXT e UPDATETEXT, AWS DMS non acquisisce gli eventi applicati al database di origine.
- Il seguente modello DML (data manipulation language) non è supportato.

```
SELECT * INTO new_table FROM existing_table
```

- Quando utilizzi SQL Server come origine, la crittografia a livello di colonna non è supportata.
- AWS DMS non supporta gli audit a livello di server su SQL Server 2008 o SQL Server 2008 R2 come sorgenti. Ciò è dovuto a un problema noto con SQL Server 2008 e 2008 R2. Ad esempio, l'esecuzione del comando seguente causa AWS DMS un errore.

```
USE [master]
GO
ALTER SERVER AUDIT [my_audit_test-20140710] WITH (STATE=on)
GO
```

- Le colonne di geometria non sono supportate in modalità LOB completa quando si utilizza SQL Server come origine. Utilizza invece la modalità LOB limitata o definisci le impostazioni dell'attività InLineLobMaxSize per utilizzare la modalità LOB in linea.
- Quando si utilizza un database di origine Microsoft SQL Server in un'attività di replica, le definizioni di SQL Server Replication Publisher non vengono rimosse se si rimuove l'attività. Un amministratore di sistema di Microsoft SQL Server deve eliminare tali definizioni da Microsoft SQL Server.
- La migrazione dei dati dalle non-schema-bound viste e dagli schemi è supportata solo per le attività a pieno carico.
- La ridenominazione delle tabelle utilizzando sp_rename non è supportata (ad esempio, sp_rename 'Sales.SalesRegion', 'SalesReg;')
- La ridenominazione delle colonne utilizzando sp_rename non è supportata (ad esempio, sp_rename 'Sales.Sales.Region', 'RegID', 'COLUMN';)
- AWS DMS non supporta l'elaborazione delle modifiche per impostare e annullare i valori predefiniti delle colonne (utilizzando la clausola con le ALTER COLUMN SET DEFAULT istruzioni). ALTER TABLE

- AWS DMS non supporta l'elaborazione delle modifiche per impostare l'annullabilità delle colonne (utilizzando la `ALTER COLUMN [SET|DROP] NOT NULL` clausola con le istruzioni). `ALTER TABLE`
- Con SQL Server 2012 e SQL Server 2014, quando si utilizza la replica DMS con i gruppi di disponibilità, il database di distribuzione non può essere inserito in un gruppo di disponibilità. SQL 2016 supporta l'inserimento del database di distribuzione in un gruppo di disponibilità, ad eccezione dei database di distribuzione utilizzati nelle topologie di unione, bidirezionali o di replica peer-to-peer
- Per le tabelle partizionate, AWS DMS non supporta impostazioni di compressione dei dati diverse per ogni partizione.
- Quando si inserisce un valore nei tipi di dati spaziali di SQL Server (GEOGRAPHY e GEOMETRY), è possibile ignorare la proprietà SRID (Spatial Reference System Identifier) o specificare un numero diverso. Quando si replicano tabelle con tipi di dati spaziali, AWS DMS sostituisce lo SRID con lo SRID predefinito (0 per GEOMETRY e 4326 per GEOGRAPHY).
- Se il database non è configurato per MS-REPLICATION o MS-CDC, è comunque possibile acquisire tabelle che non dispongono di una chiave primaria, ma vengono acquisiti solo gli eventi INSERT/DELETE DML. Gli eventi UPDATE e TRUNCATE TABLE vengono ignorati.
- Gli indici Columnstore non sono supportati.
- Le tabelle ottimizzate per la memoria (utilizzando OLTP in memoria) non sono supportate.
- Quando si replica una tabella con una chiave primaria costituita da più colonne, l'aggiornamento delle colonne Chiave primaria durante il pieno carico non è supportato.
- La durata ritardata non è supportata.
- L'impostazione dell'endpoint `readBackupOnly=Y` (attributo aggiuntivo di connessione) non funziona sulle istanze di origine di RDS per SQL Server a causa del modo in cui RDS esegue i backup.
- EXCLUSIVE_AUTOMATIC_TRUNCATION non funziona sulle istanze di origine di Amazon RDS per SQL Server perché gli utenti RDS non hanno accesso all'esecuzione della stored procedure di SQL Server `sp_rep1done`.
- AWS DMS non acquisisce i comandi truncate.
- AWS DMS non supporta la replica da database con il ripristino accelerato del database (ADR) attivato.
- AWS DMS non supporta l'acquisizione di istruzioni DDL (Data Definition Language) e DML (Data Manipulation Language) all'interno di una singola transazione.
- AWS DMS non supporta la replica di pacchetti applicativi a livello di dati (DACPAC).

- Le istruzioni UPDATE che coinvolgono chiavi primarie o indici univoci e aggiornano più righe di dati possono causare conflitti quando si applicano modifiche al database di destinazione. Ad esempio, quando il database di destinazione applica gli aggiornamenti come istruzioni INSERT e DELETE anziché tramite una singola istruzione UPDATE. Con la modalità di applicazione ottimizzata in batch, la tabella può essere ignorata. Con la modalità di applicazione transazionale, l'operazione UPDATE può comportare violazioni dei vincoli. Per evitare questo problema, ricarica la tabella pertinente. In alternativa, individua i record problematici nella tabella di controllo Applica eccezioni (`dmslogs.aws_dms_apply_exceptions`) e modificali manualmente nel database di destinazione. Per ulteriori informazioni, consulta [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).
- AWS DMS non supporta la replica di tabelle e schemi, in cui il nome include un carattere speciale del set seguente.

```
\\ -- \n \" \b \r ' \t ;
```

- Il mascheramento dei dati non è supportato. AWS DMS migra i dati mascherati senza mascheramento.
- AWS DMS replica fino a 32.767 tabelle con chiavi primarie e fino a 1.000 colonne per ogni tabella. Questo perché AWS DMS crea un articolo di replica di SQL Server per ogni tabella replicata e gli articoli di replica di SQL Server presentano queste limitazioni.
- Quando si utilizza l'acquisizione dei dati di modifica (CDC), è necessario definire tutte le colonne che compongono un indice univoco come NOT NULL. Se questo requisito non viene soddisfatto, viene restituito l'errore di sistema 22838 di SQL Server.

Quando si accede ai log delle transazioni di backup si applicano le seguenti limitazioni:

- I backup crittografati non sono supportati.
- I backup archiviati in un URL o in Windows Azure non sono supportati.
- AWS DMS non supporta l'elaborazione diretta dei backup dei log delle transazioni a livello di file da cartelle condivise alternative.

Autorizzazioni per attività solo pieno carico

Le seguenti autorizzazioni sono necessarie per eseguire le attività solo pieno carico. Tieni presente che AWS DMS non crea l'`dms_user` accesso. Per informazioni sulla creazione di un accesso per SQL Server, consulta [Creazione di un utente di database con Microsoft SQL Server](#).

```
USE db_name;

CREATE USER dms_user FOR LOGIN dms_user;
ALTER ROLE [db_datareader] ADD MEMBER dms_user;
GRANT VIEW DATABASE STATE to dms_user ;

USE master;

GRANT VIEW SERVER STATE TO dms_user;
```

Prerequisiti per l'utilizzo della replica continua (CDC) da un'origine SQL Server

Puoi utilizzare la replica continua (acquisizione dei dati di modifica o CDC) per un database autogestito di SQL Server on-premise o su Amazon EC2 oppure per un database cloud come Amazon RDS o un'istanza gestita da Microsoft Azure SQL.

I seguenti requisiti si applicano specificamente quando si usa la replica continua con un database SQL Server come origine per AWS DMS:

- SQL Server deve essere configurato per i backup completi ed è necessario eseguire un backup prima di iniziare la replica dei dati.
- Il modello di ripristino deve essere impostato su Bulk logged o su Full.
- Il backup di SQL Server su più dischi non è supportato. Se il backup è definito per scrivere il backup del database su più file su dischi diversi, non è AWS DMS possibile leggere i dati e l' AWS DMS operazione ha esito negativo.
- Per le origini SQL Server autogestite, le definizioni di SQL Server Replication Publisher per l'origine utilizzata in un'attività di CDC DMS non vengono rimosse quando si rimuove l'attività. Un amministratore di sistema di SQL Server deve eliminare queste definizioni da SQL Server per le origini gestite dal cliente.
- Durante CDC, AWS DMS deve cercare i backup del registro delle transazioni di SQL Server per leggere le modifiche. AWS DMS non supporta i backup dei log delle transazioni di SQL Server creati utilizzando software di backup di terze parti che non sono in formato nativo. Per supportare i backup dei log delle transazioni che sono in formato nativo e creati utilizzando software di backup di terze parti, aggiungi l'attributo di connessione `use3rdPartyBackupDevice=Y` all'endpoint di origine.
- Per le origini SQL Server gestite dal cliente, tenere presente che SQL Server non acquisisce le modifiche su nuove tabelle create finché non vengono pubblicate. Quando le tabelle vengono

aggiunte a un'origine SQL Server, AWS DMS gestisce la creazione della pubblicazione. Tuttavia il processo potrebbe richiedere alcuni minuti. Le operazioni effettuate sulle nuove tabelle create durante il ritardo non vengono acquisite o replicate nella destinazione.

- AWS DMS l'acquisizione dei dati di modifica richiede l'attivazione della registrazione completa delle transazioni in SQL Server. Per attivare il log completo delle transazioni in SQL Server, abilita la replica MS-REPLICATION o l'acquisizione dei dati di modifica (CDC).
- Le voci tlog di SQL Server non vengono contrassegnate per il riutilizzo finché il processo CDC MS non elabora le modifiche.
- Le operazioni CDC non sono supportate su tabelle ottimizzate per la memoria. Queste limitazioni si applicano a SQL Server 2014 (quando la funzionalità è stata introdotta per la prima volta) e versioni successive.
- AWS DMS l'acquisizione dei dati di modifica richiede per impostazione predefinita un database di distribuzione su Amazon EC2 o su un server SQL On-Prem come origine. Pertanto assicurati di aver attivato il distributore durante la configurazione della replica MS per tabelle con chiavi primarie.

Acquisizione delle modifiche ai dati per SQL Server autogestito on-premise o su Amazon EC2

Per acquisire le modifiche di un database Microsoft SQL Server di origine, assicurati che il database sia configurato per i backup completi. Configura il database in modalità di ripristino completo o in modalità di registrazione in blocco.

Per un'origine SQL Server autogestita, AWS DMS utilizza quanto segue:

Replica MS-REPLICATION

Per acquisire le modifiche di tabelle con chiavi primarie. È possibile configurarlo automaticamente assegnando i privilegi di amministratore di sistema all'utente dell' AWS DMS endpoint sull'istanza di origine di SQL Server. Oppure puoi seguire i passaggi in questa sezione per preparare l'origine e utilizzare un utente che non dispone dei privilegi di amministratore di sistema per l'endpoint.

AWS DMS

Acquisizione MS-CDC

Per acquisire le modifiche di tabelle senza chiavi primarie. Abilita l'acquisizione MS-CDC a livello di database e per tutte le tabelle singolarmente.

Quando si configura un database SQL Server per la replica continua (CDC), è possibile eseguire una delle seguenti operazioni:

- Configurare la replica continua utilizzando il ruolo sysadmin.
- Configurare la replica continua in modo che non utilizzi il ruolo sysadmin.

Configurazione della replica continua su un SQL Server autogestito

Questa sezione contiene informazioni sulla configurazione della replica continua su un SQL Server autogestito con o senza l'utilizzo del ruolo sysadmin.

Argomenti

- [Configurazione della replica continua su un SQL Server autogestito: utilizzo del ruolo sysadmin](#)
- [Configurazione della replica continua su un SQL Server autonomo: senza il ruolo sysadmin](#)

Configurazione della replica continua su un SQL Server autogestito: utilizzo del ruolo sysadmin

AWS DMS la replica continua per SQL Server utilizza la replica nativa di SQL Server per le tabelle con chiavi primarie e l'acquisizione dei dati delle modifiche (CDC) per le tabelle senza chiavi primarie.

Prima di configurare la replica continua, consulta [Prerequisiti per l'utilizzo della replica continua \(CDC\) da un'origine SQL Server](#).

Per le tabelle con chiavi primarie, in genere AWS DMS è possibile configurare gli artefatti richiesti sull'origine. Tuttavia, per le istanze di origine SQL Server autogestite, assicurati di configurare prima manualmente la distribuzione di SQL Server. Dopo averlo fatto, gli utenti di AWS DMS origine con autorizzazione sysadmin possono creare automaticamente la pubblicazione per le tabelle con chiavi primarie.

Per verificare se la distribuzione è già stata configurata, eseguire il comando seguente.

```
sp_get_distributor
```

Se il risultato è NULL per la distribuzione delle colonne, la distribuzione non è configurata. Puoi utilizzare la procedura seguente per configurare la distribuzione.

Per configurare la distribuzione

1. Connettiti al database di origine SQL Server utilizzando lo strumento SQL Server Management Studio (SSMS).
2. Apri il menu contestuale (pulsante destro del mouse) della cartella Replica, quindi scegli Configura distribuzione. Viene visualizzata la Configurazione guidata della distribuzione.
3. Segui la procedura guidata per immettere i valori predefiniti e creare la distribuzione.

Per configurare CDC

AWS DMS la versione 3.4.7 e successive possono configurare MS CDC per il database e tutte le tabelle automaticamente se non si utilizza una replica di sola lettura. Per usare questa funzionalità, imposta l'attributo aggiuntivo di connessione `SetUpMsCdcForTables` su `true`. Per informazioni sugli attributi aggiuntivi di connessione, consulta [Impostazioni degli endpoint](#).

Per le versioni AWS DMS precedenti alla 3.4.7 o per una replica di sola lettura come origine, procedi nel seguente modo:

1. Per le tabelle senza chiavi primarie, configura l'acquisizione MS-CDC per il database. Per farlo, utilizza un account a cui è assegnato il ruolo `sysadmin` ed esegui il comando seguente.

```
use [DBname]
EXEC sys.sp_cdc_enable_db
```

2. Quindi, configura l'acquisizione MS-CDC per ciascuna delle tabelle di origine. Per ogni tabella con chiavi univoche ma senza una chiave primaria, esegui la seguente query per configurare l'acquisizione MS-CDC.

```
exec sys.sp_cdc_enable_table
@source_schema = N'schema_name',
@source_name = N'table_name',
@index_name = N'unique_index_name',
@role_name = NULL,
@supports_net_changes = 1
GO
```

3. Per ogni tabella senza una chiave primaria né chiavi univoche, esegui la seguente query per configurare l'acquisizione MS-CDC.

```
exec sys.sp_cdc_enable_table
```

```
@source_schema = N'schema_name',  
@source_name = N'table_name',  
@role_name = NULL  
GO
```

Per ulteriori informazioni sulla configurazione di MS-CDC per tabelle specifiche, consulta la [documentazione di SQL Server](#).

Configurazione della replica continua su un SQL Server autonomo: senza il ruolo sysadmin

Per informazioni sulla configurazione della replica continua su un SQL Server autonomo senza il ruolo sysadmin, consulta [Configurazione della replica continua su un SQL Server autonomo senza il ruolo sysadmin](#).

Configurazione della replica continua su un'istanza database di SQL Server nel cloud

In questa sezione viene descritto come configurare CDC su un'istanza database SQL Server ospitata nel cloud. Un'istanza SQL Server ospitata nel cloud è un'istanza in esecuzione su Amazon RDS per SQL Server, un'istanza gestita da Azure SQL o qualsiasi altra istanza gestita da SQL Server nel cloud. Per informazioni sulle limitazioni alla replica continua per ogni tipo di database, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Prima di configurare la replica continua, consulta [Prerequisiti per l'utilizzo della replica continua \(CDC\) da un'origine SQL Server](#).

Diversamente dalle origini Microsoft SQL Server autogestite, Amazon RDS per SQL Server non supporta MS-Replication. Pertanto, AWS DMS deve utilizzare MS-CDC per le tabelle con o senza chiavi primarie.

Amazon RDS non concede i privilegi di amministratore di sistema per l'impostazione degli artefatti di replica da AWS DMS utilizzare per le modifiche in corso in un'istanza di SQL Server di origine. Assicurati di attivare l'acquisizione MS-CDC per l'istanza Amazon RDS (utilizzando i privilegi di utente master) come indicato nella procedura seguente.

Per attivare l'acquisizione MS-CDC per un'istanza database SQL Server nel cloud

1. Esegui una delle seguenti query a livello di database.

Utilizza questa query per un'istanza database RDS per SQL Server.

```
exec msdb.dbo.rds_cdc_enable_db 'DB_name'
```

Utilizza questa query per un'istanza database gestita da Azure SQL.

```
USE DB_name  
GO  
EXEC sys.sp_cdc_enable_db  
GO
```

2. Per ogni tabella con una chiave primaria, esegui la seguente query per attivare l'acquisizione MS-CDC.

```
exec sys.sp_cdc_enable_table  
@source_schema = N'schema_name',  
@source_name = N'table_name',  
@role_name = NULL,  
@supports_net_changes = 1  
GO
```

Per ogni tabella con chiavi univoche ma senza una chiave primaria, esegui la seguente query per attivare l'acquisizione MS-CDC.

```
exec sys.sp_cdc_enable_table  
@source_schema = N'schema_name',  
@source_name = N'table_name',  
@index_name = N'unique_index_name',  
@role_name = NULL,  
@supports_net_changes = 1  
GO
```

Per ogni tabella senza una chiave primaria né chiavi univoche, esegui la seguente query per attivare l'acquisizione MS-CDC.

```
exec sys.sp_cdc_enable_table  
@source_schema = N'schema_name',  
@source_name = N'table_name',  
@role_name = NULL  
GO
```

3. Imposta la disponibilità del periodo di conservazione delle modifiche sull'origine utilizzando il seguente comando.

```
use dbname
EXEC sys.sp_cdc_change_job @job_type = 'capture' ,@pollinginterval = 86399
exec sp_cdc_stop_job 'capture'
exec sp_cdc_start_job 'capture'
```

Il parametro `@pollinginterval` viene misurato in secondi con un valore consigliato impostato su 86399. Ciò significa che il log delle transazioni mantiene le modifiche per 86.399 secondi (un giorno) quando `@pollinginterval = 86399`. La procedura `exec sp_cdc_start_job 'capture'` avvia le impostazioni.

Note

In alcune versioni di SQL Server, se il valore di `pollinginterval` è impostato su più di 3599 secondi, viene ripristinato a cinque secondi predefiniti. Quando ciò accade, le voci T-Log vengono eliminate prima di poterle leggere. AWS DMS Per determinare quali versioni di SQL Server sono interessate da questo problema noto, consulta [questo articolo della Knowledge Base di Microsoft](#).

Se utilizzi Amazon RDS con Multi-AZ, assicurati di impostare anche la versione secondaria in modo che abbia i valori corretti in caso di failover.

```
exec rdsadmin..rds_set_configuration 'cdc_capture_pollinginterval' , 86399
```

Se un'attività di AWS DMS replica che acquisisce le modifiche in corso all'origine di SQL Server si interrompe per più di un'ora, utilizzare la procedura seguente.

Per mantenere il periodo di conservazione durante un' AWS DMS attività di replica

1. Arresta il processo di troncamento dei log delle transazioni utilizzando il comando seguente.

```
exec sp_cdc_stop_job 'capture'
```

2. Trova l'attività sulla AWS DMS console e riprendila.
3. Scegli la scheda Monitoraggio e seleziona il parametro `CDCLatencySource`.

- Una volta che il parametro `CDCLatencySource` è uguale a 0 (zero) e si stabilizza su tale valore, riavvia l'attività che tronca i log delle transazioni utilizzando il seguente comando.

```
exec sp_cdc_start_job 'capture'
```

Ricordati di avviare il processo che tronca i log delle transazioni di SQL Server. In caso contrario, lo spazio di storage dell'istanza SQL Server potrebbe esaurirsi.

Limitazioni per la replica continua su un'istanza database SQL Server nel cloud

- AWS DMS supporta la replica in corso (CDC) solo con il registro delle transazioni attivo. Non è possibile utilizzare il log dei backup con CDC.
- È possibile perdere gli eventi se si spostano dal log delle transazioni attivo al log dei backup o li tronchi dal log delle transazioni attivo.

Impostazioni consigliate per l'utilizzo di Amazon RDS for SQL Server come origine per AWS DMS

Quando utilizzi Amazon RDS per SQL Server come origine, il processo di acquisizione si basa sui parametri `maxscans` e `maxtrans`. Questi parametri determinano il numero massimo di scansioni eseguite dall'acquisizione nel log delle transazioni e il numero di transazioni elaborate per ogni scansione.

Per i database in cui il numero di transazioni è superiore a `maxtrans*maxscans`, l'aumento del valore di `polling_interval` può causare un accumulo di record del log delle transazioni attivo. Questo accumulo può, a sua volta, portare a un aumento delle dimensioni del log delle transazioni.

Tieni presente che AWS DMS non si basa sul processo di acquisizione MS-CDC. Il processo di acquisizione MS-CDC contrassegna le voci del log delle transazioni come elaborate. Ciò consente al processo di backup del log delle transazioni di rimuovere le voci dal log delle transazioni.

Si consiglia di monitorare la dimensione del log delle transazioni e l'esito dei processi di acquisizione MS-CDC. Se i job MS-CDC falliscono, il log delle transazioni potrebbe crescere eccessivamente e causare errori di replica. AWS DMS È possibile monitorare gli errori del processo di acquisizione MS-CDC utilizzando la vista di gestione dinamica `sys.dm_cdc_errors` nel database di origine. È possibile monitorare la dimensione del log delle transazioni utilizzando il comando di gestione `DBCC SQLPERF (LOGSPACE)`.

Per risolvere l'aumento delle dimensioni del log delle transazioni causato dall'acquisizione MS-CDC

1. Verificate la provenienza Log Space Used % da cui AWS DMS viene eseguita la replica del database e verificate che aumenti continuamente.

```
DBCC SQLPERF(LOGSPACE)
```

2. Identifica cosa blocca il processo di backup del log delle transazioni.

```
Select log_reuse_wait, log_reuse_wait_desc, name from sys.databases where name = db_name();
```

Se il valore `log_reuse_wait_desc` è uguale a `REPLICATION`, la conservazione del backup del log è causata dalla latenza dell'acquisizione MS-CDC.

3. Aumenta il numero di eventi elaborati dal processo di acquisizione incrementando i valori dei parametri `maxtrans` e `maxscans`.

```
EXEC sys.sp_cdc_change_job @job_type = 'capture' ,@maxtrans = 5000, @maxscans = 20  
exec sp_cdc_stop_job 'capture'  
exec sp_cdc_start_job 'capture'
```

Per risolvere questo problema, imposta i valori di `maxscans` e `maxtrans` in modo che `maxtrans*maxscans` siano uguali al numero medio di eventi generati per le tabelle AWS DMS replicate dal database di origine per ogni giorno.

Se imposti questi parametri su un valore superiore a quello consigliato, i processi di acquisizione elaborano tutti gli eventi nei log delle transazioni. Se si impostano questi parametri su un valore inferiore a quello consigliato, la latenza dell'acquisizione MS-CDC aumenta e il log delle transazioni incrementa le dimensioni.

L'identificazione dei valori appropriati per `maxscans` e `maxtrans` può essere difficile perché le modifiche del carico di lavoro producono un numero variabile di eventi. In questo caso, consigliamo di configurare il monitoraggio della latenza dell'acquisizione MS-CDC. Per ulteriori informazioni, consulta [Monitorare il processo](#) nella documentazione di SQL Server. Quindi configura `maxtrans` e `maxscans` in modo dinamico in base ai risultati del monitoraggio.

Se l'AWS DMS attività non riesce a trovare i numeri di sequenza di registro (LSN) necessari per riprendere o continuare l'attività, l'operazione potrebbe non riuscire e richiedere un ricaricamento completo.

Note

Quando si utilizza AWS DMS per replicare i dati da un'origine RDS per SQL Server, è possibile che si verifichino errori nel tentativo di riprendere la replica dopo un evento di stop-start dell'istanza Amazon RDS. Ciò è dovuto al fatto che il processo di SQL Server Agent riavvia il processo di acquisizione quando viene riavviato dopo l'evento di arresto e avvio. Questo processo ignora l'intervallo di polling dell'acquisizione MS-CDC.

Per questo motivo, nei database con volumi di transazioni inferiori all'elaborazione del processo di acquisizione MS-CDC, ciò può causare l'elaborazione o la marcatura dei dati come replicati e di backup prima che AWS DMS possano riprendere da dove si era interrotta, con il seguente errore:

```
[SOURCE_CAPTURE ]E: Failed to access LSN '0000dbd9:0006f9ad:0003' in
the backup log sets since BACKUP/LOG-s are not available. [1020465]
(sqlserver_endpoint_capture.c:764)
```

Per mitigare questo problema, imposta i valori `maxtrans` e `maxscans` come consigliato in precedenza.

Metodi di compressione supportati per SQL Server

Tieni presente le seguenti informazioni sul supporto per i metodi di compressione di SQL Server in AWS DMS:

- AWS DMS supporta la compressione Row/Page in SQL Server versione 2008 e successive.
- AWS DMS non supporta il formato di archiviazione Vardecimal.
- AWS DMS non supporta colonne sparse e compressione della struttura colonnare.

Utilizzo di gruppi di disponibilità di SQL Server autogestiti AlwaysOn

I gruppi di disponibilità Always On di SQL Server forniscono disponibilità elevata e ripristino di emergenza come alternativa a livello aziendale al mirroring del database.

In AWS DMS, è possibile migrare le modifiche da una singola replica del gruppo di disponibilità primario o secondario.

Utilizzo della replica del gruppo di disponibilità principale

Per utilizzare il gruppo di disponibilità primario come origine in AWS DMS, procedi come segue:

1. Attiva l'opzione di distribuzione in tutte le istanze SQL Server nelle repliche di disponibilità. Per ulteriori informazioni, consulta [Configurazione della replica continua su un SQL Server autogestito](#).
2. Nella AWS DMS console, apri le impostazioni del database di origine di SQL Server. Per Nome server, specifica il nome DNS (Domain Name Service) o l'indirizzo IP configurato per l'ascoltatore del gruppo di disponibilità.

Quando si avvia un' AWS DMS attività per la prima volta, l'avvio potrebbe richiedere più tempo del solito. Ciò avviene perché la creazione degli articoli della tabella viene duplicata dal server dei gruppi di disponibilità.

Utilizzo della replica del gruppo di disponibilità secondario

Per utilizzare un gruppo di disponibilità secondario come fonte in AWS DMS, procedi come segue:

1. Utilizzate le stesse credenziali utilizzate dall'utente dell'endpoint di AWS DMS origine per la connessione a singole repliche.
2. Assicurati che l'istanza di AWS DMS replica sia in grado di risolvere i nomi DNS per tutte le repliche esistenti e di connettersi ad esse. È possibile utilizzare la seguente query SQL per ottenere i nomi DNS per tutte le repliche.

```
select ar.replica_server_name, ar.endpoint_url from sys.availability_replicas ar
JOIN sys.availability_databases_cluster adc
ON adc.group_id = ar.group_id AND adc.database_name = '<source_database_name>';
```

3. Quando crei l'endpoint di origine, specifica il nome DNS dell'ascoltatore del gruppo di disponibilità per il nome del server dell'endpoint o per l'indirizzo del server del segreto dell'endpoint. Per ulteriori informazioni sugli ascoltatori del gruppo di disponibilità, consulta [Che cos'è un ascoltatore del gruppo di disponibilità?](#) nella documentazione di SQL Server.

È possibile utilizzare un server DNS pubblico o un server DNS on-premise per risolvere l'ascoltatore del gruppo di disponibilità, la replica principale e le repliche secondarie. Per

utilizzare un server DNS on-premise, configura il risolutore Amazon Route 53. Per ulteriori informazioni, consulta [Utilizzo del server dei nomi in locale](#).

4. Aggiungi i seguenti attributi aggiuntivi di connessione all'endpoint di origine.

Attributo aggiuntivo di connessione	Valore	Note
<code>applicationIntent</code>	<code>ReadOnly</code>	Senza questa impostazione ODBC, l'attività di replica viene indirizzata alla replica del gruppo di disponibilità principale. Per ulteriori informazioni, consulta Supporto client SQL Server nativo per disponibilità elevata e ripristino di emergenza nella documentazione di SQL Server.
<code>multiSubnetFailover</code>	<code>yes</code>	Per ulteriori informazioni, consulta Supporto client SQL Server nativo per disponibilità elevata e ripristino di emergenza nella documentazione di SQL Server.
<code>alwaysOnSharedBackupIsEnabled</code>	<code>false</code>	Per ulteriori informazioni, consulta Impostazioni degli endpoint quando si utilizza SQL Server come origine per AWS DMS .
<code>activateSafeguard</code>	<code>false</code>	Per ulteriori informazioni, consulta la sezione seguente: Limitazioni .
<code>setUpMsDcForTables</code>	<code>false</code>	Per ulteriori informazioni, consulta la sezione seguente: Limitazioni .

5. Abilita l'opzione di distribuzione in tutte le repliche del gruppo di disponibilità. Aggiungi tutti i nodi all'elenco dei distributori. Per ulteriori informazioni, consulta [Per configurare la distribuzione](#).
6. Esegui la seguente query sulla replica principale di lettura/scrittura per abilitare la pubblicazione del database. Questa query viene eseguita una sola volta per il database.

```
sp_replicationdboption @dbname = N'<source DB name>', @optname = N'publish', @value  
= N'true';
```

Limitazioni

Di seguito sono riportate le limitazioni per l'utilizzo di una replica del gruppo di disponibilità secondario:

- AWS DMS non supporta Safeguard quando utilizza una replica del gruppo di disponibilità di sola lettura come origine. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza SQL Server come origine per AWS DMS](#).
- AWS DMS non supporta l'attributo di connessione `setUpMsCdcForTables` extra quando utilizza una replica del gruppo di disponibilità di sola lettura come origine. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza SQL Server come origine per AWS DMS](#).
- AWS DMS può utilizzare una replica del gruppo di disponibilità secondario autogestita come database di origine per la replica continua (change data capture o CDC) a partire dalla versione 3.4.7. Le repliche di lettura multi-AZ di SQL Server nel cloud non sono supportate. Se utilizzi versioni precedenti di AWS DMS, assicurati di utilizzare la replica del gruppo di disponibilità principale come database di origine per CDC.

Failover su altri nodi

Se imposti l'attributo di connessione `ApplicationIntent` aggiuntivo per l'endpoint `suReadOnly`, l'AWS DMS attività si connette al nodo di sola lettura con la priorità di routing di sola lettura più alta. Quindi esegue il failover su altri nodi di sola lettura del gruppo di disponibilità quando il nodo di sola lettura con la priorità più alta non è disponibile. Se non lo imposti `ApplicationIntent`, l'AWS DMS attività si connette solo al nodo primario (lettura/scrittura) del gruppo di disponibilità.

Requisiti di sicurezza quando si utilizza SQL Server come origine per AWS Database Migration Service

L'account AWS DMS utente deve avere almeno il ruolo `db_owner` utente nel database di origine di SQL Server a cui ci si sta connettendo.

Impostazioni degli endpoint quando si utilizza SQL Server come origine per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine SQL Server in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in [AWS CLI](#), con la sintassi `--microsoft-sql-server-settings '{"EndpointSetting": "value", ...}'` JSON.

Nella tabella seguente vengono elencate le impostazioni degli endpoint che è possibile utilizzare con SQL Server come origine.

Nome	Descrizione
ActivateSafeguard	<p>Questo attributo attiva o disattiva la protezione. Per informazioni sulla protezione, consulta Safeguard Policy .</p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>{false, true}</code></p> <p>Esempio: <code>'{"ActivateSafeguard": true}'</code></p>
AlwaysOnSharedSync hedBackupIsEnabled	<p>Questo attributo regola il comportamento AWS DMS durante la migrazione da un database di origine di SQL Server ospitato come parte di un cluster di gruppi di disponibilità Always On.</p> <p>AWS DMS ha migliorato il supporto per i database di origine di SQL Server configurati per l'esecuzione in un cluster Always On. In questo caso, AWS DMS tenta di verificare se i backup delle transazioni vengono eseguiti da nodi del cluster Always On diversi dal nodo in cui è ospitata l'istanza del database di origine. All'avvio dell'attività di migrazione, AWS DMS tenta di connettersi a ogni nodo del cluster, ma fallisce se non riesce a connettersi a nessuno dei nodi.</p>

Nome	Descrizione
	<p>Se devi AWS DMS eseguire il polling di tutti i nodi del cluster Always On per i backup delle transazioni, imposta questo attributo su. <code>false</code></p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>true</code> o <code>false</code></p> <p>Esempio: <code>'{"AlwaysOnSharedSynchedBackupIsEnabled": false}'</code></p>
<p><code>"ApplicationIntent": "readonly"</code></p>	<p>Questa impostazione dell'attributo del driver ODBC consente a SQL Server di indirizzare l'attività di replica al nodo di sola lettura con la priorità più alta. Senza questa impostazione, SQL Server indirizza l'attività di replica al nodo di lettura-scrittura principale.</p>
<p><code>EnableNonSysadminWrapper</code></p>	<p>Utilizza questa impostazione degli endpoint quando configuri la replica continua su un server SQL autonomo senza un utente sysadmin. Questo parametro è supportato o nella AWS DMS versione 3.4.7 e successive. Per informazioni sulla configurazione della replica continua su un SQL Server autonomo, consulta Configurazione della replica continua su un SQL Server autonomo: senza il ruolo sysadmin.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code></p> <p>Esempio: <code>'{"EnableNonSysadminWrapper": true}'</code></p>
<p><code>ExecuteTimeout</code></p>	<p>Utilizza questo attributo aggiuntivo di connessione per impostare il timeout in secondi dell'istruzione client per l'istanza SQL Server. Il valore predefinito è 60 secondi.</p> <p>Esempio: <code>'{"ExecuteTimeout": 100}'</code></p>

Nome	Descrizione
<code>FatalOnSimpleModel</code>	<p>Se configurata su <code>true</code>, questa impostazione genera un errore irreversibile quando il modello di ripristino del database SQL Server è impostato su <code>simple</code>.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code> o <code>false</code></p> <p>Esempio: <code>'{"FatalOnSimpleModel": true}'</code></p>
<code>ForceLobLookup</code>	<p>Forza la ricerca LOB su un LOB in linea.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code></p> <p>Esempio: <code>'{"ForceLobLookup": false}'</code></p>
<code>"MultiSubnetFailover": "Yes"</code>	<p>Questo attributo del driver ODBC consente a DMS di connettersi al nuovo gruppo principale in caso di failover del gruppo di disponibilità. L'attributo è progettato per situazioni in cui la connessione è interrotta o l'indirizzo IP dell'ascoltatore non è corretto. In queste situazioni, AWS DMS tenta di connettersi a tutti gli indirizzi IP associati al listener del gruppo di disponibilità.</p>

Nome	Descrizione
ReadBackupOnly	<p>L'uso di questo attributo richiede i privilegi sysadmin. Quando questo attributo è impostato su Y, durante la replica in corso AWS DMS legge le modifiche solo dai backup del registro delle transazioni e non legge dal file di registro delle transazioni attivo. L'impostazione di questo parametro su Y consente di controllare l'aumento delle dimensioni del file di log delle transazioni attive durante le attività di caricamento completo e di replica continua. Tuttavia, può aggiungere della latenza di origine alla replica in corso.</p> <p>Valori validi: N o Y. Il valore predefinito è N.</p> <p>Esempio: <code>'{"ReadBackupOnly": Y}'</code></p> <p>Nota: questo parametro non funziona sulle istanze di origine Amazon RDS per SQL Server a causa del modo in cui RDS esegue i backup.</p>

Nome	Descrizione
SafeguardPolicy	<p>Per prestazioni ottimali, AWS DMS tenta di acquisire tutte le modifiche non lette dal registro delle transazioni attivo (TLOG). A volte, tuttavia, a causa dei troncamenti, il TLOG attivo potrebbe non contenere tutte le modifiche non lette. In tal caso, AWS DMS accede al backup del registro per acquisire le modifiche mancanti. Per ridurre al minimo la necessità di accedere al backup del registro, AWS DMS impedisce il troncamento utilizzando uno dei seguenti metodi:</p> <ol style="list-style-type: none">1. <code>RELY_ON_SQL_SERVER_REPLICATION_AGENT</code> (Avvia transazioni nel database): Questa è l'impostazione predefinita per AWS DMS <p>Quando si utilizza questa impostazione, AWS DMS richiede che l'agente di lettura log di SQL Server sia in esecuzione, in modo che AWS DMS possa spostare le transazioni contrassegnate per la replica dal TLOG attivo. Tieni presente che se l'agente di lettura log non è in esecuzione, il TLOG attivo può esaurire lo spazio, facendo sì che il database di origine passi alla modalità di sola lettura fino alla risoluzione del problema. Se è necessario abilitare Microsoft Replication nel database per uno scopo diverso da AWS DMS, è necessario scegliere questa impostazione.</p> <p>Quando si utilizza questa impostazione, AWS DMS riduce al minimo le letture di backup dei log creando una tabella denominata <code>awsdms_truncation_safeguard</code> e impedisce il troncamento di TLOG imitando una transazione aperta nel database. In questo modo si evita che il database tronchi gli eventi e li sposti nel log di backup per cinque minuti (per impostazione predefinita). Assicurati che la tabella non sia inclusa in nessun piano di manutenzione, poiché</p>

Nome	Descrizione
	<p>potrebbe causare l'esito negativo del processo di manutenzione. È possibile eliminare la tabella in modo sicuro se non ci sono attività configurate con l'opzione di database <code>Start Transactions</code> .</p> <p>2. <code>EXCLUSIVE_AUTOMATIC_TRUNCATION</code> (Utilizzabile esclusivamente <code>sp_repldone</code> con una singola attività): quando si utilizza questa impostazione, AWS DMS ha il pieno controllo del processo dell'agente di replica che contrassegna le voci di registro come utilizzate. <code>ready for truncation sp_repldone</code> Con questa impostazione, AWS DMS non utilizza una transazione fittizia come con l'impostazione <code>RELY_ON_SQL_SERVER_REPLICATION_AGENT</code> (predefinita). È possibile utilizzare questa impostazione solo quando MS Replication non viene utilizzato per scopi diversi dal database AWS DMS di origine. Inoltre, quando si utilizza questa impostazione, solo un' AWS DMS attività può accedere al database. Se è necessario eseguire AWS DMS attività parallele sullo stesso database, utilizzare <code>RELY_ON_SQL_SERVER_REPLICATION_AGENT</code> .</p> <ul style="list-style-type: none"> • Questa impostazione richiede che l'agente di lettura log sia arrestato nel database. Se il Log Reader Agent è in esecuzione all'avvio dell' AWS DMS attività, quest'ultima ne forzerà l'interruzione. In alternativa, è possibile arrestare l'agente di lettura log manualmente prima di iniziare l'attività. • Quando si utilizza questo metodo con l'acquisizione MS-CDC, è necessario arrestare e disabilitare i processi di acquisizione MS-CDC e pulizia dell'acquisizione MS-CDC. • Non è possibile utilizzare questa impostazione quando il processo di migrazione di Microsoft SQL Server viene eseguito su un computer Distribut

Nome	Descrizione
	<p>or remoto, poiché AWS DMS non ha accesso al computer remoto.</p> <ul style="list-style-type: none"> • <code>EXCLUSIVE_AUTOMATIC_TRUNCATION</code> non funziona sulle istanze di origine Amazon RDS per SQL Server perché gli utenti di Amazon RDS non hanno accesso per eseguire la stored procedure <code>sp_repldone</code> . • Se imposti <code>SafeguardPolicy</code> su <code>EXCLUSIVE_AUTOMATIC_TRUNCATION</code> senza utilizzare il ruolo <code>sysadmin</code>, devi concedere le autorizzazioni per gli oggetti <code>dbo.syscategories</code> e <code>dbo.sysjobs</code> all'utente <code>dmsuser</code>. <p>Valore predefinito: <code>RELY_ON_SQL_SERVER_REPLICATION_AGENT</code></p> <p>Valori validi: <code>{EXCLUSIVE_AUTOMATIC_TRUNCATION , RELY_ON_SQL_SERVER_REPLICATION_AGENT }</code></p> <p>Esempio: <code>'{"SafeguardPolicy": "EXCLUSIVE_AUTOMATIC_TRUNCATION"}'</code></p>

Nome	Descrizione
SetupMsCdcForTables	<p>Questo attributo attiva l'acquisizione MS-CDC per il database di origine e per le tabelle nella mappatura delle attività che non hanno la replica MS abilitata. L'impostazione di questo valore su true esegue la stored procedure <code>sp_cdc_enable_db</code> sul database di origine ed esegue la stored procedure <code>sp_cdc_enable_table</code> su ogni tabella dell'attività in cui non è abilitata la replica MS nel database di origine. Per ulteriori informazioni sull'attivazione della distribuzione, consulta Configurazione della replica continua su un SQL Server autogestito.</p> <p>Valori validi: {true, false}</p> <p>Esempio: '{"SetupMsCdcForTables": true}'</p>
TlogAccessMode	<p>Indica la modalità utilizzata per recuperare i dati CDC.</p> <p>Valore predefinito: PreferTlog</p> <p>Valori validi: BackupOnly , PreferBackup , PreferTlog , TlogOnly</p> <p>Esempio: '{"TlogAccessMode": "PreferTlog"}'</p>
Use3rdPartyBackupDevice	<p>Quando questo attributo è impostato su Y, AWS DMS elabora i backup dei log delle transazioni di terze parti se sono stati creati in formato nativo.</p>

Tipi di dati di origine per SQL Server

La migrazione dei dati che utilizza SQL Server come origine AWS DMS supporta la maggior parte dei tipi di dati di SQL Server. La tabella seguente mostra i tipi di dati di origine di SQL Server supportati durante l'utilizzo AWS DMS e la mappatura predefinita AWS DMS dei tipi di dati.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati SQL Server	AWS DMS tipi di dati
BIGINT	INT8
BIT	BOOLEAN
DECIMAL	NUMERIC
INT	INT4
MONEY	NUMERIC
NUMERIC (p,s)	NUMERIC
SMALLINT	INT2
SMALLMONEY	NUMERIC
TINYINT	UINT1
REAL	REAL4
FLOAT	REAL8
DATETIME	DATETIME
DATETIME2 (SQL Server 2008 e versioni successive)	DATETIME
SMALLDATETIME	DATETIME
DATE	DATE
TIME	TIME
DATETIMEOFFSET	WSTRING

Tipi di dati SQL Server	AWS DMS tipi di dati
CHAR	STRING
VARCHAR	STRING
VARCHAR (max)	<p>CLOB</p> <p>TEXT</p> <p>Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati CLOB per un'attività specifica.</p> <p>Per le tabelle di SQL Server, AWS DMS aggiorna le colonne LOB nella destinazione anche per le istruzioni UPDATE che non modificano il valore della colonna LOB in SQL Server.</p> <p>Durante CDC, AWS DMS supporta i tipi di dati CLOB solo nelle tabelle che includono una chiave primaria.</p>
NCHAR	WSTRING
NVARCHAR (lunghezza)	WSTRING

Tipi di dati SQL Server	AWS DMS tipi di dati
NVARCHAR (max)	<p data-bbox="833 226 943 258">NCLOB</p> <p data-bbox="833 306 938 338">NTEXT</p> <p data-bbox="833 386 1495 659">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso di SupportLobs per un'attività specifica. Per ulteriori informazioni sull'abilitazione del supporto LOB, consulta Impostazione del supporto LOB per i database di origine in un task AWS DMS.</p> <p data-bbox="833 707 1484 926">Per le tabelle di SQL Server, AWS DMS aggiorna le colonne LOB nella destinazione anche per le istruzioni UPDATE che non modificano il valore della colonna LOB in SQL Server.</p> <p data-bbox="833 974 1490 1104">Durante CDC, AWS DMS supporta i tipi di dati CLOB solo nelle tabelle che includono una chiave primaria.</p>
BINARY	BYTES
VARBINARY	BYTES

Tipi di dati SQL Server	AWS DMS tipi di dati
VARBINARY (max)	<p>BLOB</p> <p>IMAGE</p> <p>Per le tabelle di SQL Server, AWS DMS aggiorna le colonne LOB nella destinazione anche per le istruzioni UPDATE che non modificano il valore della colonna LOB in SQL Server.</p> <p>Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati BLOB per un'attività specifica.</p> <p>AWS DMS supporta i tipi di dati BLOB solo nelle tabelle che includono una chiave primaria.</p>
TIMESTAMP	BYTES
UNIQUEIDENTIFIER	STRING
HIERARCHYID	<p>Utilizza HIERARCHYID durante la replica su un endpoint di destinazione SQL Server.</p> <p>Utilizza WSTRING (250) durante la replica su tutti gli altri endpoint di destinazione.</p>

Tipi di dati SQL Server	AWS DMS tipi di dati
XML	<p data-bbox="833 226 943 258">NCLOB</p> <p data-bbox="833 306 1484 527">Per le tabelle di SQL Server, AWS DMS aggiorna le colonne LOB nella destinazione anche per le istruzioni UPDATE che non modificano il valore della colonna LOB in SQL Server.</p> <p data-bbox="833 575 1492 705">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei tipi di dati NCLOB per un'attività specifica.</p> <p data-bbox="833 753 1487 877">Durante CDC, AWS DMS supporta i tipi di dati NCLOB solo nelle tabelle che includono una chiave primaria.</p>
GEOMETRY	<p data-bbox="833 926 1455 1056">Utilizza GEOMETRY durante la replica sugli endpoint di destinazione che supportano questo tipo di dati.</p> <p data-bbox="833 1104 1503 1228">Utilizza CLOB durante la replica sugli endpoint di destinazione che non supportano questo tipo di dati.</p>
GEOGRAPHY	<p data-bbox="833 1278 1479 1409">Utilizza GEOGRAPHY durante la replica sugli endpoint di destinazione che supportano questo tipo di dati.</p> <p data-bbox="833 1457 1503 1581">Utilizza CLOB durante la replica sugli endpoint di destinazione che non supportano questo tipo di dati.</p>

AWS DMS non supporta tabelle che includono campi con i seguenti tipi di dati.

- CURSOR
- SQL_VARIANT

- TABLE

Note

I tipi di dati definiti dall'utente sono supportati secondo il tipo di base. Ad esempio, un tipo di dati definito dall'utente basato su DATETIME viene gestito come tipo di dati DATETIME.

Utilizzo di un database SQL di Azure di Microsoft come origine per AWS DMS

Con AWS DMS, puoi utilizzare un database Microsoft Azure SQL come origine in modo analogo a SQL Server. AWS DMS supporta, come origine, lo stesso elenco di versioni di database che sono valide per SQL Server in esecuzione on-premise o su un'istanza Amazon EC2.

Per ulteriori informazioni, consulta [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#).

Note

AWS DMS non supporta operazioni CDC (Change Data Capture) con il database SQL di Azure.

Utilizzo di un'istanza gestita da Microsoft Azure SQL come origine per AWS DMS

Con AWS DMS, puoi utilizzare un'istanza gestita da Microsoft Azure SQL come origine in modo analogo a SQL Server. AWS DMS supporta, come origine, lo stesso elenco di versioni di database che sono valide per SQL Server in esecuzione on-premise o su un'istanza Amazon EC2.

Per ulteriori informazioni, consulta [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#).

Utilizzo di un server flessibile Microsoft Azure Database per PostgreSQL come origine per AWS DMS

Con AWS DMS, puoi utilizzare il server flessibile Microsoft Azure Database per PostgreSQL come origine più o meno allo stesso modo in cui usi PostgreSQL.

Per informazioni sulle versioni del server flessibile Microsoft Azure Database per PostgreSQL supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Configurazione del server flessibile Microsoft Azure per PostgreSQL per la replica e la decodifica logica

Puoi usare le funzionalità di replica e decodifica logica nel server flessibile Microsoft Azure Database per PostgreSQL durante la migrazione del database.

Per la decodifica logica, DMS utilizza il plug-in `test_decoding` o `pglogical`. Se il plug-in `pglogical` è disponibile su un database PostgreSQL di origine, DMS crea uno slot di replica utilizzando `pglogical`, altrimenti viene utilizzato il plug-in `test_decoding`.

Per configurare il server flessibile Microsoft Azure per PostgreSQL come endpoint di origine per DMS, procedi nel seguente modo:

1. Apri la pagina Parametri del server sul portale.
2. Imposta il parametro del server `wal_level` su `LOGICAL`.
3. Se desideri utilizzare l'estensione `pglogical`, imposta i parametri `shared_preload_libraries` e `azure.extensions` su `pglogical`.
4. Imposta il parametro `max_replication_slots` sul numero massimo di attività DMS che intendi eseguire contemporaneamente. In Microsoft Azure, il valore predefinito per questo parametro è 10. Il valore massimo di questo parametro dipende dalla memoria disponibile dell'istanza PostgreSQL, che consente da 2 a 8 slot di replica per GB di memoria.
5. Imposta il parametro `max_wal_senders` su un valore maggiore di 1. Il parametro `max_wal_senders` imposta il numero di attività simultanee che è possibile eseguire. Il valore predefinito è 10.
6. Imposta il valore del parametro `max_worker_processes` almeno su 16. In caso contrario, è possibile che vengano restituiti errori come i seguenti:

```
WARNING: out of background worker slots.
```

7. Salvare le modifiche. Riavvia il server per applicare le modifiche.
8. Verifica che l'istanza PostgreSQL consenta il traffico di rete proveniente dalla risorsa di connessione.
9. Fornisci le autorizzazioni di replica a un utente esistente o crea un nuovo utente con le autorizzazioni di replica utilizzando i seguenti comandi.
 - Fornisci a un utente esistente le autorizzazioni di replica utilizzando il seguente comando:

```
ALTER USER <existing_user> WITH REPLICATION;
```

- Crea un nuovo utente con le autorizzazioni di replica utilizzando il seguente comando:

```
CREATE USER aws_dms_user PASSWORD 'aws_dms_user_password';  
GRANT azure_pg_admin to aws_dms_user;  
ALTER ROLE aws_dms_user REPLICATION LOGIN;
```

Per ulteriori informazioni sulla replica logica con PostgreSQL, consulta i seguenti argomenti:

- [Abilitazione dell'acquisizione dei dati di modifica \(CDC\) mediante la replica logica](#)
- [Utilizzo dei punti di avvio CDC nativi per impostare un carico CDC di un endpoint di origine PostgreSQL](#)
- [Logical replication and logical decoding in Azure Database for PostgreSQL - Flexible Server](#) nella [documentazione del database di Azure per PostgreSQL](#).

Utilizzo di un server flessibile Microsoft Azure Database per MySQL come origine per AWS DMS

Con AWS DMS, puoi utilizzare il server flessibile Microsoft Azure Database per MySQL come origine più o meno allo stesso modo in cui usi MySQL.

Per informazioni sulle versioni del server flessibile Microsoft Azure Database per MySQL supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Per ulteriori informazioni sull'utilizzo di un database compatibile con MySQL gestito dal cliente con AWS DMS, consulta [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#).

Limitazioni relative all'utilizzo di Azure MySQL come origine per AWS Database Migration Service

- Il valore predefinito per la variabile di sistema del server flessibile Azure MySQL `sql_generate_invisible_primary_key` è ON e il server aggiunge automaticamente una chiave primaria invisibile generata a qualsiasi tabella creata senza una chiave primaria esplicita. AWS DMS non supporta la replica continua per le tabelle MySQL con vincoli di chiave primaria invisibile generata.

Utilizzo di OCI MySQL Heatwave come origine per AWS DMS

Con AWS DMS, puoi usare OCI MySQL Heatwave come origine più o meno allo stesso modo in cui utilizzi MySQL. L'uso di OCI MySQL Heatwave come origine richiede alcune modifiche di configurazione aggiuntive.

Per informazioni sulle versioni di OCI MySQL Heatwave supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Configurazione di OCI MySQL Heatwave per la replica logica

Per configurare l'istanza OCI MySQL Heatwave come endpoint di origine per DMS, procedi come segue:

1. Accedi alla console OCI e apri il menu principale a forma di hamburger (≡) nell'angolo in alto a sinistra.
2. Scegli Database e Sistemi DB.
3. Apri il menu Configurazioni.
4. Scegliere Create configuration (Crea configurazione).
5. Immetti un nome per la configurazione, ad esempio **dms_configuration**.
6. Scegli la forma della tua attuale istanza OCI MySQL Heatwave. Puoi trovare la forma nella scheda delle proprietà di configurazione del sistema database dell'istanza nella sezione Configurazione del sistema database: forma.
7. Nella sezione Variabili dell'utente scegli la variabile di sistema `binlog_row_value_options`. Il valore predefinito è `PARTIAL_JSON`. Cancella il valore.
8. Scegli il pulsante Crea.
9. Apri l'istanza OCI MySQL Heatwave e scegli il pulsante Modifica.

10. Nella sezione Configurazione seleziona il pulsante Cambia configurazione e scegli la configurazione della forma che hai creato nel passaggio 4.
11. Quando le modifiche diventano effettive, l'istanza è pronta per la replica logica.

Utilizzo di Google Cloud per MySQL come origine per AWS DMS

Con AWS DMS, puoi usare Google Cloud per MySQL come origine più o meno allo stesso modo in cui utilizzi MySQL.

Per informazioni sulle versioni di GCP MySQL supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Per ulteriori informazioni, consulta [Utilizzo di un database compatibile con MySQL come origine per AWS DMS](#).

Note

Il supporto per GCP MySQL 8.0 come origine è disponibile in AWS DMS versione 3.4.6. AWS DMS non supporta la modalità `SSL verify-full` per GCP per le istanze MySQL. L'impostazione di sicurezza GCP MySQL `Allow only SSL connections` non è supportata poiché richiede la verifica del certificato del server e del client. AWS DMS supporta solo la verifica dei certificati del server.

AWS DMS supporta il valore predefinito `CRC32` di GCP CloudSQL per MySQL per il flag del database `binlog_checksum`.

Utilizzo di Google Cloud per PostgreSQL come origine per AWS DMS

Con AWS DMS, puoi utilizzare Google Cloud per PostgreSQL come origine più o meno allo stesso modo in cui usi i database PostgreSQL autogestiti.

Per informazioni sulle versioni di GCP PostgreSQL supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Per ulteriori informazioni, consulta [Utilizzo di un database PostgreSQL come origine AWS DMS](#).

Configurazione di Google Cloud per PostgreSQL per la replica e la decodifica logica

Puoi utilizzare le funzionalità di replica e decodifica logica in Google Cloud SQL per PostgreSQL durante la migrazione del database.

Per la decodifica logica, DMS utilizza uno dei seguenti plug-in:

- `test_decoding`
- `pglogical`

Se il plug-in `pglogical` è disponibile su un database PostgreSQL di origine, DMS crea uno slot di replica utilizzando `pglogical`, altrimenti viene utilizzato il plug-in `test_decoding`.

Tieni presenti le seguenti indicazioni quando usi la decodifica logica con AWS DMS:

1. Con Google Cloud SQL per PostgreSQL, abilita la decodifica logica impostando il flag `cloudsql.logical_decoding` su `on`.
2. Per abilitare `pglogical`, imposta il flag `cloudsql.enable_pglogical` su `on` e riavvia il database.
3. Per utilizzare le funzionalità di decodifica logica, crea un utente PostgreSQL con l'attributo `REPLICATION`. Quando usi l'estensione `pglogical` l'utente deve avere il ruolo `cloudsqlsuperuser`. Per creare un utente con il ruolo `cloudsqlsuperuser`, procedi come indicato di seguito:

```
CREATE USER new_aws_dms_user WITH REPLICATION
IN ROLE cloudsqlsuperuser LOGIN PASSWORD 'new_aws_dms_user_password';
```

Per impostare questo attributo su un utente esistente, completa queste operazioni:

```
ALTER USER existing_user WITH REPLICATION;
```

4. Imposta il parametro `max_replication_slots` sul numero massimo di attività DMS che intendi eseguire contemporaneamente. In Google Cloud SQL, il valore predefinito per questo parametro è 10. Il valore massimo di questo parametro dipende dalla memoria disponibile dell'istanza PostgreSQL, che consente da 2 a 8 slot di replica per GB di memoria.

Per ulteriori informazioni sulla replica logica con PostgreSQL, consulta i seguenti argomenti:

- [Abilitazione dell'acquisizione dei dati di modifica \(CDC\) mediante la replica logica](#)
- [Utilizzo dei punti di avvio CDC nativi per impostare un carico CDC di un endpoint di origine PostgreSQL](#)
- [Configurazione di replica e decodifica logiche](#) nella [documentazione di Cloud SQL per PostgreSQL](#).

Utilizzo di un database PostgreSQL come origine AWS DMS

È possibile migrare i dati da uno o più database PostgreSQL utilizzando AWS DMS. Con un database PostgreSQL come origine, puoi eseguire la migrazione dei dati a un altro database PostgreSQL o a uno degli altri database supportati.

Per informazioni sulle versioni di PostgreSQL supportate come sorgente, AWS DMS consulta [Fonti per AWS DMS](#)

AWS DMS supporta PostgreSQL per questi tipi di database:

- Database locali
- Database su un'istanza Amazon EC2
- Database su un'istanza database Amazon RDS
- Database su un'istanza database basata su Amazon Aurora edizione compatibile con PostgreSQL
- Database su un'istanza database basata su Amazon Aurora edizione serverless compatibile con PostgreSQL

Note

DMS supporta Amazon Aurora PostgreSQL serverless V1 come origine per solo pieno carico. Tuttavia puoi usare Amazon Aurora PostgreSQL serverless V2 come origine per le attività di pieno carico, pieno carico e CDC nonché sola CDC.

AWS DMS versione da usare

Usa qualsiasi AWS DMS versione disponibile.

Usa AWS DMS la versione 3.4.3 e successive.

Usa AWS DMS la versione 3.4.7 e successive.

Usa la AWS DMS versione 3.5.1 e successive.

Usa AWS DMS la versione 3.5.3 e successive.

Puoi utilizzare il protocollo Secure Sockets Layer (SSL) per crittografare le connessioni tra l'endpoint PostgreSQL e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint PostgreSQL, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Come requisito di sicurezza aggiuntivo, quando si utilizza PostgreSQL come origine, l'account utente specificato deve essere un utente registrato nel database PostgreSQL.

Per configurare un database PostgreSQL come endpoint di origine, procedi AWS DMS come segue:

- Crea un utente PostgreSQL con le autorizzazioni appropriate per fornire l' AWS DMS accesso al tuo database di origine PostgreSQL.

Note

- Se il database di origine PostgreSQL è autogestito, consulta [Utilizzo di database PostgreSQL autogestiti come sorgente in AWS DMS](#) per ulteriori informazioni.
- Se il database di origine PostgreSQL è gestito da Amazon RDS, consulta [Utilizzo di database PostgreSQL AWS gestiti come sorgente DMS](#) per ulteriori informazioni.

- Crea un endpoint do origine PostgreSQL conforme alla configurazione del database PostgreSQL scelta.
- Crea un'attività o una serie di attività per migrare le tabelle.

Per creare un' full-load-only attività, non è necessaria alcuna ulteriore configurazione dell'endpoint.

Prima di creare un'attività per l'acquisizione dei dati di modifica (un'attività di sola CDC o pieno carico e CDC), consulta [Abilitazione del CDC utilizzando un database PostgreSQL autogestito come sorgente AWS DMS](#) o [Abilitazione del CDC con un' AWS istanza DB PostgreSQL gestita con AWS DMS](#).

Argomenti

- [Utilizzo di database PostgreSQL autogestiti come sorgente in AWS DMS](#)
- [Utilizzo di database PostgreSQL AWS gestiti come sorgente DMS](#)
- [Abilitazione dell'acquisizione dei dati di modifica \(CDC\) mediante la replica logica](#)
- [Utilizzo dei punti di avvio CDC nativi per impostare un carico CDC di un endpoint di origine PostgreSQL](#)
- [Migrazione da PostgreSQL a PostgreSQL utilizzando AWS DMS](#)
- [Migrazione da Babelfish per Amazon Aurora PostgreSQL utilizzando AWS DMS](#)
- [Rimozione di AWS DMS artefatti da un database sorgente PostgreSQL](#)
- [Impostazioni di configurazione aggiuntive quando si utilizza un database PostgreSQL come origine DMS](#)
- [Utilizzo dell'impostazione dell' MapBooleanAsBoolean endpoint PostgreSQL](#)
- [Impostazioni degli endpoint e attributi di connessione aggiuntivi \(ECA\) quando si utilizza PostgreSQL come sorgente DMS](#)
- [Limitazioni all'utilizzo di un database PostgreSQL come origine DMS](#)
- [Tipi di dati di origine per PostgreSQL](#)

Utilizzo di database PostgreSQL autogestiti come sorgente in AWS DMS

Con un database PostgreSQL autogestito come origine, puoi migrare i dati su un altro database PostgreSQL o su uno degli altri database di destinazione supportati da AWS DMS. Il database di origine può essere un database on-premise o un motore autogestito in esecuzione su un'istanza

Amazon EC2. È possibile utilizzare un'istanza database sia per le attività di pieno carico che per l'acquisizione dei dati di modifica (CDC).

Prerequisiti per l'utilizzo di un database PostgreSQL autogestito come sorgente AWS DMS

Prima di migrare i dati da un database di origine PostgreSQL autogestito, procedi come segue:

- Assicurati di utilizzare un database PostgreSQL versione 9.4.x o successiva.
- Per le attività di pieno carico e CDC o le attività di sola CDC, fornisci le autorizzazioni di superuser per l'account utente specificato per il database di origine PostgreSQL. Le autorizzazioni di superuser sono necessarie all'account utente per accedere alle funzioni specifiche della replica nell'origine. Per le attività solo pieno carico, l'account utente richiede le autorizzazioni SELECT sulle tabelle per eseguirne la migrazione.
- Aggiungere l'indirizzo IP del server di AWS DMS replica al file di `pg_hba.conf` configurazione e abilitare la replica e le connessioni socket. Di seguito è riportato un esempio.

```
# Replication Instance
host all all 12.3.4.56/00 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
host replication dms 12.3.4.56/00 md5
```

Il file di configurazione di PostgreSQL `pg_hba.conf` controlla l'autenticazione client. (HBA sta per autenticazione basata su host) Il file è solitamente memorizzato nella directory dei dati del cluster di database.

- Se stai configurando un database come origine per la replica logica usando see AWS DMS [Abilitazione del CDC utilizzando un database PostgreSQL autogestito come sorgente AWS DMS](#)

Note

Alcune AWS DMS transazioni rimangono inattive per qualche tempo prima che il motore DMS le utilizzi nuovamente. Il parametro `idle_in_transaction_session_timeout` in PostgreSQL versione 9.6 e successive consente di mandare in timeout e in errore le transazioni inattive. Non terminare le transazioni inattive quando utilizzi AWS DMS.

Abilitazione del CDC utilizzando un database PostgreSQL autogestito come sorgente AWS DMS

AWS DMS supporta l'acquisizione dei dati di modifica (CDC) mediante la replica logica. Per abilitare la replica logica su un database di origine PostgreSQL autogestito, imposta i seguenti parametri e valori nel file di configurazione `postgresql.conf`:

- Imposta `wal_level = logical`.
- Imposta `max_replication_slots` su un valore maggiore di 1.

Imposta il valore `max_replication_slots` in base al numero di attività che desideri eseguire. Ad esempio, per eseguire cinque attività dovrai impostare un minimo di cinque slot. Gli slot si aprono automaticamente non appena viene avviata un'attività e restano aperti anche quando l'attività non è più in esecuzione. Assicurati di eliminare manualmente gli slot aperti. Tieni presente che DMS rilascia automaticamente gli slot di replica che ha creato quando l'attività viene eliminata.

- Imposta `max_wal_senders` su un valore maggiore di 1.

Il parametro `max_wal_senders` imposta il numero di attività simultanee che è possibile eseguire.

- Il parametro `wal_sender_timeout` termina le connessioni di replica che sono inattive per un tempo maggiore del numero specificato di millisecondi. L'impostazione predefinita per un database PostgreSQL on-premise è di 60.000 millisecondi (60 secondi). L'impostazione del valore su 0 (zero) disabilita il meccanismo di timeout ed è un'opzione valida per DMS.

Quando si imposta `wal_sender_timeout` su un valore diverso da zero, un'attività DMS con CDC richiede un minimo di 10.000 millisecondi (10 secondi) e non riesce se il valore è inferiore a 10.000. Mantieni il valore inferiore a 5 minuti per evitare ritardi durante un failover multi-AZ di un'istanza di replica DMS.

Alcuni parametri sono statici e possono essere impostati solo all'avvio del server. Qualsiasi modifica alle relative voci nel file di configurazione (per un database autogestito) o nel gruppo di parametri di database (per un database RDS per PostgreSQL) viene ignorata fino al riavvio del server. Per ulteriori informazioni, consultare la [documentazione di PostgreSQL](#).

Per ulteriori informazioni sull'abilitazione della CDC, consulta [Abilitazione dell'acquisizione dei dati di modifica \(CDC\) mediante la replica logica](#).

Utilizzo di database PostgreSQL AWS gestiti come sorgente DMS

È possibile utilizzare un'istanza database PostgreSQL AWS gestita come origine per AWS DMS. È possibile eseguire attività di pieno carico e acquisizione dei dati di modifica (CDC) utilizzando un'origine PostgreSQL gestita da AWS.

Prerequisiti per l'utilizzo di un AWS database PostgreSQL gestito come sorgente DMS

Prima di migrare i dati da un database AWS di origine PostgreSQL gestito, procedi come segue:

- Si consiglia di utilizzare un account AWS utente con le autorizzazioni minime richieste per l'istanza DB PostgreSQL come account utente per l'endpoint di origine PostgreSQL per AWS DMS. L'utilizzo di un account master è sconsigliato. L'account deve avere il ruolo `rds_superuser` e il ruolo `rds_replication`. Il ruolo `rds_replication` fornisce le autorizzazioni per gestire gli slot logici e per eseguire lo streaming dei dati utilizzando gli slot logici.

Assicurati di creare diversi oggetti dall'account utente master per l'account che utilizzi. Per informazioni sulla creazione di questi oggetti, consulta [Migrazione di un database Amazon RDS per PostgreSQL senza utilizzare l'account utente master](#).

- Se il database di origine è in un cloud privato virtuale (VPC), seleziona il gruppo di sicurezza VPC che fornisce accesso all'istanza database in cui risiede il database. Ciò è necessario affinché l'istanza di replica DMS si connetta correttamente all'istanza database di origine. Quando il database e l'istanza di replica DMS si trovano nello stesso VPC, aggiungi il gruppo di sicurezza appropriato alle relative regole in entrata.

Note

Alcune AWS DMS transazioni rimangono inattive per qualche tempo prima che il motore DMS le utilizzi nuovamente. Il parametro `idle_in_transaction_session_timeout` in PostgreSQL versione 9.6 e successive consente di mandare in timeout e in errore le transazioni inattive. Non terminare le transazioni inattive quando utilizzi AWS DMS.

Abilitazione del CDC con un' AWS istanza DB PostgreSQL gestita con AWS DMS

AWS DMS supporta CDC sui database Amazon RDS PostgreSQL quando l'istanza DB è configurata per utilizzare la replica logica. La tabella seguente riassume la compatibilità della replica logica di ciascuna versione di PostgreSQL AWS gestita.

Non è possibile utilizzare le repliche di lettura RDS PostgreSQL per CDC (replica continua).

Versione PostgreSQL	AWS DMS supporto a pieno carico	AWS DMS supporto CDC
Aurora PostgreSQL versione 2.1 compatibile con PostgreSQL 10.5 (o versioni precedenti)	Sì	No
Aurora PostgreSQL versione 2.2 compatibile con PostgreSQL 10.6 (o versioni successive)	Sì	Sì
RDS per PostgreSQL compatibile con PostgreSQL 10.21 (o versioni successive)	Sì	Sì

Per abilitare la replica logica per un'istanza database RDS per PostgreSQL

1. Usa l'account utente AWS principale per l'istanza DB PostgreSQL come account utente per l'endpoint di origine PostgreSQL. L'account utente master dispone dei ruoli necessari che consentono di configurare il CDC.

Se utilizzi un account diverso dall'account utente master, è necessario creare diversi oggetti dall'account utente master per l'account che utilizzi. Per ulteriori informazioni, consulta [Migrazione di un database Amazon RDS per PostgreSQL senza utilizzare l'account utente master](#).

2. Imposta il parametro `rds.logical_replication` su 1 nel gruppo di parametri del cluster di database. Questo parametro statico richiede un riavvio dell'istanza database per avere effetto. Come parte dell'applicazione di questo parametro AWS DMS imposta i parametri `wal_level`, `max_wal_senders`, `max_replication_slots` e `max_connections`. Queste modifiche ai parametri possono aumentare la generazione dei WAL (Write Ahead Log), quindi impostare solo `rds.logical_replication` quando si utilizzano slot di replica logica.
3. Il parametro `wal_sender_timeout` termina le connessioni di replica che sono inattive per un tempo maggiore del numero specificato di millisecondi. L'impostazione predefinita per un

database PostgreSQL AWS gestito è 30000 millisecondi (30 secondi). L'impostazione del valore su 0 (zero) disabilita il meccanismo di timeout ed è un'opzione valida per DMS.

Quando si imposta `wal_sender_timeout` su un valore diverso da zero, un'attività DMS con CDC richiede un minimo di 10.000 millisecondi (10 secondi) e non riesce se il valore è compreso tra 0 e 10.000. Mantieni il valore inferiore a 5 minuti per evitare ritardi durante un failover multi-AZ di un'istanza di replica DMS.

4. Assicurati che il valore del parametro `max_worker_processes` nel gruppo di parametri del cluster di database sia uguale o superiore ai valori totali combinati di `max_logical_replication_workers`, `autovacuum_max_workers` e `max_parallel_workers`. Un numero elevato di processi di lavoro in background potrebbe influire sui carichi di lavoro delle applicazioni su istanze di piccole dimensioni. Quindi, monitora le prestazioni del database se imposti un valore di `max_worker_processes` superiore a quello predefinito.
5. Quando si utilizza Aurora PostgreSQL come sorgente con CDC, impostare su `synchronous_commit ON`

Migrazione di un database Amazon RDS per PostgreSQL senza utilizzare l'account utente master

In alcuni casi, si può decidere di non utilizzare l'account utente master per l'istanza di database Amazon RDS PostgreSQL che si sta utilizzando come origine. In questi casi, è necessario creare diversi oggetti per acquisire gli eventi DDL (Data Definition Language). Puoi creare questi oggetti nell'account diverso dall'account master e quindi creare un trigger nell'account utente master.

Note

Se configuri l'impostazione dell'endpoint `captureDDLs` su `false` nell'endpoint di origine, non è necessario creare la tabella e il trigger seguenti nel database di origine.

Per creare questi oggetti, utilizza la procedura seguente.

Per creare oggetti

1. Scegli lo schema in cui devono essere creati gli oggetti. Lo schema predefinito è `public`. Verifica che lo schema esista e che l'account *OtherThanMaster* vi possa accedere.
2. Accedi all'istanza database PostgreSQL utilizzando l'account utente diverso dall'account master, qui l'account *OtherThanMaster*.

3. Crea la tabella `awsdms_ddl_audit` eseguendo il comando seguente, sostituendo *objects_schema* nel codice e il nome dello schema da utilizzare.

```
CREATE TABLE objects_schema.awsdms_ddl_audit
(
  c_key      bigserial primary key,
  c_time     timestamp,      -- Informational
  c_user     varchar(64),    -- Informational: current_user
  c_txn      varchar(16),    -- Informational: current transaction
  c_tag      varchar(24),    -- Either 'CREATE TABLE' or 'ALTER TABLE' or 'DROP TABLE'
  c_oid      integer,       -- For future use - TG_OBJECTID
  c_name     varchar(64),    -- For future use - TG_OBJECTNAME
  c_schema   varchar(64),    -- For future use - TG_SCHEMANAME. For now - holds
  current_schema
  c_ddlqry   text           -- The DDL query associated with the current DDL event
);
```

4. Crea la funzione `awsdms_intercept_ddl` eseguendo il comando seguente, sostituendo *objects_schema* nel codice e il nome dello schema da utilizzare.

```
CREATE OR REPLACE FUNCTION objects_schema.awsdms_intercept_ddl()
  RETURNS event_trigger
LANGUAGE plpgsql
SECURITY DEFINER
AS $$
  declare _qry text;
BEGIN
  if (tg_tag='CREATE TABLE' or tg_tag='ALTER TABLE' or tg_tag='DROP TABLE' or
  tg_tag = 'CREATE TABLE AS') then
    SELECT current_query() into _qry;
    insert into objects_schema.awsdms_ddl_audit
    values
    (
      default,current_timestamp,current_user,cast(TXID_CURRENT()as
      varchar(16)),tg_tag,0,'',current_schema,_qry
    );
    delete from objects_schema.awsdms_ddl_audit;
  end if;
END;
```

```
$$;
```

5. Esci dall'account *OtherThanMaster* e collegati con un account che disponga del ruolo `rds_superuser`.
6. Crea il trigger evento `awsdms_intercept_ddl` utilizzando il seguente comando.

```
CREATE EVENT TRIGGER awsdms_intercept_ddl ON ddl_command_end  
EXECUTE PROCEDURE objects_schema.awsdms_intercept_ddl();
```

7. Assicurati che tutti gli utenti e i ruoli che accedono a questi eventi dispongano delle autorizzazioni DDL necessarie. Per esempio:

```
grant all on public.awsdms_ddl_audit to public;  
grant all on public.awsdms_ddl_audit_c_key_seq to public;
```

Una volta completata la procedura precedente, puoi creare l'endpoint di origine AWS DMS utilizzando l'account *OtherThanMaster*.

Note

Questi eventi sono attivati dalle istruzioni `CREATE TABLE`, `ALTER TABLE` e `DROP TABLE`.

Abilitazione dell'acquisizione dei dati di modifica (CDC) mediante la replica logica

Puoi usare la funzionalità di replica logica nativa di PostgreSQL per abilitare l'acquisizione dei dati di modifica (CDC) durante la migrazione del database per le origini PostgreSQL. Puoi utilizzare questa funzionalità con un'istanza database SQL PostgreSQL autogestita e Amazon RDS per PostgreSQL. Questo approccio riduce i tempi di inattività e aiuta a garantire che il database di destinazione sia sincronizzato con il database PostgreSQL di origine.

AWS DMS supporta CDC per tabelle PostgreSQL con chiavi primarie. Se una tabella non dispone di una chiave primaria, i log write-ahead (WAL) non includono un'immagine precedente della riga di database. In questo caso, DMS non è in grado di aggiornare la tabella. Puoi utilizzare impostazioni di configurazione aggiuntive e l'identità di replica della tabella come soluzione alternativa. Tuttavia, questo approccio può generare log aggiuntivi. Ti consigliamo di utilizzare l'identità di replica

delle tabelle come soluzione alternativa solo dopo attenti test. Per ulteriori informazioni, consulta [Impostazioni di configurazione aggiuntive quando si utilizza un database PostgreSQL come origine DMS](#).

Note

REPLICA IDENTITY FULL è supportato con un plug-in di decodifica logica, ma non è supportato con un plug-in pglogical. Per ulteriori informazioni, consulta [la documentazione di pglogical](#).

Per attività a pieno carico e solo CDC e CDC, AWS DMS utilizza slot di replica logici per conservare i log WAL per la replica fino alla decodifica dei log. Al riavvio (non alla ripresa) di un'attività di pieno carico e CDC o un'attività di sola CDC, lo slot di replica viene ricreato.

Note

Per la decodifica logica, DMS utilizza il plug-in `test_decoding` o `pglogical`. Se il plug-in `pglogical` è disponibile su un database PostgreSQL di origine, DMS crea uno slot di replica utilizzando `pglogical`, altrimenti viene utilizzato un plug-in `test_decoding`. Per ulteriori informazioni sul plug-in `test-decoding`, consulta la [documentazione di PostgreSQL](#). Se il parametro di database `max_slot_wal_keep_size` è impostato su un valore non predefinito e `restart_lsn` dello slot di replica è inferiore al numero LSN corrente di oltre questa dimensione, l'attività DMS ha esito negativo a causa della rimozione dei file WAL richiesti.

Configurazione del plug-in pglogical

Implementato come estensione PostgreSQL, il plug-in `pglogical` è un sistema e un modello di replica logica per la replica dei dati selettiva. La tabella seguente identifica le versioni del database PostgreSQL di origine che supportano il plug-in `pglogical`.

Origine PostgreSQL	Supporta pglogical
PostgreSQL 9.4 autogestito o versioni successive	Sì

Origine PostgreSQL	Supporta pglogical
Amazon RDS PostgreSQL 9.5 o versioni precedenti	No
Amazon RDS PostgreSQL 9.6 o versioni successive	Sì
Aurora PostgreSQL da 1.x a 2.5.x	No
Aurora PostgreSQL 2.6.x o versioni successive	Sì
Aurora PostgreSQL 3.3.x o versioni successive	Sì

Prima di configurare pglogical per l'uso con AWS DMS, abilita innanzitutto la replica logica per l'acquisizione dei dati di modifica (CDC) sul tuo database di origine PostgreSQL.

- Per informazioni sull'abilitazione della replica logica per CDC su database di origine PostgreSQL autogestiti, consulta [Abilitazione del CDC utilizzando un database PostgreSQL autogestito come sorgente AWS DMS](#).
- Per informazioni sull'abilitazione della replica logica per CDC su database di origine PostgreSQL gestiti da AWS, consulta [Abilitazione del CDC con un' AWS istanza DB PostgreSQL gestita con AWS DMS](#).

Dopo aver abilitato la replica logica sul database di origine PostgreSQL, segui i passaggi riportati di seguito per configurare pglogical per l'uso con DMS.

Per utilizzare il plugin pglogical per la replica logica su un database sorgente PostgreSQL con AWS DMS

1. Crea un'estensione pglogical sul database PostgreSQL di origine:
 - a. Imposta il parametro corretto:
 - Per i database PostgreSQL autogestiti, imposta il parametro di database `shared_preload_libraries= 'pglogical'`.

- Per i database PostgreSQL su Amazon RDS e Amazon Aurora edizione compatibile con PostgreSQL, imposta il parametro `shared_preload_libraries` su `pglogical` nello stesso gruppo di parametri RDS.
 - b. Riavvia il database di origine PostgreSQL.
 - c. Sul database PostgreSQL, esegui il comando `create extension pglogical;`.
2. Per verificare che `pglogical` sia stato installato, esegui il comando seguente:

```
select * FROM pg_catalog.pg_extension
```

È ora possibile creare un' AWS DMS attività che esegua l'acquisizione dei dati di modifica per l'endpoint del database di origine PostgreSQL.

Note

Se non abiliti `pglogical` sul database di origine PostgreSQL, AWS DMS utilizza il plug-in `test_decoding` per impostazione predefinita. Quando `pglogical` è abilitato per la decodifica logica, utilizza `pglogical` per impostazione predefinita. AWS DMS Tuttavia, puoi impostare l'attributo aggiuntivo di connessione `PluginName` per utilizzare il plug-in `test_decoding`.

Utilizzo dei punti di avvio CDC nativi per impostare un carico CDC di un endpoint di origine PostgreSQL

Per abilitare i punti di avvio CDC nativi con PostgreSQL come origine è necessario impostare l'attributo aggiuntivo di connessione `s1otName` sul nome di uno slot di replica logica esistente quando si crea l'endpoint. Questo slot di replica logica contiene le modifiche in corso dal momento della creazione dell'endpoint, quindi supporta la replica da un punto precedente nel tempo.

PostgreSQL scrive le modifiche al database nei file WAL che vengono scartati solo quando AWS DMS legge correttamente le modifiche dallo slot di replica logica. Utilizzando gli slot di replica logica è possibile proteggere le modifiche registrate dall'eliminazione prima che vengano utilizzate dal motore di replica.

Tuttavia, a seconda della velocità di modifica e utilizzo, le modifiche presenti in uno slot di replica logica possono causare un utilizzo elevato del disco. Ti consigliamo di impostare gli allarmi relativi all'utilizzo dello spazio nell'istanza PostgreSQL di origine quando vengono utilizzati gli slot di replica logica. Per ulteriori informazioni sull'impostazione dell'attributo di connessione aggiuntivo `s1otName`,

consulta [Impostazioni degli endpoint e attributi di connessione aggiuntivi \(ECA\) quando si utilizza PostgreSQL come sorgente DMS](#).

La seguente procedura percorre questo approccio in modo più dettagliato.

Per utilizzare un punto di avvio CDC nativo per impostare un caricamento CDC di un endpoint di origine PostgreSQL

1. Identificare lo slot di replica logica utilizzato da un'attività di replica precedente (un'attività padre) che si desidera utilizzare come punto iniziale. Quindi interrogare la visualizzazione `pg_replication_slots` sul database di origine per assicurarsi che questo slot non abbia connessioni attive. In tal caso, risolvile e chiudile prima di procedere.

Per i passaggi seguenti, si supponga che lo slot di replica logica sia `abc1d2efghijk_34567890_z0yx98w7_6v54_32ut_1srq_1a2b34c5d67ef`.

2. Creare un nuovo endpoint di origine che include la seguente impostazione dell'attributo di connessione aggiuntivo:

```
slotName=abc1d2efghijk_34567890_z0yx98w7_6v54_32ut_1srq_1a2b34c5d67ef;
```

3. Crea una nuova attività solo CDC utilizzando la console o l'API. AWS CLI AWS DMS Ad esempio, utilizzando l'interfaccia a riga di comando è possibile eseguire il seguente comando `create-replication-task`.

```
aws dms create-replication-task --replication-task-identifier postgresql-slot-name-test
--source-endpoint-arn arn:aws:dms:us-west-2:012345678901:endpoint:ABCD1EFGHIJK2LMNOPQRST3UV4
--target-endpoint-arn arn:aws:dms:us-west-2:012345678901:endpoint:ZYX9WVUTSRQ0NM8LKJIHGF7ED6
--replication-instance-arn arn:aws:dms:us-west-2:012345678901:rep:AAAAAAAAAAAA5BB4CCC3DDDD2EE
--migration-type cdc --table-mappings "file://mappings.json" --cdc-start-position
"4AF/B00000D0"
--replication-task-settings "file://task-pg.json"
```

Nel comando precedente vengono impostate le seguenti opzioni:

- L'opzione `source-endpoint-arn` è impostata sul nuovo valore creato nella fase 2.

- L'opzione `replication-instance-arn` è impostata sullo stesso valore dell'attività padre della fase 1.
- Le opzioni `table-mappings` e `replication-task-settings` sono impostate sugli stessi valori dell'attività padre della fase 1.
- L'opzione `cdc-start-position` è impostata su un valore di posizione iniziale. Per trovare questa posizione iniziale, interrogare la visualizzazione `pg_replication_slots` nel database di origine o visualizzare i dettagli della console per l'attività padre nel passaggio 1. Per ulteriori informazioni, consulta [Determinazione di un punto di inizio nativo CDC](#).

Per abilitare la modalità di avvio CDC personalizzata quando si crea una nuova attività solo CDC utilizzando la AWS DMS console, procedi come segue:

- Nella sezione Impostazioni delle attività scegli Abilita la modalità di avvio CDC personalizzata per Modalità di avvio CDC per le transazioni di origine.
- Per Punto di avvio CDC personalizzato per le transazioni di origine scegli Specifica un numero di sequenza del log. Specifica il numero di modifica del sistema o scegli Specifica un checkpoint di ripristino e fornisci un checkpoint di ripristino.

Quando viene eseguita questa attività CDC, AWS DMS genera un errore se lo slot di replica logica specificato non esiste. Genera un errore anche se l'attività non viene creata con un'impostazione valida per `cdc-start-position`.

Quando utilizzi punti di avvio CDC nativi con il plug-in `pglogical` e desideri utilizzare un nuovo slot di replica, completa i passaggi di configurazione seguenti prima di creare un'attività di CDC.

Per utilizzare un nuovo slot di replica non creato in precedenza come parte di un'altra attività DMS

1. Crea uno slot di replica come illustrato di seguito:

```
SELECT * FROM pg_create_logical_replication_slot('replication_slot_name',  
'pglogical');
```

2. Dopo che il database ha creato lo slot di replica, recupera e annota i valori `restart_lsn` e `confirmed_flush_lsn` per lo slot:


```
select * from pg_replication_slots where slot_name like 'replication_slot_name';
```

Tieni presente che il punto di avvio CDC nativo per un'attività di CDC creata dopo lo slot di replica non può essere precedente al valore `confirmed_flush_lsn`.

Per informazioni sui valori `restart_lsn` e `confirmed_flush_lsn`, consulta [pg_replication_slots](#).

3. Crea un nodo pglogical.

```
SELECT pglogical.create_node(node_name := 'node_name', dsn := 'your_dsn_name');
```

4. Crea due set di replica utilizzando la funzione `pglogical.create_replication_set`. Il primo set di replica tiene traccia degli aggiornamenti e delle eliminazioni per le tabelle con chiavi primarie. Il secondo set di replica tiene traccia solo degli inserimenti e ha lo stesso nome del primo set di replica, con l'aggiunta del prefisso "i".

```
SELECT pglogical.create_replication_set('replication_slot_name', false, true, true, false);  
SELECT pglogical.create_replication_set('ireplication_slot_name', true, false, false, true);
```

5. Aggiungi una tabella al set di repliche.

```
SELECT pglogical.replication_set_add_table('replication_slot_name',  
      'schemaname.tablename', true);  
SELECT pglogical.replication_set_add_table('ireplication_slot_name',  
      'schemaname.tablename', true);
```

6. Imposta l'attributo aggiuntivo di connessione seguente quando crei l'endpoint di origine.

```
PluginName=PGLOGICAL;slotName=slot_name;
```

A questo punto puoi creare un'attività di sola CDC con un punto di avvio nativo PostgreSQL utilizzando il nuovo slot di replica. Per ulteriori informazioni sul plug-in pglogical, consulta la [documentazione di pglogical 3.7](#)

Migrazione da PostgreSQL a PostgreSQL utilizzando AWS DMS

Quando si esegue la migrazione da un motore di database diverso da PostgreSQL a un database PostgreSQL, è quasi sempre lo strumento di migrazione migliore da utilizzare AWS DMS .

Tuttavia, per una migrazione da un database PostgreSQL a un database PostgreSQL, gli strumenti PostgreSQL possono essere più efficaci.

Utilizzo degli strumenti nativi PostgreSQL per migrare i dati

Ti consigliamo di utilizzare gli strumenti per la migrazione dei database PostgreSQL come `pg_dump` nei seguenti casi:

- Hai una migrazione omogenea, dove effettui la migrazione da un database di origine PostgreSQL a un database PostgreSQL di destinazione.
- Desideri migrare un intero database.
- Gli strumenti nativi ti consentono di migrare i dati con tempi di inattività ridotti.

L'utilità `pg_dump` utilizza il comando `COPY` per creare uno schema e il dump dei dati di un database PostgreSQL. Lo script del dump generato da `pg_dump` carica i dati in un database con lo stesso nome e ricrea le tabelle, gli indici e le chiavi esterne. Utilizza il comando `pg_restore` e il parametro `-d` per ripristinare i dati in un database con un nome diverso.

Se esegui la migrazione dei dati da un database di origine PostgreSQL in esecuzione su EC2 a una destinazione Amazon RDS per PostgreSQL, puoi utilizzare il plug-in `pglogical`.

Per ulteriori informazioni sull'importazione di un database PostgreSQL in Amazon RDS per PostgreSQL o Amazon Aurora edizione compatibile con PostgreSQL, consulta <https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/PostgreSQL.Procedural.Importing.html>.

Utilizzo di DMS per la migrazione dei dati da PostgreSQL a PostgreSQL

AWS DMS può migrare i dati, ad esempio, da un database PostgreSQL di origine locale a un'istanza Amazon RDS for PostgreSQL o Aurora PostgreSQL di destinazione. Nella maggior parte dei casi, la migrazione di tipi di dati core o di base PostgreSQL avviene correttamente.

Note

Quando si replicano tabelle partizionate da un'origine PostgreSQL a una destinazione PostgreSQL, non è necessario menzionare la tabella padre come parte dei criteri di selezione nell'attività DMS. La menzione della tabella padre causa la duplicazione dei dati nelle tabelle

figlio sulla destinazione, causando probabilmente una violazione delle chiavi primarie. Selezionando solo le tabelle figlio nella tabella che mappa i criteri di selezione, la tabella padre viene compilata automaticamente.

I tipi di dati supportati nel database di origine ma non supportati nella destinazione potrebbero non essere migrati correttamente. AWS DMS trasmette alcuni tipi di dati come stringhe se il tipo di dati è sconosciuto. Alcuni tipi di dati, ad esempio XML e JSON, possono migrare come file di piccole dimensioni, ma potrebbero non migrare correttamente se i documenti sono di grandi dimensioni.

Quando esegui la migrazione del tipo di dati, tieni presente quanto segue:

- In alcuni casi, il tipo di dati PostgreSQL NUMERIC(p,s) non specifica la precisione e la scala. Per DMS 3.4.2 e versioni precedenti, DMS utilizza una precisione di 28 e una scala di 6 per impostazione predefinita, NUMERIC(28,6). Ad esempio, il valore 0,611111104488373 dell'origine viene convertito in 0,611111 nella destinazione PostgreSQL.
- Una tabella con un tipo di dati ARRAY deve avere una chiave primaria. Una tabella con un tipo di dati ARRAY priva di una chiave primaria viene sospesa durante il pieno carico.

La tabella seguente mostra i tipi di dati di origine PostgreSQL e indica se possono essere migrati correttamente:

Tipo di dati	Migrazione corretta	Migrazione parziale	Nessuna migrazione	Commenti
INTEGER	X			
SMALLINT	X			
BIGINT	X			
NUMERIC/DECIMAL(p,s)		X		Dove $0 < p < 39$ e $0 < s$
NUMERIC/DECIMAL		X		Dove $p > 38$ o $p = s = 0$
REAL	X			

Tipo di dati	Migrazione corretta	Migrazione parziale	Nessuna migrazione	Commenti
DOUBLE	X			
SMALLSERIAL	X			
SERIAL	X			
BIGSERIAL	X			
MONEY	X			
CHAR		X		Senza precisione specificata
CHAR(n)	X			
VARCHAR		X		Senza precisione specificata
VARCHAR(n)	X			
TEXT	X			
BYTEA	X			

Tipo di dati	Migrazione corretta	Migrazione parziale	Nessuna migrazione	Commenti
TIMESTAMP	X			I valori infiniti positivi e negativi vengono troncati rispettivamente a "9999-12-31 23:59:59" e "4713-01-01 00:00:00 BC".
TIMESTAMP WITH TIME ZONE		X		
DATE	X			
TIME	X			
TIME WITH TIME ZONE		X		
INTERVAL		X		
BOOLEAN	X			
ENUM			X	
CIDR	X			
INET			X	
MACADDR			X	
TSVECTOR			X	
TSQUERY			X	

Tipo di dati	Migrazione corretta	Migrazione parziale	Nessuna migrazione	Commenti
XML		X		
POINT	X			Tipo di dati spaziali PostGIS
LINE			X	
LSEG			X	
BOX			X	
PATH			X	
POLYGON	X			Tipo di dati spaziali PostGIS
CIRCLE			X	
JSON		X		
ARRAY	X			Richiede la chiave primaria
COMPOSITE			X	
RANGE			X	
LINestring	X			Tipo di dati spaziali PostGIS
MULTIPOINT	X			Tipo di dati spaziali PostGIS

Tipo di dati	Migrazione corretta	Migrazione parziale	Nessuna migrazione	Commenti
MULTILINESTRING	X			Tipo di dati spaziali PostGIS
MULTIPOLYGON	X			Tipo di dati spaziali PostGIS
GEOMETRYCOLLECTION	X			Tipo di dati spaziali PostGIS

Migrazione dei tipi di dati spaziali di PostGIS

I dati spaziali identificano le informazioni sulla geometria di un oggetto o di una posizione nello spazio. I database relazionali a oggetti PostgreSQL supportano i tipi di dati spaziali PostGIS.

Prima di migrare gli oggetti formati da dati spaziali PostgreSQL, assicurati che il plug-in PostGIS sia abilitato a livello globale. In questo modo si garantisce la AWS DMS creazione delle colonne di dati spaziali di origine esatte per l'istanza DB di destinazione PostgreSQL.

Per le AWS DMS migrazioni omogenee da PostgreSQL a PostgreSQL, supporta la migrazione di tipi e sottotipi di oggetti dati geometrici e geografici (coordinate geodetiche) di PostGIS come i seguenti:

- POINT
- LINESTRING
- POLYGON
- MULTIPOINT
- MULTILINESTRING
- MULTIPOLYGON
- GEOMETRYCOLLECTION

Migrazione da Babelfish per Amazon Aurora PostgreSQL utilizzando AWS DMS

Puoi migrare le tabelle di origine PostgreSQL di Babelfish for Aurora su qualsiasi endpoint di destinazione supportato utilizzando AWS DMS.

Quando crei il tuo endpoint di AWS DMS origine utilizzando la console DMS, l'API o i comandi CLI, imposti l'origine su Amazon Aurora PostgreSQL e il nome del database su **babelfish_db**. Nella sezione Endpoint Settings, assicurati che sia impostato su Babelfish e che DatabaseModesia impostato sul nome del database Babelfish T-SQL di BabelfishDatabaseNameorigine. Invece di usare la porta TCP Babelfish **1433**, usa la porta TCP Aurora PostgreSQL. **5432**

È necessario creare le tabelle prima di migrare i dati per assicurarsi che DMS utilizzi i tipi di dati e i metadati delle tabelle corretti. Se non crei le tabelle sulla destinazione prima di eseguire la migrazione, DMS potrebbe creare le tabelle con tipi di dati e autorizzazioni errati.

Aggiunta delle regole di trasformazione all'attività di migrazione

Quando crei un'attività di migrazione per una fonte Babelfish, devi includere regole di trasformazione che assicurino che DMS utilizzi le tabelle di destinazione precreate.

Se hai impostato la modalità di migrazione multi-database quando hai definito il tuo cluster Babelfish per PostgreSQL, aggiungi una regola di trasformazione che rinomina il nome dello schema nello schema T-SQL. Ad esempio, se il nome dello schema T-SQL è dbo e il nome dello schema Babelfish for PostgreSQL è mydb_dbo, rinomina lo schema utilizzando una regola di trasformazione. Per trovare il nome dello schema PostgreSQL, [consulta l'architettura Babelfish](#) nella Guida per l'utente di Amazon Aurora.

Se utilizzi la modalità a database singolo, non è necessario utilizzare una regola di trasformazione per rinominare gli schemi di database. I nomi degli schemi PostgreSQL hanno one-to-one una mappatura con i nomi degli schemi nel database T-SQL.

Il seguente esempio di regola di trasformazione mostra come rinominare il nome dello schema da back a: mydb_dbo dbo

```
{
  "rules": [
    {
      "rule-type": "transformation",
      "rule-id": "566251737",
      "rule-name": "566251737",
      "rule-target": "schema",
```



```
    "object-locator": {
      "schema-name": "mydb_dbo"
    },
    "rule-action": "rename",
    "value": "dbo",
    "old-value": null
  },
  {
    "rule-type": "selection",
    "rule-id": "566111704",
    "rule-name": "566111704",
    "object-locator": {
      "schema-name": "mydb_dbo",
      "table-name": "%"
    },
    "rule-action": "include",
    "filters": []
  }
]
```

Limitazioni per l'utilizzo di un endpoint sorgente PostgreSQL con le tabelle Babelfish

Le seguenti limitazioni si applicano quando si utilizza un endpoint sorgente PostgreSQL con tabelle Babelfish:

- DMS supporta solo la migrazione dalla versione 16.2/15.6 di Babelfish e successive e dalla versione DMS 3.5.3 e successive.
- DMS non replica le modifiche alla definizione delle tabelle Babelfish sull'endpoint di destinazione. Una soluzione alternativa per questa limitazione consiste nell'applicare prima le modifiche alla definizione della tabella sulla destinazione, quindi modificare la definizione della tabella sul sorgente Babelfish.
- Quando si creano tabelle Babelfish con il tipo di dati BYTEA, DMS le converte nel tipo di `varbinary(max)` dati durante la migrazione a SQL Server come destinazione.
- DMS non supporta la modalità Full LOB per i tipi di dati binari. Utilizzate invece la modalità LOB limitata per i tipi di dati binari.
- DMS non supporta la convalida dei dati per Babelfish come fonte.
- Per l'impostazione delle attività della modalità di preparazione della tabella di Target, utilizza solo le modalità Non fare nulla o Truncate. Non utilizzare la modalità Rilascia tabelle nella destinazione. Quando si utilizza Drop tables on target, DMS può creare tabelle con tipi di dati errati.

- Quando si utilizza la replica continua (CDC o Full load e CDC), imposta l'attributo di connessione `PluginName` aggiuntivo (ECA) su `TEST_DECODING`

Rimozione di AWS DMS artefatti da un database sorgente PostgreSQL

Per acquisire eventi DDL, AWS DMS crea vari artefatti nel database PostgreSQL all'avvio di un'attività di migrazione. Al termine dell'attività è possibile rimuovere gli artefatti.

Per rimuovere gli artefatti, invia le seguenti istruzioni (nell'ordine), dove `{AmazonRDSMigration}` è lo schema in cui sono stati creati gli artefatti. L'eliminazione di uno schema deve essere eseguita con estrema attenzione. Non eliminare mai uno schema operativo, soprattutto uno pubblico.

```
drop event trigger awsdms_intercept_ddl;
```

Il trigger evento non appartiene a uno schema specifico.

```
drop function {AmazonRDSMigration}.awsdms_intercept_ddl()  
drop table {AmazonRDSMigration}.awsdms_ddl_audit  
drop schema {AmazonRDSMigration}
```

Impostazioni di configurazione aggiuntive quando si utilizza un database PostgreSQL come origine DMS

Puoi aggiungere ulteriori impostazioni di configurazione durante la migrazione dei dati da un database PostgreSQL in due modi:

- Puoi aggiungere valori all'attributo di connessione aggiuntivo per acquisire eventi DDL e per specificare lo schema in cui vengono creati gli artefatti operativi del database DDL. Per ulteriori informazioni, consulta [Impostazioni degli endpoint e attributi di connessione aggiuntivi \(ECA\) quando si utilizza PostgreSQL come sorgente DMS](#).
- Puoi sostituire i parametri della stringa di connessione. Scegli questa opzione per eseguire una delle seguenti operazioni:
 - AWS DMS Specificare i parametri interni. Questi parametri sono raramente necessari e non sono quindi visualizzati nell'interfaccia utente.
 - Specificate i valori pass-through (`passthru`) per il client di database specifico. AWS DMS include i parametri pass-through nella stringa di connessione passata al client del database.

- Utilizzando il parametro table-level `REPLICA IDENTITY` in PostgreSQL 9.4 e versioni successive, puoi controllare le informazioni scritte nei log WAL (write-ahead log). In particolare, lo fa per i log WAL che identificano le righe che vengono aggiornate o eliminate. `REPLICA IDENTITY FULL` registra i precedenti valori di tutte le colonne della riga. Utilizza `REPLICA IDENTITY FULL` con attenzione per ogni tabella poiché `FULL` genera una quantità aggiuntiva di log WAL che potrebbe non essere necessaria. Per ulteriori informazioni, consulta [ALTER TABLE-REPLICA IDENTITY](#).

Utilizzo dell'impostazione dell' `MapBooleanAsBoolean` endpoint PostgreSQL

Puoi utilizzare le impostazioni degli endpoint PostgreSQL per mappare un booleano come tale dall'origine PostgreSQL a una destinazione Amazon Redshift. Per impostazione predefinita, il tipo `BOOLEAN` viene migrato come `varchar(5)`. È possibile specificare `MapBooleanAsBoolean` per consentire a PostgreSQL di migrare il tipo booleano come tale, come mostrato nell'esempio seguente.

```
--postgres-sql-settings '{"MapBooleanAsBoolean": true}'
```

Tieni presente che questa impostazione, affinché abbia effetto, deve essere configurata sia sull'endpoint di origine che su quello di destinazione.

Poiché MySQL non ha il tipo `BOOLEAN`, usa una regola di trasformazione anziché questa impostazione per la migrazione dei dati `BOOLEAN` su MySQL.

Impostazioni degli endpoint e attributi di connessione aggiuntivi (ECA) quando si utilizza PostgreSQL come sorgente DMS

Puoi utilizzare le impostazioni degli endpoint e gli attributi di connessione aggiuntivi (ECA) per configurare il tuo database di origine PostgreSQL. Le impostazioni degli endpoint vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando contenuto in, con la sintassi JSON. [AWS CLI](#) `--postgres-sql-settings` `'{"EndpointSetting": "value", ...}'`


La tabella seguente mostra le impostazioni degli endpoint e le ECA che è possibile utilizzare con PostgreSQL come sorgente.

Nome attributo	Descrizione
CaptureDDLs	<p>Per acquisire eventi DDL, AWS DMS crea vari artefatti nel database PostgreSQL all'avvio dell'attività. Successivamente puoi rimuovere gli artefatti, come descritto in Rimozione di AWS DMS artefatti da un database sorgente PostgreSQL.</p> <p>Se il valore è impostato su <code>false</code>, non è necessario creare tabelle o trigger nel database di origine.</p> <p>Gli eventi DDL in streaming vengono acquisiti.</p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--postgre-sql-settings '{"CaptureDDLs": true}'</code></p>
ConsumeMonotonicEvents	<p>Utilizzato per controllare la modalità di replica delle transazioni monolitiche con numeri di sequenza di log (LSN) duplicati. Quando questo parametro è impostato su <code>false</code>, gli eventi con LSN duplicati vengono consumati e replicati sulla destinazione. Se questo parametro è impostato su <code>true</code>, viene replicato solo il primo evento, mentre gli eventi con LSN duplicati non vengono consumati né replicati sulla destinazione.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>false/true</code></p> <p>Esempio: <code>--postgre-sql-settings '{"ConsumeMonotonicEvents": true}'</code></p>
DdlArtifactsSchema	<p>Imposta lo schema in cui vengono creati gli artefatti del database DDL operativo.</p> <p>Valore predefinito: <code>pubblico</code></p>

Nome attributo	Descrizione
	<p>Valori validi: stringa</p> <p>Esempio: <code>--postgres-sql-settings '{"DdlArtifactsSchema": " <i>xyzddl</i>schema "}'</code></p>
ExecuteTimeout	<p>Imposta il timeout dell'istruzione del client per l'istanza PostgreSQL in secondi. Il valore predefinito è 60 secondi.</p> <p>Esempio: <code>--postgres-sql-settings '{"ExecuteTimeout": 100}'</code></p>
FailTasksOnLobTruncation	<p>Se è impostato su <code>true</code>, questo valore non consentirà la riuscita di un'attività se le dimensioni attuali di una colonna LOB sono maggiori di quelle specificate in <code>LobMaxSize</code> .</p> <p>Se un'attività è impostata sulla modalità LOB limitata e questa opzione è impostata su <code>true</code>, l'operazione ha esito negativo invece di troncatura i dati LOB.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: booleani</p> <p>Esempio: <code>--postgres-sql-settings '{"FailTasksOnLobTruncation": true}'</code></p>
fetchCacheSize	<p>Questo attributo aggiuntivo di connessione imposta il numero di righe che il cursore recupera durante l'operazione pieno carico. A seconda delle risorse disponibili nell'istanza di replica, è possibile aumentare o diminuire il valore.</p> <p>Valore predefinito: <code>10000</code></p> <p>Valori validi: numero</p> <p>Esempio ECA: <code>fetchCacheSize=10000;</code></p>

Nome attributo	Descrizione
HeartbeatFrequency	<p>Imposta la frequenza heartbeat WAL (in minuti).</p> <p>Valore predefinito: 5</p> <p>Valori validi: numero</p> <p>Esempio: <code>--postgresql-settings '{"HeartbeatFrequency": 1}'</code></p>
HeartbeatSchema	<p>Imposta lo schema in cui vengono creati gli artefatti di heartbeat.</p> <p>Valore predefinito: <code>public</code></p> <p>Valori validi: stringa</p> <p>Esempio: <code>--postgresql-settings '{"HeartbeatSchema": "xyzheartbeatSchema"}'</code></p>
MapJsonbAsClob	<p>Per impostazione predefinita, mappa JSONB su NCLOB. AWS DMS È possibile specificare MapJsonbAsClob per consentire a PostgreSQL di migrare il tipo JSONB come CLOB.</p> <p>Esempio: <code>--postgresql-settings='{"MapJsonbAsClob": "true"}'</code></p>

Nome attributo	Descrizione
MapLongVarcharAs	<p>Per impostazione predefinita, AWS DMS mappa VARCHAR su WSTRING. È possibile specificare MapLongVarcharAs per consentire a PostgreSQL di migrare il tipo VARCHAR(N) (dove N è maggiore di 16387) ai seguenti tipi:</p> <ul style="list-style-type: none">• WSTRING• CLOB• NCLOB <p>Esempio: <code>--postgres-sql-settings='{ "MapLongVarcharAs": "CLOB" }'</code></p>

Nome attributo	Descrizione
MapUnboundedNumericAsString	<p>Questo parametro tratta le colonne con tipi di dati NUMERIC illimitati come STRING per eseguire correttamente la migrazione senza perdere la precisione del valore numerico. Usa questo parametro solo per la replica dall'origine PostgreSQL alla destinazione PostgreSQL o ai database con compatibilità PostgreSQL.</p> <p>Valore predefinito: false</p> <p>Valori validi: false/true</p> <p>Esempio: <code>--postgre-sql-settings '{"MapUnboundedNumericAsString": true}'</code></p> <p>L'utilizzo di questo parametro può comportare un peggioramento delle prestazioni di replica a causa della trasformazione da valore numerico a stringa e di nuovo a valore numerico. Questo parametro è supportato per l'uso da DMS versione 3.4.4 e successive</p> <div data-bbox="688 1100 1507 1751" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><p>Utilizza MapUnboundedNumericAsString solo negli endpoint di origine e di destinazione PostgreSQL insieme.</p><p>L'uso di MapUnboundedNumericAsString su endpoint PostgreSQL di origine limita la precisione a 28 durante la CDC. L'uso di MapUnboundedNumericAsString su endpoint di destinazione, migra i dati con precisione 28 scala 6.</p><p>Non utilizzare MapUnboundedNumericAsString con destinazioni non PostgreSQL.</p></div>

Nome attributo	Descrizione
PluginName	<p data-bbox="686 226 1430 310">Specifica il plug-in da utilizzare per creare uno slot di replica.</p> <p data-bbox="686 352 1325 394">Valori validi: <code>pglogical</code> , <code>test_decoding</code></p> <p data-bbox="686 436 1442 520">Esempio: <code>--postgre-sql-settings '{"Plugin Name": "test_decoding"}'</code></p>

Nome attributo	Descrizione
SlotName	<p>Imposta il nome di uno slot di replica logica creato in precedenza per un caricamento CDC dell'istanza di origine PostgreSQL.</p> <p>Se utilizzato con il parametro di <code>CdcStartPosition</code> richiesta AWS DMS API, questo attributo consente anche l'utilizzo di punti di partenza CDC nativi. DMS verifica che lo slot di replica logica specificato esista prima di avviare l'attività di carico CDC. Verifica inoltre che l'attività sia stata creata con un'impostazione valida di <code>CdcStartPosition</code>. Se lo slot specificato non esiste o l'attività non dispone di un'impostazione <code>CdcStartPosition</code> valida, DMS genera un errore.</p> <p>Per ulteriori informazioni su come impostare il parametro della richiesta <code>CdcStartPosition</code>, consulta Determinazione di un punto di inizio nativo CDC.</p> <p>Per ulteriori informazioni sull'utilizzo di <code>CdcStartPosition</code>, consulta la documentazione per le operazioni API <code>CreateReplicationTask</code>, <code>StartReplicationTask</code> e <code>ModifyReplicationTask</code> nella Documentazione di riferimento delle API AWS Database Migration Service.</p> <p>Valori validi: stringa</p> <p>Esempio: <code>--postgre-sql-settings '{"SlotName": "abc1d2efghijk_34567890_z0yx98w7_6v54_32ut_1srq_1a2b34c5d67ef"}'</code></p>
unboundedVarcharMaxSize	<p>Questo attributo di connessione aggiuntivo (ECA) definisce la dimensione massima di una colonna di dati definita come tipo <code>VarChar</code> senza un identificatore di lunghezza massima. L'impostazione predefinita è 8000 byte. Il valore massimo è 10485760 byte.</p>

Limitazioni all'utilizzo di un database PostgreSQL come origine DMS

Quando si utilizza un database PostgreSQL come origine per AWS DMS, si applicano le seguenti limitazioni:

- AWS DMS non funziona con Amazon RDS for PostgreSQL 10.4 o Amazon Aurora PostgreSQL 10.4 come origine o destinazione.
- Una tabella acquisita deve avere una chiave primaria. Se una tabella non ha una chiave primaria, ignora le operazioni di record DELETE e UPDATE per quella tabella. AWS DMS Come soluzione alternativa, consulta [Abilitazione dell'acquisizione dei dati di modifica \(CDC\) mediante la replica logica](#).

Nota: non è consigliabile eseguire la migrazione senza una chiave primaria/un indice univoco, altrimenti si applicano limitazioni aggiuntive come nessuna funzionalità di applicazione in batch, funzionalità LOB completa, convalida dei dati e l'impossibilità di replicare in modo efficiente sulla destinazione Redshift.

- AWS DMS ignora il tentativo di aggiornare un segmento di chiave primaria. In questi casi, la destinazione identifica l'aggiornamento come un'operazione che non ha aggiornato righe. Tuttavia, poiché i risultati di aggiornamento di una chiave primaria in PostgreSQL sono imprevedibili, non vengono scritti record nella tabella delle eccezioni.
- AWS DMS non supporta l'opzione Avvia processo di modifica da Timestamp run.
- AWS DMS non replica le modifiche risultanti da operazioni di partizione o sottopartizione (, o). ADD DROP TRUNCATE
- La replica di più tabelle con lo stesso nome ma scritto con lettere maiuscole e minuscole diverse (ad esempio tabella1, TABELLA1 e Tabella1) può causare un comportamento imprevedibile. A causa di questo problema, AWS DMS non supporta questo tipo di replica.
- Nella maggior parte dei casi, AWS DMS supporta l'elaborazione delle modifiche delle istruzioni DDL CREATE, ALTER e DROP per le tabelle. AWS DMS non supporta questa elaborazione delle modifiche se le tabelle sono contenute in un blocco interno del corpo di una funzione o di una procedura o in altri costrutti annidati.

Ad esempio, la seguente modifica non viene acquisita.

```
CREATE OR REPLACE FUNCTION attu.create_distributors1() RETURNS void
LANGUAGE plpgsql
AS $$
BEGIN
```

```
create table attu.distributors1(did serial PRIMARY KEY,name
varchar(40) NOT NULL);
END;
$$;
```

- Attualmente, i tipi di dati boolean in un'origine PostgreSQL vengono migrati a una destinazione SQL Server come tipo di dati bit con valori incoerenti. Come soluzione alternativa, precrea la tabella con un tipo di VARCHAR(1) dati per la colonna (o chiedi a AWS DMS di creare la tabella). Quindi fai in modo che l'elaborazione a valle tratti una «F» come False e una «T» come True.
- AWS DMS non supporta l'elaborazione delle modifiche delle operazioni TRUNCATE.
- Il tipo di dati OID LOB non viene migrato nella destinazione.
- AWS DMS supporta il tipo di dati PostGIS solo per migrazioni omogenee.
- Se l'origine è un database PostgreSQL on-premise o su un'istanza Amazon EC2, accertati che il plug-in di output test_decoding sia installato nell'endpoint di origine. Puoi trovare questo plug-in nel pacchetto contrib PostgreSQL. Per ulteriori informazioni sul plug-in di test-decoding, consulta la [documentazione di PostgreSQL](#).
- AWS DMS non supporta l'elaborazione delle modifiche per impostare e annullare i valori predefiniti delle colonne (utilizzando la clausola ALTER COLUMN SET DEFAULT nelle istruzioni ALTER TABLE).
- AWS DMS non supporta l'elaborazione delle modifiche per impostare l'annullabilità delle colonne (utilizzando la clausola ALTER COLUMN [SET|DROP] NOT NULL nelle istruzioni ALTER TABLE).
- Quando la replica logica è abilitata, il numero massimo di modifiche conservate in memoria per transazione è 4 MB. Dopodiché, le modifiche vengono riversate su disco. Di conseguenza ReplicationSlotDiskUsage aumenta e restart_lsn non avanza finché la transazione non viene completata o interrotta e il rollback non termina. Poiché si tratta di una transazione lunga, il rollback può richiedere tempi lunghi. Pertanto, evita transazioni di lunga durata o molte sottotransazioni quando la replica logica è abilitata. Prova invece a suddividere la transazione in diverse transazioni più piccole.

Nelle versioni 13 e successive di Aurora PostgreSQL, è possibile ottimizzare il logical_decoding_work_mem parametro per controllare quando le fuoriuscite di DMS modificano i dati sul disco. Per ulteriori informazioni, consulta [Versare file in Aurora PostgreSQL](#).

- Una tabella con un tipo di dati ARRAY deve avere una chiave primaria. Una tabella con un tipo di dati ARRAY priva di una chiave primaria viene sospesa durante il pieno carico.
- AWS DMS non supporta la replica di tabelle partizionate. Quando viene rilevata una tabella partizionata, avviene quanto segue:

- L'endpoint fornisce un report di tabelle padre e figlio.
- AWS DMS crea la tabella sulla destinazione come tabella normale con le stesse proprietà delle tabelle selezionate.
- Se la tabella padre nel database di origine ha lo stesso valore di chiave primaria delle tabelle figlio, viene generato un errore di "chiavi duplicate".
- Per replicare le tabelle partizionate da un'origine PostgreSQL a una destinazione PostgreSQL, crea manualmente le tabelle padre e figlio nella destinazione. Quindi definisci un'attività separata per la replica su tali tabelle. In questo caso, imposta la configurazione dell'attività su Tronca prima di caricare.
- Il tipo di dati PostgreSQL NUMERIC non viene fissato nelle dimensioni. Quando si trasferiscono dati di tipo NUMERIC ma senza precisione e dimensioni, per impostazione predefinita DMS usa NUMERIC(28,6) (una precisione di 28 e dimensione 6). Ad esempio, il valore 0.611111104488373 dell'origine viene convertito in 0.611111 nella destinazione PostgreSQL.
- AWS DMS supporta Aurora PostgreSQL Serverless V1 come origine solo per attività a pieno carico. AWS DMS supporta Aurora PostgreSQL Serverless V2 come fonte per attività a pieno carico, a pieno carico e solo CDC e CDC.
- AWS DMS non supporta la replica di una tabella con un indice univoco creato con una funzione di coalescenza.
- Quando si utilizza la modalità LOB, sia la tabella di origine che la tabella di destinazione corrispondente devono avere una chiave primaria identica. Se una delle tabelle non dispone di una chiave primaria, il risultato delle operazioni di registrazione DELETE e UPDATE è imprevedibile.
- Quando si utilizza la funzionalità di caricamento parallelo, la segmentazione delle tabelle in base a partizioni o sottopartizioni non è supportata. Per ulteriori informazioni sul caricamento parallelo, consulta [Utilizzo del caricamento parallelo per le tabelle, le viste e le raccolte selezionate](#).
- AWS DMS non supporta i vincoli differiti.
- AWS DMS la versione 3.4.7 supporta PostgreSQL 14.x come sorgente con queste limitazioni:
 - AWS DMS non supporta l'elaborazione delle modifiche dei commit in due fasi.
 - AWS DMS non supporta la replica logica per lo streaming di lunghe transazioni in corso.
- AWS DMS non supporta CDC per Amazon RDS Proxy for PostgreSQL come sorgente.
- Quando si utilizzano [filtri di origine](#) che non contengono una colonna di chiave primaria, le operazioni DELETE non verranno acquisite.
- Se il database di origine è anche la destinazione di un altro sistema di replica di terze parti, le modifiche DDL potrebbero non migrare durante CDC in quanto potrebbero impedire l'attivazione

del trigger dell'evento `awsdms_intercept_ddl`. Per aggirare la situazione, modifica il trigger nel database di origine come segue:

```
alter event trigger awsdms_intercept_ddl enable always;
```

- AWS DMS non supporta il cluster di database CDC per Amazon RDS Multi-AZ per PostgreSQL come sorgente, poiché i cluster di database RDS per PostgreSQL Multi-AZ non supportano la replica logica.

Tipi di dati di origine per PostgreSQL

La tabella seguente mostra i tipi di dati sorgente PostgreSQL supportati durante l' AWS DMS utilizzo e la mappatura predefinita ai tipi di dati. AWS DMS

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere. [Tipi di dati per AWS Database Migration Service](#)

Tipi di dati PostgreSQL	Tipi di dati DMS
INTEGER	INT4
SMALLINT	INT2
BIGINT	INT8
NUMERIC (p,s)	Se la precisione è compresa tra 0 e 38, utilizzare e NUMERIC. Se la precisione è 39 o maggiore, utilizzare STRING.
DECIMAL(P,S)	Se la precisione è compresa tra 0 e 38, utilizzare e NUMERIC. Se la precisione è 39 o maggiore, utilizzare STRING.

Tipi di dati PostgreSQL	Tipi di dati DMS
REAL	REAL4
DOUBLE	REAL8
SMALLSERIAL	INT2
SERIAL	INT4
BIGSERIAL	INT8
MONEY	NUMERIC(38,4) Il tipo di dati MONEY è mappato su FLOAT in SQL Server.
CHAR	WSTRING (1)
CHAR(N)	WSTRING (n)
VARCHAR(N)	WSTRING (n)
TEXT	NCLOB
CITEXT	NCLOB
BYTEA	BLOB
TIMESTAMP	DATETIME
TIMESTAMP WITH TIME ZONE	DATETIME
DATE	DATE
TIME	TIME
TIME WITH TIME ZONE	TIME
INTERVAL	STRING (128): 1 YEAR, 2 MONTHS, 3 DAYS, 4 HOURS, 5 MINUTES, 6 SECONDS

Tipi di dati PostgreSQL	Tipi di dati DMS
BOOLEAN	CHAR (5) false o true
ENUM	STRING (64)
CIDR	STRING (50)
INET	STRING (50)
MACADDR	STRING (18)
BIT(n)	STRING (n)
BIT VARYING (n)	STRING (n)
UUID	STRING
TSVECTOR	CLOB
TSQUERY	CLOB
XML	CLOB
POINT	STRING (255) "(x,y)"
LINE	STRING (255) "(x,y,z)"
LSEG	STRING (255) "((x1,y1),(x2,y2))"
BOX	STRING (255) "((x1,y1),(x2,y2))"
PATH	CLOB "((x1,y1),(xn,yn))"
POLYGON	CLOB "((x1,y1),(xn,yn))"
CIRCLE	STRING (255) "(x,y),r"
JSON	NCLOB
JSONB	NCLOB

Tipi di dati PostgreSQL	Tipi di dati DMS
ARRAY	NCLOB
COMPOSITE	NCLOB
HSTORE	NCLOB
INT4RANGE	STRING (255)
INT8RANGE	STRING (255)
NUMRANGE	STRING (255)
STRRANGE	STRING (255)

Utilizzo dei tipi di dati di origine LOB per PostgreSQL

Le dimensioni di colonna PostgreSQL influenzano la conversione dei tipi di dati LOB PostgreSQL in tipi di dati AWS DMS . Per utilizzare questa funzione, effettua la procedura riportata di seguito per i seguenti tipi di dati AWS DMS :

- BLOB: imposta Limita dimensioni LOB a sul valore di Dimensione massima dei LOB (KB) al momento della creazione dell'attività.
- CLOB: la replica gestisce ogni carattere come carattere UTF8. Pertanto, individua il testo con il maggiore numero di caratteri nella colonna `max_num_chars_text`. Utilizza questa lunghezza per specificare il valore di Limita dimensioni LOB a. Se i dati includono caratteri a 4 byte, moltiplicare per 2 per specificare il valore di Limit LOB size to (Limita dimensioni LOB a), che è espresso in byte. In questo caso, Limit LOB size to (Limita dimensioni LOB a) è uguale a `max_num_chars_text` moltiplicato per 2.
- NCLOB: la replica gestisce ogni carattere come carattere a due byte. Pertanto, individua il testo con il maggiore numero di caratteri nella colonna (`max_num_chars_text`) e moltiplicarlo per 2. Questa operazione viene eseguita per specificare il valore di Limita dimensioni LOB a. In questo caso, Limit LOB size to (Limita dimensioni LOB a) è uguale a `max_num_chars_text` moltiplicato per 2. Se i dati includono caratteri a 4 byte, moltiplicare ancora per 2. In questo caso, Limit LOB size to (Limita dimensioni LOB a) è uguale a `max_num_chars_text` moltiplicato per 4.

Utilizzo di un database compatibile con MySQL come origine per AWS DMS

Puoi migrare i dati da qualsiasi database compatibile con MySQL (MySQL, MariaDB o Amazon Aurora MySQL) utilizzando Database Migration Service. AWS

Per informazioni sulle versioni di MySQL supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Puoi utilizzare il protocollo SSL per crittografare le connessioni tra l'endpoint compatibile con MySQL e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint compatibile con MySQL, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Nelle sezioni seguenti, il termine "autogestito" si applica a qualsiasi database installato on-premise o su Amazon EC2. Il termine "gestito da AWS" si applica a qualsiasi database su Amazon RDS, Amazon Aurora o Amazon S3.

Per ulteriori dettagli sull'utilizzo di database compatibili con MySQL AWS DMS, vedere le seguenti sezioni.

Argomenti

- [Migrazione da MySQL a MySQL mediante AWS DMS](#).
- [Utilizzo di qualsiasi database compatibile con MySQL come fonte per AWS DMS](#)
- [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#)
- [Utilizzo di un AWS database compatibile con MySQL gestito come fonte per AWS DMS](#)
- [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#)
- [Supporto per transazione XA](#)
- [Impostazioni degli endpoint quando si utilizza MySQL come sorgente per AWS DMS](#)
- [Tipi di dati di origine per MySQL](#)

Migrazione da MySQL a MySQL mediante AWS DMS.

Per una migrazione eterogenea, in cui si esegue la migrazione da un motore di database diverso da MySQL a un database MySQL, è quasi sempre lo strumento di migrazione migliore da utilizzare. AWS DMS Ma per una migrazione omogenea, ad esempio da un database MySQL a un database MySQL, ti consigliamo di utilizzare un progetto di migrazione di dati omogeneo. Le migrazioni di dati

omogenee utilizzano strumenti di database nativi per fornire prestazioni e precisione di migrazione dei dati migliorate rispetto a AWS DMS.

Utilizzo di qualsiasi database compatibile con MySQL come fonte per AWS DMS

Prima di iniziare a utilizzare un database MySQL come sorgente AWS DMS per, assicurati di avere i seguenti prerequisiti. Questi prerequisiti si applicano sia alle fonti autogestite che a quelle gestite. AWS

È necessario disporre di un account con il ruolo di AWS DMS amministratore di replica. Il ruolo richiede i seguenti privilegi:

- **REPLICATION CLIENT:** questo privilegio è richiesto per le attività di sola CDC. In altre parole, le full-load-only attività non richiedono questo privilegio.
- **REPLICATION SLAVE:** questo privilegio è richiesto per le attività di sola CDC. In altre parole, le full-load-only attività non richiedono questo privilegio.
- **SUPER:** questo privilegio è richiesto solo nelle versioni di MySQL precedenti alla 5.6.6.

L' AWS DMS utente deve inoltre disporre dei privilegi SELECT per le tabelle di origine designate per la replica.

Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS

Puoi utilizzare i seguenti database gestiti dal cliente compatibili con MySQL come origini per AWS DMS:

- MySQL Community Edition
- MySQL Standard Edition
- MySQL Enterprise Edition
- MySQL Cluster Carrier Grade Edition
- MariaDB Community Edition
- MariaDB Enterprise Edition
- MariaDB Column Store

Per utilizzare CDC, assicurati di abilitare la registrazione binaria. Per abilitare la registrazione binaria, devi configurare i seguenti parametri nel file `my.ini` (Windows) o `my.cnf` (UNIX) di MySQL.

Parametro	Valore
<code>server_id</code>	Imposta questo parametro su un valore uguale o maggiore di 1.
<code>log-bin</code>	Imposta il percorso del file di log binario, ad esempio <code>log-bin=E:\MySQL_Logs\BinLog</code> . Non includere l'estensione del file.
<code>binlog_format</code>	Imposta questo parametro su ROW. Si consiglia questa impostazione per la replica perché, in alcuni casi, quando <code>binlog_format</code> è impostato su STATEMENT , si possono verificare incoerenze della replica dei dati sulla destinazione. Il motore di database scrive dati incoerenti simili sulla destinazione quando <code>binlog_format</code> è impostato su MIXED perché passa automaticamente alla registrazione basata su STATEMENT , il che può comportare la scrittura di dati non coerenti sul database di destinazione.
<code>expire_logs_days</code>	Imposta questo parametro su un valore uguale o maggiore di 1. Per prevenire un utilizzo eccessivo di spazio su disco, si consiglia di non utilizzare il valore predefinito di 0.
<code>binlog_checksum</code>	Imposta questo parametro su NONE per la versione DMS 3.4.7 o precedente.
<code>binlog_row_image</code>	Imposta questo parametro su FULL.
<code>log_slave_updates</code>	Imposta questo parametro su TRUE se stai utilizzando come origine una replica di lettura di MySQL o di MariaDB.

Se l'origine utilizza il motore di database NDB (cluster), i parametri seguenti devono essere configurati per abilitare il CDC sulle tabelle che utilizzano il motore di storage. Aggiungi queste modifiche nel file `my.ini` (Windows) o `my.cnf` (UNIX) di MySQL.

Parametro	Valore
<code>ndb_log_bin</code>	Imposta questo parametro su ON. Questo valore garantisce che le modifiche nelle tabelle cluster vengono registrate nel log binario.

Parametro	Valore
<code>ndb_log_u pdate_as_write</code>	Imposta questo parametro su OFF. Questo valore impedisce la scrittura nel log binario delle istruzioni UPDATE come istruzioni INSERT.
<code>ndb_log_u pdated_only</code>	Imposta questo parametro su OFF. Questo valore garantisce che il log binario contiene l'intera riga e non soltanto le colonne modificate.

Utilizzo di un AWS database compatibile con MySQL gestito come fonte per AWS DMS

È possibile utilizzare i seguenti database AWS gestiti compatibili con MySQL come sorgenti per: AWS DMS

- MySQL Community Edition
- MariaDB Community Edition
- Amazon Aurora edizione compatibile con MySQL

Quando utilizzi un database compatibile con MySQL AWS gestito come fonte per AWS DMS, assicurati di avere i seguenti prerequisiti per CDC:

- Per abilitare i log binari per RDS per MySQL e per RDS per MariaDB, abilita i backup automatici a livello di istanza. Per abilitare i log binari per un cluster Aurora MySQL, modifica la variabile `binlog_format` nel gruppo di parametri.

Per ulteriori informazioni sull'impostazione dei backup automatici, consulta [Abilitazione dei backup automatici](#) nella Guida per l'utente di Amazon RDS.

Per ulteriori informazioni sulla configurazione della registrazione binaria per un database Amazon RDS per MySQL, consulta [Configurazione del log binario](#) nella Guida per l'utente di Amazon RDS.

Per ulteriori informazioni sulla configurazione della registrazione binaria per un cluster MySQL Aurora, consulta [Come posso attivare la registrazione binaria per il cluster Amazon Aurora MySQL edizione compatibile?](#)

- Se intendi utilizzare CDC, attiva la registrazione binaria. Per ulteriori informazioni sulla configurazione della registrazione binaria per un database Amazon RDS per MySQL, consulta [Configurazione del log binario](#) nella Guida per l'utente di Amazon RDS.

- Assicuratevi che i log binari siano disponibili per. AWS DMS Poiché i database compatibili con AWS-managed MySQL eliminano i log binari il prima possibile, è necessario aumentare il periodo di tempo in cui i log rimangono disponibili. Ad esempio, per aumentare il periodo di conservazione dei log binari a 24 ore, esegui il comando seguente.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

- Imposta il parametro `binlog_format` su "ROW".

Note

Su MySQL o MariaDB, `binlog_format` è un parametro dinamico, quindi non è necessario riavviare il computer per rendere effettivo il nuovo valore. Tuttavia, il nuovo valore verrà applicato solo alle nuove sessioni. Se si passa `binlog_format` su ROW per scopi di replica, il database può comunque creare log binari successivi utilizzando il formato MIXED, se tali sessioni sono iniziate prima della modifica del valore. Ciò potrebbe impedire la corretta acquisizione di tutte le modifiche nel AWS DMS database di origine. Quando modifichi l'impostazione `binlog_format` su un database MariaDB o MySQL, assicurati di riavviare il database per chiudere tutte le sessioni esistenti o riavviare qualsiasi applicazione che esegua operazioni DML (Data Manipulation Language). Forzando il database a riavviare tutte le sessioni dopo aver modificato il `binlog_format` parametro, ROW si assicurerà che il database scriva tutte le successive modifiche al database di origine utilizzando il formato corretto, in modo che sia AWS DMS possibile acquisire correttamente tali modifiche.

- Imposta il parametro `binlog_row_image` su "Full".
- Imposta il `binlog_checksum` parametro su "NONE" DMS versione 3.4.7 o precedente. Per ulteriori informazioni sull'impostazione dei parametri in Amazon RDS MySQL, consulta [Abilitazione dei backup automatici](#) nella Guida per l'utente di Amazon RDS.
- Se stai utilizzando una replica di lettura Amazon RDS MySQL o Amazon RDS MariaDB come origine, abilita i backup sulla replica di lettura e assicurati che il parametro `log_slave_updates` sia impostato su TRUE.

Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS

Quando si utilizza un database MySQL come origine, considerare quanto segue:

- L'acquisizione dei dati di modifica (CDC) non è supportata per Amazon RDS MySQL 5.5 o versioni precedenti. Per Amazon RDS MySQL, è necessario utilizzare la versione 5.6, 5.7 o 8.0 per abilitare CDC. CDC è supportata per origini MySQL 5.5 autogestite.
- Per CDC, `CREATE TABLE`, `ADD COLUMN` e `DROP COLUMN` che modificano il tipo di dati di colonne e `renaming a column` sono supportati. Tuttavia `DROP TABLE`, `RENAME TABLE` e gli aggiornamenti apportati ad altri attributi, come il valore predefinito della colonna, la nullabilità delle colonne, il set di caratteri e così via, non sono supportati.
- Per le tabelle partizionate sull'origine, quando si imposta la modalità di preparazione della tabella di Target su `Drop tables on target`, AWS DMS crea una tabella semplice senza partizioni sulla destinazione MySQL. Per eseguire la migrazione di tabelle partizionate a una tabella partizionata nella destinazione, crea in anticipo le tabelle partizionate nel database di destinazione MySQL.
- L'utilizzo di un'istruzione `ALTER TABLE table_name ADD COLUMN column_name` per aggiungere colonne all'inizio (`FIRST`) o a metà di una tabella (`AFTER`) non è supportato. Le colonne vengono sempre aggiunte alla fine della tabella.
- Il CDC non è supportato quando un nome di tabella contiene caratteri maiuscoli e minuscoli e il motore di origine è ospitato in un sistema operativo con nomi di file che non fanno distinzione tra lettere maiuscole e minuscole. Un esempio è Microsoft Windows oppure OS X che utilizza HFS +.
- Puoi usare Aurora, compatibile con MySQL, Edition Serverless v1 a pieno carico, ma non puoi usarlo per CDC. perché non è possibile abilitare i prerequisiti per MySQL. Per ulteriori informazioni, consulta [Parameter groups and Aurora Serverless v1](#).

L'edizione Serverless v2 compatibile con Aurora MySQL supporta CDC.

- L'attributo `AUTO_INCREMENT` di una colonna non viene migrato a una colonna del database di destinazione.
- L'acquisizione delle modifiche quando i log binari non sono archiviati su uno storage a blocchi standard non è supportata. Ad esempio, CDC non funziona quando i log binari sono archiviati su Amazon S3.
- AWS DMS crea tabelle di destinazione con il motore di archiviazione InnoDB per impostazione predefinita. Se è necessario utilizzare un motore di storage diverso da InnoDB, occorre creare manualmente la tabella ed eseguirvi la migrazione utilizzando la modalità [nessuna azione](#).
- Non è possibile utilizzare le repliche Aurora MySQL come origine, a AWS DMS meno che la modalità attività di migrazione DMS non sia Migra dati esistenti, solo a pieno carico.

- Se l'origine compatibile con MySQL viene arrestata durante il caricamento completo, l'attività AWS DMS non si arresta con un errore. L'attività termina correttamente, ma la destinazione potrebbe non essere sincronizzata con l'origine. In questo caso, riavvia l'attività o ricarica le tabelle interessate.
- Gli indici creati su una parte di un valore di colonna non vengono migrati. Ad esempio, l'indice `CREATE INDEX first_ten_chars ON customer (name(10))` non viene creato nella destinazione.
- In alcuni casi, l'attività è configurata per non replicare i LOB (« SupportLobs "è false nelle impostazioni dell'attività oppure l'opzione Non includere le colonne LOB è stata scelta nella console attività»). In questi casi, AWS DMS non migra alcuna colonna MEDIUMBLOB, LONGBLOB, MEDIUMTEXT e LONGTEXT verso la destinazione.

Le colonne BLOB, TINYBLOB, TEXT e TINYTEXT non sono interessate e vengono migrate nella destinazione.

- Le tabelle di dati temporali o le tabelle con versioni di sistema non sono supportate nei database di origine e di destinazione di MariaDB.
- Se si esegue la migrazione tra due cluster Amazon RDS Aurora MySQL, l'endpoint di origine RDS Aurora MySQL deve essere un'istanza di lettura/scrittura, non un'istanza di replica.
- AWS DMS attualmente non supporta la migrazione delle visualizzazioni per MariaDB.
- AWS DMS non supporta le modifiche DDL per le tabelle partizionate per MySQL. Per ignorare la sospensione della tabella per le modifiche DDL della partizione durante CDC, imposta `skipTableSuspensionForPartitionDdl` su `true`.
- AWS DMS supporta solo transazioni XA nella versione 3.5.0 e successive. Le versioni precedenti non supportano le transazioni XA. AWS DMS non supporta le transazioni XA nella versione 10.6 di MariaDB. Per ulteriori informazioni, consulta la sezione seguente: [the section called “Supporto per transazione XA”](#).
- AWS DMS non utilizza i GTID per la replica, anche se i dati di origine li contengono.
- AWS DMS non supporta la compressione delle transazioni di registro binario.
- AWS DMS non propaga gli eventi ON DELETE CASCADE e ON UPDATE CASCADE per i database MySQL utilizzando il motore di archiviazione InnoDB. Per questi eventi, MySQL non genera eventi binlog per riflettere le operazioni a cascata sulle tabelle secondarie. Di conseguenza, non AWS DMS è possibile replicare le modifiche corrispondenti alle tabelle secondarie. Per ulteriori informazioni, consulta [Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati](#).
- AWS DMS non acquisisce le modifiche alle colonne calcolate (`VIRTUALEGENERATED ALWAYS`). Per ovviare a questa limitazione, esegui queste operazioni:

- Crea in anticipo la tabella di destinazione nel database di destinazione e crea l'attività AWS DMS con l'impostazione dell'attività di pieno carico `DO_NOTHING` o `TRUNCATE_BEFORE_LOAD`.
- Aggiungi una regola di trasformazione per rimuovere la colonna calcolata dall'ambito dell'attività. Per informazioni sulle regole di trasformazione, consulta [Operazioni e regole di trasformazione](#).

Supporto per transazione XA

Una transazione Extended Architecture (XA) è una transazione che può essere utilizzata per raggruppare una serie di operazioni da più risorse transazionali in un'unica transazione globale affidabile. Una transazione XA utilizza un protocollo di commit in due fasi. In generale, l'acquisizione delle modifiche mentre sono presenti transazioni XA aperte potrebbe portare alla perdita di dati. Se il database non utilizza transazioni XA, puoi ignorare questa autorizzazione e la configurazione `IgnoreOpenXaTransactionsCheck` utilizzando il valore predefinito `TRUE`. Per iniziare la replica da un'origine che contiene transazioni XA, effettua le seguenti operazioni:

- Assicurati che l'utente dell' AWS DMS endpoint disponga delle seguenti autorizzazioni:

```
grant XA_RECOVER_ADMIN on *.* to 'userName'@'%';
```

- Configura l'impostazione dell'endpoint `IgnoreOpenXaTransactionsCheck` su `false`.

Note

AWS DMS non supporta le transazioni XA su MariaDB Source DB versione 10.6.

Impostazioni degli endpoint quando si utilizza MySQL come sorgente per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine MySQL in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in [AWS CLI](#), con la sintassi JSON. `--my-sql-settings '{"EndpointSetting": "value", ...}'`

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con MySQL come origine.

Nome	Descrizione
EventsPollInterval	<p>Specifica la frequenza di controllo del log binario per nuove modifiche/eventi quando il database è inattivo.</p> <p>Valore predefinito: 5</p> <p>Valori validi: 1-60</p> <p>Esempio: <code>--my-sql-settings '{"EventsPollInterval": 5}'</code></p> <p>Nell'esempio, AWS DMS verifica le modifiche nei log binari ogni cinque secondi.</p>
ExecuteTimeout	<p>Per AWS DMS le versioni 3.4.7 e successive, imposta il timeout dell'istruzione client per un endpoint di origine MySQL, in secondi.</p> <p>Valore predefinito: 60</p> <p>Esempio: <code>--my-sql-settings '{"ExecuteTimeout": 1500}'</code></p>
ServerTimezone	<p>Specifica il fuso orario del database di origine MySQL.</p> <p>Esempio: <code>--my-sql-settings '{"ServerTimezone": "US/Pacific"}</code></p>
AfterConnectScript	<p>Specifica uno script da eseguire immediatamente dopo la connessione all'endpoint. AWS DMS L'esecuzione dell'attività di migrazione continua a prescindere se l'istruzione SQL riesce o non riesce.</p> <p>I valori validi: una o più istruzioni SQL valide, attivate da un punto e virgola.</p> <p>Esempio: <code>--my-sql-settings '{"AfterConnectScript": "ALTER SESSION SET CURRENT_SCHEMA=system"}</code></p>

Nome	Descrizione
CleanSrcMetadataOnMismatch	<p>Esegue la pulizia e crea nuovamente le informazioni dei metadati delle tabelle sull'istanza di replica se si verifica una mancata corrispondenza. Ad esempio, in una situazione in cui l'esecuzione di un'alterazione DDL sulla tabella potrebbe avere come risultato informazioni diverse relative alla tabella memorizzata nella cache nell'istanza di replica. booleano.</p> <p>Valore predefinito: <code>false</code></p> <p>Esempio: <code>--my-sql-settings '{"CleanSrcMetadataOnMismatch": false}'</code></p>
skipTableSuspensionForPartitionDdl	<p>AWS DMS non supporta le modifiche DDL per le tabelle partizionate per MySQL. Per AWS DMS le versioni 3.4.6 e successive, impostandola in modo da <code>true</code> ignorare la sospensione della tabella per le modifiche DDL della partizione durante il CDC. AWS DMS ignora <code>partition ed-table-related DDL</code> e continua a elaborare ulteriori modifiche al registro binario.</p> <p>Valore predefinito: <code>false</code></p> <p>Esempio: <code>--my-sql-settings '{"skipTableSuspensionForPartitionDdl": true}'</code></p>
IgnoreOpenXaTransactionsCheck	<p>Per AWS DMS le versioni 3.5.0 e successive, specifica se le attività devono ignorare le transazioni XA aperte all'avvio. Imposta su <code>false</code> se l'origine ha transazioni XA.</p> <p>Valore predefinito: <code>true</code></p> <p>Esempio: <code>--my-sql-settings '{"IgnoreOpenXaTransactionsCheck": false}'</code></p>

Tipi di dati di origine per MySQL

La tabella seguente mostra i tipi di dati di origine del database MySQL supportati durante l' AWS DMS utilizzo e la AWS DMS mappatura predefinita dei tipi di dati.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere. [Tipi di dati per AWS Database Migration Service](#)

Tipi di dati MySQL	AWS DMS tipi di dati
INT	INT4
BIGINT	INT8
MEDIUMINT	INT4
TINYINT	INT1
SMALLINT	INT2
UNSIGNED TINYINT	UINT1
UNSIGNED SMALLINT	UINT2
UNSIGNED MEDIUMINT	UINT4
UNSIGNED INT	UINT4
UNSIGNED BIGINT	UINT8
DECIMAL(10)	NUMERIC (10,0)
BINARY	BYTES(1)
BIT	BOOLEAN
BIT(64)	BYTES(8)
BLOB	BYTES(65535)

Tipi di dati MySQL	AWS DMS tipi di dati
LONGBLOB	BLOB
MEDIUMBLOB	BLOB
TINYBLOB	BYTES(255)
DATE	DATE
DATETIME	<p>DATETIME</p> <p>DATETIME senza un valore tra parentesi viene replicato senza millisecondi. DATETIME con un valore tra parentesi compreso tra 1 e 5 (ad esempio DATETIME(5)) viene replicato con i millisecondi.</p> <p>Quando si replica una colonna DATETIME, l'ora rimane la stessa sulla destinazione. Non viene convertita in UTC.</p>
TIME	STRING
TIMESTAMP	<p>DATETIME</p> <p>Quando si replica una colonna TIMESTAMP, l'ora viene convertita in UTC sulla destinazione.</p>
ANNO	INT2
DOUBLE	REAL8

Tipi di dati MySQL	AWS DMS tipi di dati
FLOAT	REAL(DOUBLE) Se i valori FLOAT non sono compresi nell'intervallo seguente, usa una trasformazione per mappare FLOAT su STRING. Per ulteriori informazioni sulle trasformazioni, consulta Operazioni e regole di trasformazione . L'intervallo FLOAT supportato è da -1.79E+308 a -2.23E-308, 0 e da 2.23E-308 a 1.79E+308
VARCHAR (45)	WSTRING (45)
VARCHAR (2000)	WSTRING (2000)
VARCHAR (4000)	WSTRING (4000)
VARBINARY (4000)	BYTES (4000)
VARBINARY (2000)	BYTES (2000)
CHAR	WSTRING
TEXT	WSTRING
LONGTEXT	NCLOB
MEDIUMTEXT	NCLOB
TINYTEXT	WSTRING(255)
GEOMETRY	BLOB
POINT	BLOB
LINestring	BLOB
POLYGON	BLOB

Tipi di dati MySQL	AWS DMS tipi di dati
MULTIPOINT	BLOB
MULTILINESTRING	BLOB
MULTIPOLYGON	BLOB
GEOMETRYCOLLECTION	BLOB
ENUM	WSTRING (<i>length</i>) Qui, <i>length</i> è la lunghezza del valore più lungo nell'ENUM.
SET	WSTRING (<i>length</i>) Qui, <i>length</i> è la lunghezza totale di tutti i valori nel SET, comprese le virgole.
JSON	CLOB

Note

In alcuni casi, è possibile specificare i tipi di dati DATETIME e TIMESTAMP con un valore "zero" (ovvero 0000-00-00). In tal caso, assicurati che il database di destinazione nell'attività di replica supporti valori "zero" per i tipi di dati DATETIME e TIMESTAMP. In caso contrario, tali valori vengono registrati come null nella destinazione.

Utilizzo di un database SAP ASE come origine per AWS DMS

Puoi eseguire la migrazione dei dati ai database di SAP Adaptive Server Enterprise (ASE), precedentemente denominato Sybase, mediante AWS DMS. Con un database SAP ASE come origine, puoi eseguire la migrazione dei dati da tutti gli altri database di destinazione AWS DMS supportati.

Per informazioni sulle versioni di SAP ASE supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Per ulteriori informazioni sull'utilizzo dei database SAP ASE e AWS DMS, consulta le seguenti sezioni.

Argomenti

- [Prerequisiti per l'utilizzo di un database SAP ASE come origine per AWS DMS](#)
- [Limitazioni dell'utilizzo di SAP ASE come origine per AWS DMS](#)
- [Autorizzazioni necessarie per utilizzare SAP ASE come origine per AWS DMS](#)
- [Rimozione del punto di troncamento](#)
- [Impostazioni degli endpoint quando si utilizza SAP ASE come origine per AWS DMS](#)
- [Tipi di dati di origine per SAP ASE](#)

Prerequisiti per l'utilizzo di un database SAP ASE come origine per AWS DMS

Affinché un database SAP ASE possa essere un'origine per AWS DMS, eseguire le operazioni seguenti:

- Abilita la replica SAP ASE per le tabelle utilizzando il comando `sp_setreptable`. Per ulteriori informazioni, consulta [Sybase Infocenter Archive](#).
- Disabilita RepAgent sul database SAP ASE. Per ulteriori informazioni, consulta [Stop and disable the RepAgent thread in the primary database](#).
- Per eseguire la replica alla versione 15.7 di SAP ASE su un'istanza Windows EC2 configurata per caratteri non latini (ad esempio, il cinese), installa SAP ASE 15.7 SP121 sul computer di destinazione.

Note

Per la replica continua, l'acquisizione dei dati di modifica (CDC), DMS esegue `dbcc logtransfer` e `dbcc log` per leggere i dati del log delle transazioni.

Limitazioni dell'utilizzo di SAP ASE come origine per AWS DMS

Quando si utilizza un database SAP ASE come origine per AWS DMS, si applicano le seguenti limitazioni:

un'operazione DML (INSERT, UPDATE, DELETE) seguita dall'eliminazione della tabella, è necessario riavviare l'attività di replica.

Autorizzazioni necessarie per utilizzare SAP ASE come origine per AWS DMS

Per utilizzare un database SAP ASE come origine in un'attività AWS DMS, è necessario concedere le autorizzazioni. Concedi all'account utente specificato nelle definizioni del database AWS DMS le seguenti autorizzazioni nel database SAP ASE:

- sa_role
- replication_role
- sybase_ts_role
- Per impostazione predefinita, quando è necessario disporre dell'autorizzazione per eseguire la stored procedure `sp_setreptable`, AWS DMS abilita l'opzione di replica SAP ASE. Se si desidera eseguire `sp_setreptable` su una tabella direttamente dall'endpoint del database e non tramite AWS DMS, è possibile utilizzare l'attributo aggiuntivo di connessione `enableReplication`. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza SAP ASE come origine per AWS DMS](#).

Rimozione del punto di troncamento

Quando un'attività viene avviata, AWS DMS stabilisce una voce `$replication_truncation_point` nella vista di sistema `syslogshold` che indica che è in corso un processo di replica. Mentre AWS DMS è in funzione, porta in avanti il punto di troncamento della replica a intervalli regolari, in base alla quantità di dati che è già stata copiata nella destinazione.

Una volta stabilita la voce `$replication_truncation_point`, mantieni l'attività AWS DMS in esecuzione per evitare che il log di database diventi eccessivamente grande. Se desideri arrestare permanentemente l'attività AWS DMS, rimuovi il punto di troncamento della replica eseguendo il comando seguente:

```
dbcc settrunc('ltm','ignore')
```

Dopo la rimozione del punto di troncamento, non potrai riprendere l'attività AWS DMS. Il log continua a essere automaticamente troncato ai checkpoint (se è impostato il troncamento automatico).

Impostazioni degli endpoint quando si utilizza SAP ASE come origine per AWS DMS

È possibile utilizzare le impostazioni di endpoint per configurare il database di origine SAP ASE in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--sybase-settings '{"EndpointSetting": "value", ...}'`.

Nella tabella seguente vengono elencate le impostazioni dell'endpoint che è possibile utilizzare con SAP ASE come origine.

Nome	Descrizione
Charset	<p>Imposta questo attributo sul nome SAP ASE che corrisponde al set di caratteri internazionali.</p> <p>Valore predefinito: <code>iso_1</code></p> <p>Esempio: <code>--sybase-settings '{"Charset": "utf8"}'</code></p> <p>Valori validi:</p> <ul style="list-style-type: none"> • <code>acsii_8</code> • <code>big5hk</code> • <code>cp437</code> • <code>cp850</code> • <code>cp852</code> • <code>cp852</code> • <code>cp855</code> • <code>cp857</code> • <code>cp858</code> • <code>cp860</code> • <code>cp864</code> • <code>cp866</code> • <code>cp869</code>

Nome	Descrizione
	<ul style="list-style-type: none">• cp874• cp932• cp936• cp950• cp1250• cp1251• cp1252• cp1253• cp1254• cp1255• cp1256• cp1257• cp1258• deckanji• euccns• eucgb• eucjis• eucksc• gb18030• greek8• iso_1• iso88592• iso88595• iso88596• iso88597• iso88598• iso88599• iso15• kz1048

Nome	Descrizione
	<ul style="list-style-type: none"> • koi8 • roman8 • iso88599 • sjis • tis620 • turkish8 • utf8 <p>Per ulteriori domande sui set di caratteri supportati in un database SAP ASE, consulta Adaptive Server Enterprise: Supported character sets.</p>
EnableReplication	<p>Imposta questo attributo se desideri abilitare <code>sp_setrep table</code> sulle tabelle dal lato database e non da AWS DMS.</p> <p>Valore predefinito: true</p> <p>Valori validi: true o false</p> <p>Esempio: <code>--sybase-settings '{"Enable Replication": false}'</code></p>
EncryptPassword	<p>Imposta questo attributo se hai abilitato "net password encryption reqd" nel database di origine.</p> <p>Valore predefinito: 0</p> <p>Valori validi: 0, 1 o 2</p> <p>Esempio: <code>--sybase-settings '{"EncryptPassword": 1}'</code></p> <p>Per ulteriori informazioni su questi valori dei parametri, consulta Adaptive Server Enterprise: Using the EncryptPassword Connection string property.</p>

Nome	Descrizione
Provider	<p>Imposta questo attributo se desideri utilizzare Transport Layer Security (TLS) 1.2 per ASE 15.7 e versioni successive. Tieni presente che AWS richiede TLS 1.2 o versioni successive e si consiglia la versione 1.3.</p> <p>Valore predefinito: Adaptive Server Enterprise</p> <p>Valori validi: Adaptive Server Enterprise 16.03.06</p> <p>Esempio: <code>--sybase-settings '{"Provider": "Adaptive Server Enterprise 16.03.06"}'</code></p>

Tipi di dati di origine per SAP ASE

Per un elenco dei tipi di dati di origine SAP ASE che sono supportati quando utilizzi AWS DMS e la mappatura predefinita dai tipi di AWS DMS, consulta la tabella seguente. AWS DMS non supporta tabelle di origine SAP ASE con colonne del tipo di dati definito dall'utente (UDT). Le colonne replicate con questo tipo di dati sono create come NULL.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la [Destinazioni per la migrazione dei dati](#) sezione relativa all'endpoint di destinazione.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati SAP ASE	Tipi di dati AWS DMS
BIGINT	INT8
UNSIGNED BIGINT	UINT8
INT	INT4
UNSIGNED INT	UINT4
SMALLINT	INT2

Tipi di dati SAP ASE	Tipi di dati AWS DMS
UNSIGNED SMALLINT	UINT2
TINYINT	UINT1
DECIMAL	NUMERIC
NUMERIC	NUMERIC
FLOAT	REAL8
DOUBLE	REAL8
REAL	REAL4
MONEY	NUMERIC
SMALLMONEY	NUMERIC
DATETIME	DATETIME
BIGDATETIME	DATETIME(6)
SMALLDATETIME	DATETIME
DATE	DATE
TIME	TIME
BIGTIME	TIME
CHAR	STRING
UNICHAR	WSTRING
NCHAR	WSTRING
VARCHAR	STRING
UNIVARCHAR	WSTRING

Tipi di dati SAP ASE	Tipi di dati AWS DMS
NVARCHAR	WSTRING
BINARY	BYTES
VARBINARY	BYTES
BIT	BOOLEAN
TEXT	CLOB
UNITEXT	NCLOB
IMAGE	BLOB

Utilizzo di MongoDB come origine per AWS DMS

Per informazioni sulle versioni di MongoDB supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Tieni presente quanto segue in relazione al supporto delle versioni di MongoDB:

- AWS DMS 3.4.5 e le versioni successive supportano MongoDB versione 4.2 e 4.4.
- AWS DMS 3.4.5 e le versioni successive e MongoDB 4.2 e le versioni successive supportano le transazioni distribuite. Per ulteriori informazioni sulle transazioni distribuite MongoDB, consulta [Transactions](#) nella [documentazione di MongoDB](#).
- AWS DMS 3.5.0 e le versioni successive non supportano le versioni di MongoDB precedenti alla 3.6.
- AWS DMS 3.5.1 e le versioni successive supportano MongoDB versione 5.0.
- AWS DMS 3.5.2 e le versioni successive supportano MongoDB versione 6.0.

Se non conosci MongoDB, è necessario avere familiarità con i seguenti importanti concetti del database MongoDB:

- Un record in MongoDB è un documento che è una struttura di dati costituita da coppie di campi e di valori. Il valore di un campo può includere altri documenti, matrici e matrici di documenti. Un documento è approssimativamente equivalente a una riga di una tabella di database relazionali.
- Una raccolta in MongoDB è un gruppo di documenti ed è approssimativamente equivalente a una tabella di database relazionale.
- Un database in MongoDB è un set di raccolte ed è approssimativamente equivalente a uno schema di database relazionale.
- Internamente, un documento MongoDB viene memorizzato come un file JSON binario (BSON) in un formato compresso che include un tipo per ogni campo del documento. Ogni documento ha un ID univoco.

Quando si usa MongoDB come origine, AWS DMS supporta due modalità di migrazione: documento o tabella. È possibile specificare la modalità di migrazione da utilizzare quando si crea l'endpoint MongoDB o impostando il parametro Modalità metadati dalla console AWS DMS. Facoltativamente, puoi creare una seconda colonna denominata `_id` che funge da chiave primaria selezionando il pulsante con il segno di spunta per `_id` come colonna separata nel pannello di configurazione dell'endpoint.

La scelta della modalità di migrazione influenza il formato risultante dei dati di destinazione come descritto di seguito.

Modalità documento

In modalità documento, il documento MongoDB viene migrato così com'è, vale a dire che i dati del documento vengono consolidati in una singola colonna denominata `_doc` in una tabella di destinazione. La modalità documento è l'impostazione predefinita quando si utilizza MongoDB come endpoint di origine.

Ad esempio, considera i seguenti documenti in una raccolta MongoDB denominata `myCollection`.

```
> db.myCollection.find()
{ "_id" : ObjectId("5a94815f40bd44d1b02bdfe0"), "a" : 1, "b" : 2, "c" : 3 }
{ "_id" : ObjectId("5a94815f40bd44d1b02bdfe1"), "a" : 4, "b" : 5, "c" : 6 }
```

Una volta completata la migrazione dei dati a una tabella di database relazionale utilizzando la modalità documento, i dati vengono strutturati come segue. I campi dei dati nel documento MongoDB sono consolidati nella colonna `_doc`.

oid_id	_doc
5a94815f40bd44d1b02bdfe0	{ "a" : 1, "b" : 2, "c" : 3 }
5a94815f40bd44d1b02bdfe1	{ "a" : 4, "b" : 5, "c" : 6 }

Puoi impostare facoltativamente l'attributo di connessione aggiuntivo `extractDocID` su `true` per creare una seconda colonna denominata "`_id`" che agisca come chiave primaria. Se prevedi di utilizzare CDC, imposta questo parametro su `true`.

In modalità documento, AWS DMS gestisce la creazione e la ridenominazione di raccolte in modo simile al seguente:

- Se aggiungi una nuova raccolta al database di origine, AWS DMS crea una nuova tabella di destinazione per la raccolta ed esegue la replica di tutti i documenti.
- Se rinomini una raccolta esistente nel database di origine, AWS DMS non rinomina la tabella di destinazione.

Se l'endpoint di destinazione è Amazon DocumentDB, esegui la migrazione in modalità documento.

Modalità tabella

In modalità tabella, AWS DMS trasforma ogni campo di primo livello all'interno di un documento MongoDB in una colonna nella tabella di destinazione. Se un campo è nidificato, AWS DMS appiattisce i valori nidificati in una singola colonna. AWS DMS quindi aggiunge un campo chiave e tipi di dati al set di colonne della tabella di destinazione.

Per ogni documento MongoDB, AWS DMS aggiunge ciascuna chiave e il tipo al set di colonne della tabella di destinazione. Ad esempio, usando la modalità tabella, AWS DMS esegue la migrazione dell'esempio precedente nella tabella riportata di seguito.

oid_id	a	b	c
5a94815f40bd44d1b02bdfe0	1	2	3
5a94815f40bd44d1b02bdfe1	4	5	6

I valori nidificati sono appiattiti in una colonna contenente nomi di chiavi separati da punti. La colonna è denominata dalla concatenazione dei nomi di campo appiattiti separati da punti. Ad esempio, AWS DMS migra un documento JSON con un campo di valori nidificati, ad esempio `{"a" : {"b" : {"c" : 1}}}`, in una colonna denominata `a.b.c`.

Per creare le colonne di destinazione, AWS DMS analizza un determinato numero di documenti MongoDB e crea un set di tutti i campi e dei relativi tipi. AWS DMS quindi utilizza questo set per creare le colonne della tabella di destinazione. Se crei o modifichi l'endpoint di origine di MongoDB utilizzando la console, è possibile specificare il numero di documenti per la scansione. Il valore predefinito è 1000 documenti. Se utilizzi la AWS CLI, puoi usare l'attributo aggiuntivo di connessione `docsToInvestigate`.

In modalità tabella, AWS DMS gestisce documenti e raccolte in modo simile al seguente:

- Quando aggiungi un documento in una raccolta esistente, il documento viene replicato. Se ci sono campi che non esistono nella destinazione, tali campi non vengono replicati.
- Quando aggiorni un documento, il documento aggiornato viene replicato. Se ci sono campi che non esistono nella destinazione, tali campi non vengono replicati.
- L'eliminazione di un documento è supportata integralmente.
- L'aggiunta di una nuova raccolta non ha come risultato una nuova tabella nella destinazione durante un'attività CDC.
- Nella fase dell'acquisizione dei dati di modifica (CDC), AWS DMS non supporta la ridenominazione di una raccolta.

Argomenti

- [Autorizzazioni necessarie per l'uso di MongoDB come origine per AWS DMS](#)
- [Configurazione di un set di repliche MongoDB per CDC](#)
- [Requisiti di sicurezza per l'uso di MongoDB come origine per AWS DMS](#)
- [Segmentazione delle raccolte MongoDB e migrazione in parallelo](#)
- [Migrazione di più database quando si utilizza MongoDB come origine per AWS DMS](#)
- [Limitazioni relative all'utilizzo di MongoDB come origine per AWS DMS](#)
- [Impostazioni di configurazione degli endpoint quando si utilizza MongoDB come origine per AWS DMS](#)
- [Tipi di dati di origine per MongoDB](#)

Autorizzazioni necessarie per l'uso di MongoDB come origine per AWS DMS

Per una migrazione AWS DMS con un'origine MongoDB, puoi creare un account utente con privilegi root o un utente con autorizzazioni solo per il database di cui eseguire la migrazione.

Il codice seguente crea un utente come account root.

```
use admin
db.createUser(
  {
    user: "root",
    pwd: "password",
    roles: [ { role: "root", db: "admin" } ]
  }
)
```

Per un'origine MongoDB 3.x, il codice seguente crea un utente con privilegi minimi sul database da migrare.

```
use database_to_migrate
db.createUser(
  {
    user: "dms-user",
    pwd: "password",
    roles: [ { role: "read", db: "local" }, "read" ]
  })
```

Per un'origine MongoDB 4.x, il codice seguente crea un utente con privilegi minimi.

```
{ resource: { db: "", collection: "" }, actions: [ "find", "changeStream" ] }
```

Ad esempio, crea il seguente ruolo nel database "admin".

```
use admin
db.createRole(
  {
    role: "changestreamrole",
    privileges: [
      { resource: { db: "", collection: "" }, actions: [ "find","changeStream" ] }
    ],
    roles: []
  })
```

```
}  
)
```

Una volta creato il ruolo, crea un utente nel database da migrare.

```
> use test  
> db.createUser(  
  {  
    user: "dms-user12345",  
    pwd: "password",  
    roles: [ { role: "changestreamrole", db: "admin" }, "read"]  
  })
```

Configurazione di un set di repliche MongoDB per CDC

Per usare la replica continua o la CDC con MongoDB, AWS DMS richiede l'accesso al log delle operazioni (oplog) di MongoDB. Per creare l'oplog, devi distribuire un set di repliche se non esiste già. Per ulteriori informazioni, consulta la [documentazione di MongoDB](#).

Puoi utilizzare il CDC con il nodo primario o secondario di un set di repliche MongoDB come endpoint di origine.

Per convertire un'istanza autonoma in un set di repliche

1. Utilizzando la riga di comando, collegati a mongo.

```
mongo localhost
```

2. Arresta il servizio mongod.

```
service mongod stop
```

3. Riavvia mongod utilizzando il seguente comando:

```
mongod --replSet "rs0" --auth -port port_number
```

4. Verifica la connessione al set di repliche utilizzando i comandi seguenti:

```
mongo -u root -p password --host rs0/localhost:port_number  
  --authenticationDatabase "admin"
```

Se prevedi di eseguire una migrazione in modalità documento, seleziona l'opzione `_id as a separate column` quando crei l'endpoint di MongoDB. Se selezioni questa opzione, viene creata una seconda colonna denominata `_id` che agisce come chiave primaria. Questa seconda colonna è necessaria ad AWS DMS per supportare operazioni DML (Data Manipulation Language).

Note

AWS DMS utilizza il log delle operazioni (oplog) per acquisire le modifiche durante la replica continua. Se MongoDB elimina i record dall'oplog prima che AWS DMS li legga, le attività non riescono. Ti consigliamo di dimensionare l'oplog in modo da mantenere le modifiche per almeno 24 ore.

Requisiti di sicurezza per l'uso di MongoDB come origine per AWS DMS

AWS DMS supporta i seguenti due metodi di autenticazione per MongoDB. I due metodi di autenticazione vengono utilizzati per crittografare la password, in modo che vengano utilizzati solo quando il parametro `authType` è impostato su `PASSWORD`.

I metodi di autenticazione di MongoDB sono i seguenti:

- `MONGODB-CR`: per la compatibilità con le versioni precedenti
- `SCRAM-SHA-1`: l'impostazione predefinita quando si utilizza MongoDB versione 3.x e 4.0

Se non è specificato un metodo di autenticazione, AWS DMS usa il metodo predefinito per la versione dell'origine MongoDB.

Segmentazione delle raccolte MongoDB e migrazione in parallelo

Per migliorare le prestazioni di un'attività di migrazione, gli endpoint di origine MongoDB supportano due opzioni per il pieno carico parallelo nella mappatura delle tabelle.

In altre parole, è possibile migrare una raccolta in parallelo utilizzando la segmentazione automatica o la segmentazione degli intervalli con la mappatura delle tabelle per il pieno carico parallelo nelle impostazioni JSON. Con la segmentazione automatica, puoi specificare i criteri che AWS DMS utilizza per segmentare automaticamente l'origine per la migrazione in ogni thread. Con la segmentazione degli intervalli puoi indicare ad AWS DMS l'intervallo specifico di ogni segmento che DMS deve migrare in ogni thread. Per ulteriori informazioni su queste impostazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Migrazione di un database MongoDB in parallelo utilizzando gli intervalli di segmentazione automatica

Puoi migrare i tuoi documenti in parallelo specificando i criteri che AWS DMS utilizza per partizionare (segmentare) automaticamente i dati per ogni thread. In particolare, si specifica il numero di documenti da migrare per thread. Utilizzando questo approccio, AWS DMS tenta di ottimizzare i limiti dei segmenti per ottenere le massime prestazioni per ogni thread.

È possibile specificare i criteri di segmentazione utilizzando le opzioni di impostazione della tabella riportate di seguito nella mappatura delle tabelle.

Opzione delle impostazioni della tabella	Descrizione
"type"	(Obbligatoria) Impostata su "partitions-auto" per MongoDB come origine.
"number-of-partitions"	(Facoltativa) Numero totale di partizioni (segmenti) utilizzate per la migrazione. Il valore predefinito è 16.
"collection-count-from-metadata"	(Facoltativa) Se questa opzione è impostata su <code>true</code> , AWS DMS utilizza un conteggio di raccolte stimato per determinare il numero di partizioni. Se è impostata su <code>false</code> , AWS DMS utilizza il numero effettivo di raccolte. Il valore predefinito è <code>true</code> .
"max-records-skip-per-page"	(Facoltativa) Il numero di record da ignorare contemporaneamente quando si determinano i limiti di ogni partizione. AWS DMS utilizza un approccio per ignorare con impaginazione per determinare il limite minimo di una partizione. Il valore predefinito è 10.000. L'impostazione di un valore relativamente elevato può causare timeout del cursore e errori delle attività. L'impostazione di un valore relativamente basso comporta un numero

Opzione delle impostazioni della tabella	Descrizione
	maggior numero di operazioni per pagina e un pieno carico più lento.
"batch-size"	(Facoltativa) Limita il numero di documenti restituiti in un batch. Ogni batch richiede un round trip al server. Se la dimensione del batch è zero (0), il cursore utilizza la dimensione massima del batch definita dal server. Il valore predefinito è 0.

L'esempio seguente mostra una mappatura delle tabelle per la segmentazione automatica.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "admin",
        "table-name": "departments"
      },
      "rule-action": "include",
      "filters": []
    },
    {
      "rule-type": "table-settings",
      "rule-id": "2",
      "rule-name": "2",
      "object-locator": {
        "schema-name": "admin",
        "table-name": "departments"
      },
      "parallel-load": {
        "type": "partitions-auto",
        "number-of-partitions": 5,
        "collection-count-from-metadata": "true",
        "max-records-skip-per-page": 1000000,
        "batch-size": 50000
      }
    }
  ]
}
```



```
}  
  }  
] }  
}
```

La segmentazione automatica presenta le seguenti limitazioni. La migrazione di ogni segmento recupera separatamente il conteggio di raccolte e il valore `_id` minimo della raccolta. Quindi utilizza l'approccio per ignorare con impaginazione per calcolare il limite minimo del segmento.

Pertanto, assicurati che il valore `_id` minimo di ogni raccolta rimanga costante fino al calcolo di tutti i limiti del segmento della raccolta. La modifica del valore `_id` minimo di una raccolta durante il calcolo dei limiti del segmento può causare la perdita di dati o errori di riga duplicata.

Migrazione di un database MongoDB in parallelo utilizzando la segmentazione degli intervalli

Puoi migrare i documenti in parallelo specificando gli intervalli per ogni segmento di un thread. Utilizzando questo approccio, indichi ad AWS DMS i documenti specifici da migrare in ogni thread in base alla scelta degli intervalli di documenti per thread.

L'immagine seguente mostra una raccolta MongoDB con sette elementi e `_id` come chiave primaria.

Key	Value	Type
▼ (1) ObjectId("5f805c74873173399a278d78")	{ 3 fields }	Object
_id	ObjectId("5f805c74873173399a278d78")	ObjectId
num	1	Int32
name	a	String
▼ (2) ObjectId("5f805c97873173399a278d79")	{ 3 fields }	Object
_id	ObjectId("5f805c97873173399a278d79")	ObjectId
num	2	Int32
name	b	String
▼ (3) ObjectId("5f805cb0873173399a278d7a")	{ 3 fields }	Object
_id	ObjectId("5f805cb0873173399a278d7a")	ObjectId
num	3	Int32
name	c	String
▼ (4) ObjectId("5f805cbb873173399a278d7b")	{ 3 fields }	Object
_id	ObjectId("5f805cbb873173399a278d7b")	ObjectId
num	4	Int32
name	d	String
▼ (5) ObjectId("5f805cc5873173399a278d7c")	{ 3 fields }	Object
_id	ObjectId("5f805cc5873173399a278d7c")	ObjectId
num	5	Int32
name	e	String
▼ (6) ObjectId("5f805cd0873173399a278d7d")	{ 3 fields }	Object
_id	ObjectId("5f805cd0873173399a278d7d")	ObjectId
num	6	Int32
name	f	String
▼ (7) ObjectId("5f805cdd873173399a278d7e")	{ 3 fields }	Object
_id	ObjectId("5f805cdd873173399a278d7e")	ObjectId
num	7	Int32
name	g	String

Per suddividere la raccolta in tre segmenti specifici che AWS DMS dovrà migrare in parallelo, puoi aggiungere le regole di mappatura delle tabelle all'attività di migrazione. Questo approccio è mostrato nel seguente esempio JSON.

```
{ // Task table mappings:
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "testdatabase",
        "table-name": "testtable"
      }
    },
  ],
}
```

```

    "rule-action": "include"
  }, // "selection" : "rule-type"
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "testdatabase",
      "table-name": "testtable"
    },
    "parallel-load": {
      "type": "ranges",
      "columns": [
        "_id",
        "num"
      ],
      "boundaries": [
        // First segment selects documents with _id less-than-or-equal-to
        5f805c97873173399a278d79
        // and num less-than-or-equal-to 2.
        [
          "5f805c97873173399a278d79",
          "2"
        ],
        // Second segment selects documents with _id > 5f805c97873173399a278d79 and
        // _id less-than-or-equal-to 5f805cc5873173399a278d7c and
        // num > 2 and num less-than-or-equal-to 5.
        [
          "5f805cc5873173399a278d7c",
          "5"
        ]
        // Third segment is implied and selects documents with _id >
        5f805cc5873173399a278d7c.
      ] // : "boundaries"
    } // : "parallel-load"
  } // "table-settings" : "rule-type"
] // : "rules"
} // :Task table mappings

```

Questa definizione di mappatura delle tabelle divide la raccolta di origine in tre segmenti ed esegue la migrazione in parallelo. Di seguito sono riportati i limiti della segmentazione.

```
Data with _id less-than-or-equal-to "5f805c97873173399a278d79" and num less-than-or-equal-to 2 (2 records)
Data with _id > "5f805c97873173399a278d79" and num > 2 and _id less-than-or-equal-to "5f805cc5873173399a278d7c" and num less-than-or-equal-to 5 (3 records)
Data with _id > "5f805cc5873173399a278d7c" and num > 5 (2 records)
```

Una volta completata l'attività di migrazione, è possibile verificare nei log delle attività che le tabelle siano state caricate in parallelo, come illustrato nell'esempio seguente. Puoi anche verificare la clausola `find` MongoDB utilizzata per scaricare ogni segmento dalla tabella di origine.

```
[TASK_MANAGER    ] I: Start loading segment #1 of 3 of table
'testdatabase'. 'testtable' (Id = 1) by subtask 1. Start load timestamp
0005B191D638FE86 (replicationtask_util.c:752)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is initialized.
(mongodb_unload.c:157)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is: { "_id" :
{ "$lte" : { "$oid" : "5f805c97873173399a278d79" } }, "num" : { "$lte" :
{ "$numberInt" : "2" } } } (mongodb_unload.c:328)

[SOURCE_UNLOAD   ] I: Unload finished for segment #1 of segmented table
'testdatabase'. 'testtable' (Id = 1). 2 rows sent.

[TASK_MANAGER    ] I: Start loading segment #1 of 3 of table
'testdatabase'. 'testtable' (Id = 1) by subtask 1. Start load timestamp
0005B191D638FE86 (replicationtask_util.c:752)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is initialized.
(mongodb_unload.c:157)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is: { "_id" : { "$lte" :
{ "$oid" : "5f805c97873173399a278d79" } }, "num" : { "$lte" : { "$numberInt" :
"2" } } } (mongodb_unload.c:328)

[SOURCE_UNLOAD   ] I: Unload finished for segment #1 of segmented table
'testdatabase'. 'testtable' (Id = 1). 2 rows sent.

[TARGET_LOAD     ] I: Load finished for segment #1 of segmented table
'testdatabase'. 'testtable' (Id = 1). 1 rows received. 0 rows skipped. Volume
transferred 480.
```

```
[TASK_MANAGER ] I: Load finished for segment #1 of table
'testdatabase'. 'testtable' (Id = 1) by subtask 1. 2 records transferred.
```

Attualmente, AWS DMS supporta i seguenti tipi di dati MongoDB come colonna delle chiavi del segmento:

- Doppio
- Stringa
- ObjectId
- Intero a 32 bit
- Intero a 64 bit

Migrazione di più database quando si utilizza MongoDB come origine per AWS DMS

AWS DMS 3.4.5 e versioni successive supportano la migrazione di più database in un'unica attività per tutte le versioni di MongoDB supportate. Se desideri migrare più database, procedi nel modo seguente:

1. Quando crei l'endpoint di origine MongoDB, esegui una delle seguenti operazioni:
 - Nella pagina Crea endpoint della console DMS, assicurati che il campo Nome del database sia vuoto nella sezione Configurazione dell'endpoint.
 - Utilizzando il comando `CreateEndpoint` della AWS CLI, assegna un valore di stringa vuoto al parametro `DatabaseName` in `MongoDBSettings`.
2. Per ogni database che desideri migrare da un'origine MongoDB, specifica il nome del database come nome dello schema nella mappatura della tabella per l'attività. Puoi farlo utilizzando l'input guidato nella console o direttamente in JSON. Per ulteriori informazioni sull'input guidato, consulta [Specificazione della selezione delle tabelle e delle regole di trasformazione dalla console](#). Per ulteriori informazioni sul JSON, consulta [Operazioni e regole di selezione](#).

Ad esempio, puoi specificare il codice JSON seguente per migrare tre database MongoDB.

Example Migrazione di tutte le tabelle in uno schema

Il codice JSON seguente esegue la migrazione di tutte le tabelle dai database `Customers`, `Orders` e `Suppliers` dell'endpoint di origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Customers",
        "table-name": "%"
      },
      "rule-action": "include",
      "filters": []
    },
    {
      "rule-type": "selection",
      "rule-id": "2",
      "rule-name": "2",
      "object-locator": {
        "schema-name": "Orders",
        "table-name": "%"
      },
      "rule-action": "include",
      "filters": []
    },
    {
      "rule-type": "selection",
      "rule-id": "3",
      "rule-name": "3",
      "object-locator": {
        "schema-name": "Inventory",
        "table-name": "%"
      },
      "rule-action": "include",
      "filters": []
    }
  ]
}
```

Limitazioni relative all'utilizzo di MongoDB come origine per AWS DMS

Di seguito sono elencate le limitazioni quando si usa MongoDB come origine per AWS DMS:

- In modalità tabella, i documenti di una raccolta devono essere coerenti nel tipo di dati utilizzato per il valore nello stesso campo. Ad esempio, se il documento di una raccolta include '`{ a: { b: value ... } }`', tutti i documenti della raccolta che fanno riferimento a *value* del campo *a.b* devono utilizzare lo stesso tipo di dati per *value*, ovunque appaia nella raccolta.
- Quando l'opzione `_id` è impostata come una colonna separata, la stringa ID non deve superare i 200 caratteri.
- L'ID oggetto e le chiavi del tipo di matrice vengono convertiti in colonne con prefisso `oid` e `array` in modalità tabella.

Internamente, viene fatto riferimento a queste colonne con i nomi con prefisso. Se utilizzi le regole di trasformazione in AWS DMS che fanno riferimento a queste colonne, è necessario specificare la colonna con prefisso. Ad esempio, devi specificare `$_oid__id` e non `$_id`, oppure `$_array__addresses` e non `$_addresses`.

- I nomi delle raccolte e delle chiavi non possono includere il simbolo del dollaro (\$).
- AWS DMS non supporta raccolte contenenti uno stesso campo con lettere maiuscole e minuscole diverse in modalità tabella con destinazione RDBMS. Ad esempio, AWS DMS non supporta la presenza di due raccolte denominate `Field1` e `field1`.
- La modalità tabella e la modalità documento presentano le limitazioni illustrate in precedenza.
- La migrazione in parallelo utilizzando la segmentazione automatica comporta le limitazioni descritte in precedenza.
- I filtri di origine non sono supportati per MongoDB.
- AWS DMS non supporta documenti in cui il livello di nidificazione è superiore a 97.
- AWS DMS non supporta le seguenti funzionalità di MongoDB versione 5.0:
 - Ripartizionamento live
 - Crittografia a livello di campo lato client
 - Migrazione della raccolta di serie temporali

Note

Una raccolta di serie temporali migrata nella fase di pieno carico viene convertita in una normale raccolta in Amazon DocumentDB perché DocumentDB non supporta le raccolte di serie temporali.

Impostazioni di configurazione degli endpoint quando si utilizza MongoDB come origine per AWS DMS

Quando configuri l'endpoint di origine MongoDB, puoi specificare più impostazioni di configurazione dell'endpoint utilizzando la console AWS DMS.

La tabella seguente descrive le impostazioni di configurazione disponibili quando si utilizzano i database MongoDB come origine AWS DMS.

Impostazione (attributo)	Valori validi	Valore predefinito e descrizione
Modalità di autenticazione	"none" "password"	Il valore "password" richiede un nome utente e una password. Quando si specifica "none", i parametri nome utente e password non vengono utilizzati.
Origine di autenticazione	Un nome di database MongoDB valido.	Il nome del database MongoDB che desideri utilizzare per convalidare le credenziali di autenticazione. Il valore predefinito è "admin".
Meccanismo di autenticazione	"default" "mongodb_cr" "scram_sha_1"	Il meccanismo di autenticazione. Il valore di "default" è "scram_sha_1". Questa impostazione non viene utilizzata quando authType è impostato su "no".
Modalità metadati	Documento e tabella	Scegli la modalità documento o la modalità tabella.
Numero di documenti da analizzare (docsToInvestigate)	Un numero intero positivo maggiore di 0.	Utilizza questa opzione in modalità tabella solo per specificare la definizione della tabella di destinazione.
_id come colonna separata	Segno di spunta nella casella	Casella di spunta facoltativa che crea una seconda colonna denominata _id che agisce come chiave primaria.

Impostazione (attributo)	Valori validi	Valore predefinito e descrizione
socketTimeoutMS	NUMBER Solo attributo aggiuntivo di connessione.	Questa impostazione è espressa in millisecondi e configura il timeout di connessione per i client MongoDB. Se il valore è minore o uguale a zero, viene utilizzato il client MongoDB predefinito.
UseUpdateLookUp	booleano true false	Se impostata su true, durante gli eventi di aggiornamento CDC, AWS DMS copia l'intero documento aggiornato nella destinazione. Se impostata su false, AWS DMS utilizza il comando di aggiornamento MongoDB per aggiornare solo i campi modificati nel documento sulla destinazione.
ReplicateShardCollections	booleano true false	<p>Se impostata su true, AWS DMS replica i dati nelle raccolte di partizione. AWS DMS utilizza questa impostazione solo se l'endpoint di destinazione è un cluster elastico DocumentDB.</p> <p>Quando questa impostazione è true, è importante tenere presenti le seguenti informazioni:</p> <ul style="list-style-type: none"> • È necessario impostare TargetTablePrepMode su nothing. • AWS DMS imposta automaticamente useUpdateLookUp su false.

Se scegli Documento come Modalità metadati, sono disponibili diverse opzioni.

Se l'endpoint di destinazione è DocumentDB, assicurati di eseguire la migrazione in modalità documento. Inoltre, modifica l'endpoint di origine e seleziona l'opzione `_id` come colonna separata. Questo è un prerequisito obbligatorio se il carico di lavoro MongoDB di origine include transazioni.

Tipi di dati di origine per MongoDB

La migrazione dei dati che utilizza MongoDB come origine per AWS DMS supporta la maggior parte dei tipi di dati di MongoDB. Nella tabella seguente puoi trovare i tipi di dati di origine MongoDB supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati su AWS DMS. Per ulteriori informazioni sui tipi di dati MongoDB, consulta la sezione relativa ai [tipi BSON](#) nella documentazione di MongoDB.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati MongoDB	Tipi di dati AWS DMS
Booleano	Bool
Binario	BLOB
Data	Data
Timestamp	Data
Int	INT4
Long	INT8
Doppio	REAL8
String (UTF-8)	CLOB
Array	CLOB
OID	Stringa
REGEX	CLOB
CODE	CLOB

Utilizzo di Amazon DocumentDB (con compatibilità con MongoDB) come fonte per AWS DMS

Per informazioni sulle versioni di Amazon DocumentDB (compatibile con MongoDB) supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Con Amazon DocumentDB utilizzato come origine, puoi migrare i dati da un cluster Amazon DocumentDB a un altro cluster Amazon DocumentDB. Puoi anche migrare i dati da un cluster Amazon DocumentDB a uno degli altri endpoint di destinazione supportati da AWS DMS.

Se non hai familiarità con Amazon DocumentDB, tieni presente i seguenti concetti importanti sui database Amazon DocumentDB:

- Un record in Amazon DocumentDB è un documento, ossia una struttura di dati costituita da coppie di campi e valori. Il valore di un campo può includere altri documenti, matrici e matrici di documenti. Un documento è approssimativamente equivalente a una riga di una tabella di database relazionali.
- Una raccolta in Amazon DocumentDB è un gruppo di documenti ed è approssimativamente equivalente alla tabella di un database relazionale.
- Un database in Amazon DocumentDB è un insieme di raccolte ed è più o meno equivalente allo schema di un database relazionale.

AWS DMS supporta due modalità di migrazione quando si utilizza Amazon DocumentDB come sorgente, modalità documento e modalità tabella. Specifica la modalità di migrazione quando crei l'endpoint di origine Amazon DocumentDB nella AWS DMS console, utilizzando l'opzione Metadata mode o l'attributo di connessione `extra.nestingLevel`. Di seguito è riportata la spiegazione di come la scelta della modalità di migrazione influenza il formato risultante dei dati di destinazione.

Modalità documento

Con la modalità documento, il documento JSON viene migrato così com'è. Ciò significa che i dati del documento vengono consolidati in uno dei due elementi. Quando utilizzi un database relazionale come destinazione, i dati sono costituiti da una singola colonna denominata `_doc` in una tabella di destinazione. Quando utilizzi un database non relazionale come destinazione, i dati sono costituiti da un singolo documento JSON. La modalità documento è quella predefinita, consigliata per la migrazione a una destinazione di Amazon DocumentDB.

Considera, ad esempio, i seguenti documenti in una raccolta Amazon DocumentDB denominata `myCollection`.

```
> db.myCollection.find()
{ "_id" : ObjectId("5a94815f40bd44d1b02bdfe0"), "a" : 1, "b" : 2, "c" : 3 }
{ "_id" : ObjectId("5a94815f40bd44d1b02bdfe1"), "a" : 4, "b" : 5, "c" : 6 }
```

Una volta completata la migrazione dei dati a una tabella di database relazionale utilizzando la modalità documento, i dati vengono strutturati come segue. I campi dei dati nel documento sono consolidati nella colonna `_doc`.

oid_id	_doc
5a94815f40bd44d1b02bdfe0	{ "a" : 1, "b" : 2, "c" : 3 }
5a94815f40bd44d1b02bdfe1	{ "a" : 4, "b" : 5, "c" : 6 }

Puoi impostare facoltativamente l'attributo aggiuntivo di connessione `extractDocID` su `true` per creare una seconda colonna denominata `"_id"` che agisca come chiave primaria. Se intendi utilizzare l'acquisizione dei dati di modifica (CDC), imposta questo parametro su `true` tranne quando utilizzi Amazon DocumentDB come destinazione.

Note

Se aggiungi una nuova raccolta al database di origine, AWS DMS crea una nuova tabella di destinazione per la raccolta e replica tutti i documenti.

Modalità tabella

In modalità tabella AWS DMS trasforma ogni campo di primo livello di un documento Amazon DocumentDB in una colonna nella tabella di destinazione. Se un campo è nidificato, AWS DMS appiattisce i valori nidificati in un'unica colonna. AWS DMS quindi aggiunge un campo chiave e i tipi di dati al set di colonne della tabella di destinazione.

Per ogni documento Amazon DocumentDB, AWS DMS aggiunge ogni chiave e tipo al set di colonne della tabella di destinazione. Ad esempio, utilizzando la modalità tabella, AWS DMS migra l'esempio precedente nella tabella seguente.

oid_id	a	b	c
--------	---	---	---

5a94815f4 0bd44d1b02bdf0	1	2	3
5a94815f4 0bd44d1b02bdf1	4	5	6

I valori nidificati sono appiattiti in una colonna contenente nomi di chiavi separati da punti. La colonna viene denominata usando la concatenazione dei nomi di campo appiattiti separati da punti. Ad esempio, AWS DMS migra un documento JSON con un campo di valori annidati, ad esempio in una colonna `{"a" : {"b" : {"c": 1}}}` denominata `a.b.c`.

Per creare le colonne di destinazione, AWS DMS analizza un numero specificato di documenti Amazon DocumentDB e crea un set di tutti i campi e i relativi tipi. AWS DMS utilizza quindi questo set per creare le colonne della tabella di destinazione. Se crei o modifichi l'endpoint di origine di Amazon DocumentDB utilizzando la console, è possibile specificare il numero di documenti per la scansione. Il valore predefinito è 1.000 documenti. Se si utilizza il AWS CLI, è possibile utilizzare l'attributo di connessione `extradocsToInvestigate`.

In modalità tabella, AWS DMS gestisce documenti e raccolte in questo modo:

- Quando aggiungi un documento in una raccolta esistente, il documento viene replicato. Se ci sono campi che non esistono nella destinazione, tali campi non vengono replicati.
- Quando aggiorni un documento, il documento aggiornato viene replicato. Se ci sono campi che non esistono nella destinazione, tali campi non vengono replicati.
- L'eliminazione di un documento è supportata integralmente.
- L'aggiunta di una nuova raccolta non ha come risultato una nuova tabella nella destinazione durante un'attività CDC.
- Nella fase Change Data Capture (CDC), AWS DMS non supporta la ridenominazione di una raccolta.

Argomenti

- [Impostazione delle autorizzazioni per utilizzare Amazon DocumentDB come origine](#)
- [Configurazione della CDC per un cluster Amazon DocumentDB](#)
- [Connessione ad Amazon DocumentDB tramite TLS](#)
- [Creazione di un endpoint di origine Amazon DocumentDB](#)

- [Segmentazione delle raccolte Amazon DocumentDB e migrazione in parallelo](#)
- [Migrazione di più database quando si utilizza Amazon DocumentDB come origine per AWS DMS](#)
- [Limitazioni nell'utilizzo di Amazon DocumentDB come fonte per AWS DMS](#)
- [Utilizzo delle impostazioni degli endpoint con Amazon DocumentDB come origine](#)
- [Tipi di dati di origine per Amazon DocumentDB](#)

Impostazione delle autorizzazioni per utilizzare Amazon DocumentDB come origine

Quando si utilizza il codice sorgente Amazon DocumentDB per una AWS DMS migrazione, è possibile creare un account utente con privilegi di root. In alternativa puoi creare un utente con le autorizzazioni solo per il database da migrare.

Il codice seguente crea un utente come account root.

```
use admin
db.createUser(
  {
    user: "root",
    pwd: "password",
    roles: [ { role: "root", db: "admin" } ]
  })
```

Per Amazon DocumentDB 3.6, il codice seguente crea un utente con privilegi minimi sul database da migrare.

```
use database_to_migrate
db.createUser(
  {
    user: "dms-user",
    pwd: "password",
    roles: [ { role: "read", db: "db_name" }, "read" ]
  })
```

Per Amazon DocumentDB 4.0 e versioni successive, AWS DMS utilizza un flusso di modifiche a livello di distribuzione. In questo caso, il codice seguente crea un utente con privilegi minimi.

```
db.createUser(
```

```
{
  user: "dms-user",
  pwd: "password",
  roles: [ { role: "readAnyDatabase", db: "admin" } ]
})
```

Configurazione della CDC per un cluster Amazon DocumentDB

Per utilizzare la replica continua o CDC con Amazon DocumentDB AWS DMS , è necessario l'accesso ai flussi di modifica del cluster Amazon DocumentDB. Per una descrizione della sequenza temporale degli eventi di aggiornamento nelle raccolte e nei database del cluster, consulta [Using change streams](#) nella Guida per gli sviluppatori di Amazon DocumentDB.

Effettua l'autenticazione al cluster Amazon DocumentDB utilizzando la shell (interprete di comandi) MongoDB. Quindi, esegui il comando seguente per abilitare i flussi di modifica.

```
db.adminCommand({modifyChangeStreams: 1,
  database: "DB_NAME",
  collection: "",
  enable: true});
```

Questo approccio consente l'uso del flusso di modifica per tutte le raccolte del database. Dopo aver abilitato i flussi di modifica, puoi creare un'attività di migrazione che migra i dati esistenti e allo stesso tempo replica le modifiche in corso. AWS DMS continua ad acquisire e applicare le modifiche anche dopo il caricamento di grandi quantità di dati. I database di origine e di destinazione vengono sincronizzati con tempi di inattività per la migrazione quasi nulli.

Note

AWS DMS utilizza il registro delle operazioni (oplog) per acquisire le modifiche durante la replica in corso. Se Amazon DocumentDB elimina i record dall'oplog prima di AWS DMS leggerli, le attività avranno esito negativo. Ti consigliamo di dimensionare l'oplog in modo da mantenere le modifiche per almeno 24 ore.

Connessione ad Amazon DocumentDB tramite TLS

Per impostazione predefinita, un nuovo cluster Amazon DocumentDB creato accetta solo connessioni protette con Transport Layer Security (TLS). Quando TLS è abilitato, ogni connessione ad Amazon DocumentDB richiede una chiave pubblica.

Puoi recuperare la chiave pubblica per Amazon DocumentDB scaricando il `rds-combined-ca-bundle.pem` file da AWS un bucket Amazon S3 ospitato. Per ulteriori informazioni sul download di questo file, consulta [Encrypting connections using TLS](#) nella Guida per gli sviluppatori di Amazon DocumentDB.

Dopo aver scaricato il `rds-combined-ca-bundle.pem` file, puoi importare la chiave pubblica in cui è contenuto. AWS DMS Di seguito viene descritto come fare.

Per importare la chiave pubblica utilizzando la AWS DMS console

1. Accedi a AWS Management Console e scegli AWS DMS.
2. Nel riquadro di navigazione, scegliere Certificates (Certificati).
3. Selezionare Import certificate (Importa certificato). Viene visualizzata la pagina Importa nuovo certificato CA.
4. Nella sezione Configurazione del certificato effettua una delle seguenti operazioni:
 - Per Identificatore del certificato immetti un nome univoco per il certificato, ad esempio `docdb-cert`.
 - Seleziona Scegli file, vai alla posizione in cui hai salvato il file `rds-combined-ca-bundle.pem` e selezionalo.
5. Scegliere Add new CA certificate (Aggiungi nuovo certificato emesso da una CA).

L'esempio AWS CLI seguente utilizza il AWS DMS `import-certificate` comando per importare il `rds-combined-ca-bundle.pem` file della chiave pubblica.

```
aws dms import-certificate \  
  --certificate-identifier docdb-cert \  
  --certificate-pem file:///./rds-combined-ca-bundle.pem
```


Creazione di un endpoint di origine Amazon DocumentDB

Puoi creare un endpoint di origine Amazon DocumentDB utilizzando la console o la AWS CLI. Usa la seguente procedura con la console.

Per configurare un endpoint di origine Amazon DocumentDB utilizzando la console AWS DMS

1. Accedi a AWS Management Console e scegli. AWS DMS
2. Nel riquadro di navigazione seleziona Endpoint e quindi scegli Crea endpoint.
3. Per Identificativo endpoint fornisci un nome che ti aiuti a identificarlo facilmente, ad esempio `docdb-source`.
4. Per Motore di origine scegli Amazon DocumentDB (compatibile con MongoDB).
5. Per Nome del server inserisci il nome del server in cui risiede l'endpoint del database Amazon DocumentDB. Ad esempio, puoi inserire il nome DNS pubblico della tua istanza Amazon EC2 `democluster.cluster-cjf6q8nxfefi.us-east-2.docdb.amazonaws.com`.
6. Per Porta immetti 27017.
7. Per SSL mode (modalità SSL), scegliere `verify-full`. Se la modalità SSL è disabilitata sul cluster Amazon DocumentDB, puoi ignorare questo passaggio.
8. Per Certificato CA scegli il certificato Amazon DocumentDB `rds-combined-ca-bundle.pem`. Per le istruzioni sull'aggiunta di questo certificato, consulta [Connessione ad Amazon DocumentDB tramite TLS](#).
9. In Nome del database immetti il nome del database da migrare.

Utilizza la seguente procedura con la CLI.

Per configurare un endpoint di origine Amazon DocumentDB utilizzando AWS CLI

- Esegui il AWS DMS `create-endpoint` comando seguente per configurare un endpoint sorgente Amazon DocumentDB, sostituendo i segnaposto con i tuoi valori.

```
aws dms create-endpoint \  
    --endpoint-identifier a_memorable_name \  
    --endpoint-type source \  
    --engine-name docdb \  
    --username value \  
    --password value \  
    --server-name servername_where_database_endpoint_resides \  
    --
```

```
--port 27017 \  
--database-name name_of_endpoint_database
```

Segmentazione delle raccolte Amazon DocumentDB e migrazione in parallelo

Per migliorare le prestazioni di un'attività di migrazione, gli endpoint di origine Amazon DocumentDB supportano due opzioni della funzionalità di caricamento parallelo completo nella mappatura delle tabelle. In altre parole, è possibile migrare una raccolta in parallelo utilizzando le opzioni di segmentazione automatica o segmentazione degli intervalli della mappatura delle tabelle per il caricamento parallelo completo nelle impostazioni JSON. Le opzioni di segmentazione automatica consentono di specificare i criteri per AWS DMS segmentare automaticamente la fonte per la migrazione in ogni thread. Le opzioni di segmentazione degli intervalli consentono di indicare AWS DMS l'intervallo specifico di ciascun segmento da migrare da DMS in ogni thread. Per ulteriori informazioni su queste impostazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Migrazione di un database Amazon DocumentDB in parallelo utilizzando intervalli di segmentazione automatica

Puoi migrare i tuoi documenti in parallelo specificando i criteri per partizionare (AWS DMS segmentare) automaticamente i dati per ogni thread, in particolare il numero di documenti da migrare per thread. Utilizzando questo approccio, AWS DMS tenta di ottimizzare i limiti dei segmenti per ottenere le massime prestazioni per ogni thread.

È possibile specificare i criteri di segmentazione utilizzando le opzioni delle impostazioni della tabella riportate di seguito nella mappatura delle tabelle:

Opzione delle impostazioni della tabella	Descrizione
"type"	(Obbligatoria) Impostato su "partitions-auto" per Amazon DocumentDB come origine.
"number-of-partitions"	(Facoltativa) Numero totale di partizioni (segmenti) utilizzate per la migrazione. Il valore predefinito è 16.
"collection-count-from-meta-data"	(Facoltativo) Se impostato su true, AWS DMS utilizza un numero di raccolte stimato per

Opzione delle impostazioni della tabella	Descrizione
	determinare il numero di partizioni. Se impostato su <code>false</code> , AWS DMS utilizza il conteggio effettivo delle raccolte. Il valore predefinito è <code>true</code> .
<code>"max-records-skip-per-page"</code>	(Facoltativo) Il numero di record da saltare contemporaneamente quando si determinano i limiti di ogni partizione. AWS DMS utilizza un approccio di salto impaginato per determinare il limite minimo per una partizione. Il valore predefinito è 10000. L'impostazione di un valore relativamente elevato può causare timeout del cursore e errori delle attività. L'impostazione di un valore relativamente basso comporta un numero maggiore di operazioni per pagina e un pieno carico più lento.
<code>"batch-size"</code>	(Facoltativa) Limita il numero di documenti restituiti in un batch. Ogni batch richiede un round trip al server. Se la dimensione del batch è zero (0), il cursore utilizza la dimensione massima del batch definita dal server. Il valore predefinito è 0.

L'esempio seguente mostra una mappatura delle tabelle per la segmentazione automatica.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "admin",
        "table-name": "departments"
      },
      "rule-action": "include",
    }
  ]
}
```

```
    "filters": []
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "admin",
      "table-name": "departments"
    },
    "parallel-load": {
      "type": "partitions-auto",
      "number-of-partitions": 5,
      "collection-count-from-metadata": "true",
      "max-records-skip-per-page": 1000000,
      "batch-size": 50000
    }
  }
]
}
```

La segmentazione automatica presenta le seguenti limitazioni. La migrazione di ogni segmento recupera separatamente il conteggio di raccolte e il valore `_id` minimo della raccolta. Quindi utilizza l'approccio per ignorare con impaginazione per calcolare il limite minimo del segmento. Pertanto, assicurati che il valore `_id` minimo di ogni raccolta rimanga costante fino al calcolo di tutti i limiti del segmento della raccolta. La modifica del valore `_id` minimo di una raccolta durante il calcolo dei limiti del segmento può causare la perdita di dati o errori di riga duplicata.

Migrazione di un database Amazon DocumentDB in parallelo utilizzando intervalli di segmenti specifici

L'esempio seguente mostra una raccolta Amazon DocumentDB con sette elementi e `_id` come chiave primaria.

Key	Value	Type
▼ (1) ObjectId("5f805c74873173399a278d78")	{ 3 fields }	Object
_id	ObjectId("5f805c74873173399a278d78")	ObjectId
num	1	Int32
name	a	String
▼ (2) ObjectId("5f805c97873173399a278d79")	{ 3 fields }	Object
_id	ObjectId("5f805c97873173399a278d79")	ObjectId
num	2	Int32
name	b	String
▼ (3) ObjectId("5f805cb0873173399a278d7a")	{ 3 fields }	Object
_id	ObjectId("5f805cb0873173399a278d7a")	ObjectId
num	3	Int32
name	c	String
▼ (4) ObjectId("5f805cbb873173399a278d7b")	{ 3 fields }	Object
_id	ObjectId("5f805cbb873173399a278d7b")	ObjectId
num	4	Int32
name	d	String
▼ (5) ObjectId("5f805cc5873173399a278d7c")	{ 3 fields }	Object
_id	ObjectId("5f805cc5873173399a278d7c")	ObjectId
num	5	Int32
name	e	String
▼ (6) ObjectId("5f805cd0873173399a278d7d")	{ 3 fields }	Object
_id	ObjectId("5f805cd0873173399a278d7d")	ObjectId
num	6	Int32
name	f	String
▼ (7) ObjectId("5f805cdd873173399a278d7e")	{ 3 fields }	Object
_id	ObjectId("5f805cdd873173399a278d7e")	ObjectId
num	7	Int32
name	g	String

Per dividere la raccolta in tre segmenti ed eseguire la migrazione in parallelo, puoi aggiungere all'attività di migrazione le regole di mappatura delle tabelle, come mostrato nel seguente esempio JSON.

```
{ // Task table mappings:
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "testdatabase",
        "table-name": "testtable"
      }
    },
  ],
}
```

```

    "rule-action": "include"
  }, // "selection" : "rule-type"
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "testdatabase",
      "table-name": "testtable"
    },
    "parallel-load": {
      "type": "ranges",
      "columns": [
        "_id",
        "num"
      ],
      "boundaries": [
        // First segment selects documents with _id less-than-or-equal-to
        5f805c97873173399a278d79
        // and num less-than-or-equal-to 2.
        [
          "5f805c97873173399a278d79",
          "2"
        ],
        // Second segment selects documents with _id > 5f805c97873173399a278d79 and
        // _id less-than-or-equal-to 5f805cc5873173399a278d7c and
        // num > 2 and num less-than-or-equal-to 5.
        [
          "5f805cc5873173399a278d7c",
          "5"
        ]
        // Third segment is implied and selects documents with _id >
        5f805cc5873173399a278d7c.
      ] // : "boundaries"
    } // : "parallel-load"
  } // "table-settings" : "rule-type"
] // : "rules"
} // :Task table mappings

```

Questa definizione di mappatura delle tabelle divide la raccolta di origine in tre segmenti ed esegue la migrazione in parallelo. Di seguito sono riportati i limiti della segmentazione.

```
Data with _id less-than-or-equal-to "5f805c97873173399a278d79" and num less-than-or-equal-to 2 (2 records)
Data with _id less-than-or-equal-to "5f805cc5873173399a278d7c" and num less-than-or-equal-to 5 and not in (_id less-than-or-equal-to "5f805c97873173399a278d79" and num less-than-or-equal-to 2) (3 records)
Data not in (_id less-than-or-equal-to "5f805cc5873173399a278d7c" and num less-than-or-equal-to 5) (2 records)
```

Una volta completata l'attività di migrazione, è possibile verificare nei log delle attività che le tabelle siano state caricate in parallelo, come illustrato nell'esempio seguente. È anche possibile verificare la clausola `find` Amazon DocumentDB utilizzata per scaricare ogni segmento dalla tabella di origine.

```
[TASK_MANAGER    ] I: Start loading segment #1 of 3 of table
'testdatabase'. 'testtable' (Id = 1) by subtask 1. Start load timestamp
0005B191D638FE86 (replicationtask_util.c:752)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is initialized.
(mongodb_unload.c:157)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is: { "_id" :
{ "$lte" : { "$oid" : "5f805c97873173399a278d79" } }, "num" : { "$lte" :
{ "$numberInt" : "2" } } } (mongodb_unload.c:328)

[SOURCE_UNLOAD   ] I: Unload finished for segment #1 of segmented table
'testdatabase'. 'testtable' (Id = 1). 2 rows sent.

[TASK_MANAGER    ] I: Start loading segment #1 of 3 of table
'testdatabase'. 'testtable' (Id = 1) by subtask 1. Start load timestamp
0005B191D638FE86 (replicationtask_util.c:752)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is initialized.
(mongodb_unload.c:157)

[SOURCE_UNLOAD   ] I: Range Segmentation filter for Segment #0 is: { "_id" : { "$lte" :
{ "$oid" : "5f805c97873173399a278d79" } }, "num" : { "$lte" : { "$numberInt" :
"2" } } } (mongodb_unload.c:328)

[SOURCE_UNLOAD   ] I: Unload finished for segment #1 of segmented table
'testdatabase'. 'testtable' (Id = 1). 2 rows sent.
```

```
[TARGET_LOAD      ] I: Load finished for segment #1 of segmented table  
'testdatabase'.'testtable' (Id = 1). 1 rows received. 0 rows skipped. Volume  
transferred 480.
```

```
[TASK_MANAGER     ] I: Load finished for segment #1 of table  
'testdatabase'.'testtable' (Id = 1) by subtask 1. 2 records transferred.
```

Attualmente, AWS DMS supporta i seguenti tipi di dati Amazon DocumentDB come colonna chiave del segmento:

- Doppio
- Stringa
- ObjectId
- Intero a 32 bit
- Intero a 64 bit

Migrazione di più database quando si utilizza Amazon DocumentDB come origine per AWS DMS

AWS DMS le versioni 3.4.5 e successive supportano la migrazione di più database in un'unica attività solo per Amazon DocumentDB versioni 4.0 e successive. Se desideri migrare più database, procedi come indicato di seguito:

1. Quando crei l'endpoint di origine di Amazon DocumentDB:
 - Nel modulo AWS DMS, lascia vuoto AWS Management Console il nome del database nella sezione Configurazione dell'endpoint nella pagina Crea endpoint.
 - Nella AWS Command Line Interface (AWS CLI), assegna un valore di stringa vuoto al DatabaseNameparametro in DocumentDBSettings specificato per l'azione. CreateEndpoint
2. Per ogni database che desideri migrare da questo endpoint di origine Amazon DocumentDB, specifica il nome di ciascun database come nome di schema della mappatura delle tabelle per l'attività utilizzando l'input guidato della console o direttamente in JSON. Per ulteriori informazioni sull'input guidato, consulta la descrizione in [Specifica della selezione delle tabelle e delle regole di trasformazione dalla console](#). Per ulteriori informazioni sul JSON, consulta [Operazioni e regole di selezione](#).

Ad esempio, puoi specificare il codice JSON seguente per migrare tre database Amazon DocumentDB.

Example Migrazione di tutte le tabelle in uno schema

Il codice JSON seguente esegue la migrazione di tutte le tabelle dai database Customers, Orders e Suppliers dell'endpoint di origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Customers",
        "table-name": "%"
      },
      "object-locator": {
        "schema-name": "Orders",
        "table-name": "%"
      },
      "object-locator": {
        "schema-name": "Inventory",
        "table-name": "%"
      },
      "rule-action": "include"
    }
  ]
}
```

Limitazioni nell'utilizzo di Amazon DocumentDB come fonte per AWS DMS

Di seguito sono riportate le limitazioni relative all'utilizzo di Amazon DocumentDB come fonte per: AWS DMS

- Quando l'opzione `_id` è impostata come una colonna separata, la stringa ID non deve superare i 200 caratteri.
- L'ID oggetto e le chiavi del tipo di matrice vengono convertiti in colonne con prefisso `oid` e `array` in modalità tabella.

Internamente, viene fatto riferimento a queste colonne con i nomi con prefisso. Se utilizzi regole di trasformazione AWS DMS che fanno riferimento a queste colonne, assicurati di specificare la colonna con prefisso. Ad esempio, devi specificare `$_oid__id` e non `$_id` oppure `$_array__addresses` e non `$_addresses`.

- I nomi delle raccolte e delle chiavi non possono includere il simbolo del dollaro (\$).
- La modalità tabella e la modalità documento presentano le limitazioni illustrate in precedenza.
- La migrazione in parallelo utilizzando la segmentazione automatica comporta le limitazioni descritte in precedenza.
- Un'origine Amazon DocumentDB (compatibile con MongoDB) non supporta l'utilizzo di un timestamp specifico come posizione iniziale per l'acquisizione dei dati di modifica (CDC). Un'attività di replica continua acquisisce le modifiche indipendentemente dal timestamp.
- Quando si utilizza DocumentDB (compatibile con MongoDB) come origine, DMS può gestire un massimo di 250 record al secondo.
- AWS DMS non supporta documenti in cui il livello di nidificazione è maggiore di 97.
- I filtri di origine non sono supportati per DocumentDB.
- AWS DMS non supporta la replica CDC (change data capture) per DocumentDB come origine in modalità cluster elastico.

Utilizzo delle impostazioni degli endpoint con Amazon DocumentDB come origine

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine Amazon DocumentDB in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in [AWS CLI](#), con la sintassi JSON. `--doc-db-settings '{"EndpointSetting": "value", ...}'`

La tabella seguente mostra le impostazioni degli endpoint che puoi utilizzare con Amazon DocumentDB come origine.

Nome attributo	Valori validi	Valore predefinito e descrizione
NestingLevel	"none" "one"	"none": specifica "none" per utilizzare la modalità documento. Specificare "one" per utilizzare la modalità tabella.
ExtractDocID	booleano true false	false: utilizza questo attributo quando NestingLevel è impostato su "none". Se il database di destinazione è Amazon DocumentDB, imposta '{"ExtractDocID": true}' .
DocsToInvestigate	Un numero intero positivo maggiore di 0.	1000: utilizza questo attributo quando NestingLevel è impostato su "one".
ReplicateShardCollections	booleano true false	Se impostato su true, AWS DMS replica i dati in raccolte di frammenti. AWS DMS utilizza questa impostazione solo se l'endpoint di destinazione è un cluster elastico DocumentDB. Quando questa impostazione è true, è importante tenere presenti le seguenti informazioni: <ul style="list-style-type: none"> • È necessario impostare TargetTablePrepMode su nothing. • AWS DMS imposta useUpdateLookup automaticamente su. false

Tipi di dati di origine per Amazon DocumentDB

Nella tabella seguente sono elencati i tipi di dati di origine di Amazon DocumentDB supportati per l'uso in AWS DMS. In questa tabella puoi anche trovare la mappatura predefinita AWS DMS dei tipi di dati. Per ulteriori informazioni sui tipi di dati, consulta [BSON types](#) nella documentazione di MongoDB.

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati Amazon DocumentDB	AWS DMS tipi di dati
Booleano	Bool
Binario	BLOB
Data	Data
Timestamp	Data
Int	INT4
Long	INT8
Doppio	REAL8
String (UTF-8)	CLOB
Array	CLOB
OID	Stringa

Utilizzo di Amazon S3 come sorgente per AWS DMS

Puoi migrare i dati da un bucket Amazon S3 utilizzando AWS DMS. Per eseguire questa operazione dovrai fornire l'accesso a un bucket Amazon S3 contenente uno o più file di dati. In questo bucket S3, includi un file JSON che descriva la mappatura tra i dati e le tabelle di database dei dati in questi file.

I file di dati di origine devono essere presenti nel bucket Amazon S3 prima dell'avvio del pieno carico. Specifica il nome del bucket tramite il parametro `bucketName`.

I file di dati di origine possono avere i seguenti formati:

- Valore separato da virgole (.csv)

- Parquet (versione DMS 3.5.3 e successive). Per informazioni sull'uso dei file in formato Parquet, consulta [Utilizzo di file in formato Parquet in Amazon S3 come origine per AWS DMS](#)

Per i file di dati di origine in formato con valori separati da virgole (.csv), denominateli utilizzando la seguente convenzione di denominazione. In questa convenzione, *schemaName* è lo schema di origine e *tableName* è il nome di una tabella all'interno di tale schema.

```
/schemaName/tableName/LOAD001.csv  
/schemaName/tableName/LOAD002.csv  
/schemaName/tableName/LOAD003.csv  
...
```

Ad esempio, supponi che i file di dati siano in mybucket nel seguente percorso Amazon S3.

```
s3://mybucket/hr/employee
```

In fase di caricamento, AWS DMS si presuppone che il nome dello schema di origine sia e che il nome della tabella di origine sia hr. employee

Oltre a bucketName (obbligatorio), puoi facoltativamente fornire un bucketFolder parametro per AWS DMS specificare dove cercare i file di dati nel bucket Amazon S3. Continuando l'esempio precedente, se lo hai bucketFolder impostato susourcedata, AWS DMS legge i file di dati nel percorso seguente.

```
s3://mybucket/sourcedata/hr/employee
```

Puoi specificare il delimitatore di colonna, di riga, l'indicatore di valori null e altri parametri utilizzando gli attributi di connessione aggiuntivi. Per ulteriori informazioni, consulta [Impostazioni degli endpoint per Amazon S3 come origine per AWS DMS](#).

Puoi specificare il proprietario del bucket e impedire lo sniping utilizzando l'impostazione dell'endpoint ExpectedBucketOwner Amazon S3, come illustrato di seguito. Quindi, quando effettui una richiesta per testare una connessione o eseguire una migrazione, S3 controlla l'ID account del proprietario del bucket rispetto al parametro specificato.

```
--s3-settings='{"ExpectedBucketOwner": "AWS_Account_ID"}
```

Argomenti

- [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#)
- [Utilizzo della CDC con Amazon S3 come origine per AWS DMS](#)
- [Prerequisiti per l'utilizzo di Amazon S3 come sorgente per AWS DMS](#)
- [Limitazioni nell'utilizzo di Amazon S3 come fonte per AWS DMS](#)
- [Impostazioni degli endpoint per Amazon S3 come origine per AWS DMS](#)
- [Tipi di dati di origine per Amazon S3](#)
- [Utilizzo di file in formato Parquet in Amazon S3 come origine per AWS DMS](#)

Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS

Oltre ai file di dati, devi fornire anche una definizione di tabella esterna. Una definizione di tabella esterna è un documento JSON che descrive come AWS DMS interpretare i dati di Amazon S3. La dimensione massima di questo documento è 2 MB. Se crei un endpoint di origine utilizzando la console di AWS DMS gestione, puoi inserire il codice JSON direttamente nella casella di mappatura delle tabelle. Se utilizzi AWS Command Line Interface (AWS CLI) o l' AWS DMS API per eseguire le migrazioni, puoi creare un file JSON per specificare la definizione della tabella esterna.

Ad esempio, supponi di avere un file di dati che include quanto segue.

```
101,Smith,Bob,2014-06-04,New York
102,Smith,Bob,2015-10-08,Los Angeles
103,Smith,Bob,2017-03-13,Dallas
104,Smith,Bob,2017-03-13,Dallas
```

Di seguito è riportato un esempio di definizione di tabella esterna per questi dati.

```
{
  "TableCount": "1",
  "Tables": [
    {
      "TableName": "employee",
      "TablePath": "hr/employee/",
      "TableOwner": "hr",
      "TableColumns": [
        {
          "ColumnName": "Id",
          "ColumnType": "INT8",
          "ColumnNullable": "false",
          "ColumnIsPk": "true"
        }
      ]
    }
  ]
}
```

```
    },
    {
      "ColumnName": "LastName",
      "ColumnType": "STRING",
      "ColumnLength": "20"
    },
    {
      "ColumnName": "FirstName",
      "ColumnType": "STRING",
      "ColumnLength": "30"
    },
    {
      "ColumnName": "HireDate",
      "ColumnType": "DATETIME"
    },
    {
      "ColumnName": "OfficeLocation",
      "ColumnType": "STRING",
      "ColumnLength": "20"
    }
  ],
  "TableColumnsTotal": "5"
}
]
```

Gli elementi in questo documento JSON sono i seguenti:

TableCount: il numero di tabelle di origine. In questo esempio è presente una sola tabella.

Tables: un array costituito da una mappa JSON per tabella di origine. In questo esempio è presente una sola mappa. Ogni mappa è formata dai seguenti elementi:

- **TableName**: il nome della tabella di origine.
- **TablePath**: il percorso nel bucket Amazon S3 in cui AWS DMS può trovare il file completo del caricamento dei dati. Se è specificato un valore `bucketFolder`, questo valore viene anteposto al percorso.
- **TableOwner**: il nome dello schema per la tabella.
- **TableColumns**: un array di una o più mappe, ognuna delle quali descrive una colonna nella tabella di origine:
 - **ColumnName**: il nome di una colonna nella tabella di origine.

- **ColumnType**: il tipo di dati della colonna. Per informazioni sui tipi di dati validi, consulta [Tipi di dati di origine per Amazon S3](#).
- **ColumnLength**: il numero di byte della colonna. La lunghezza massima delle colonne è limitata a 2147483647 byte (2.047 MegaBytes) poiché una sorgente S3 non supporta la modalità FULL LOB. **ColumnLength** è valido per i seguenti tipi di dati:
 - BYTE
 - STRING
- **ColumnNullable**: un valore booleano che è `true` se questa colonna può contenere valori NULL (predefinito = `false`).
- **ColumnIsPk**: un valore booleano che è `true` se questa colonna è parte della chiave primaria (predefinito = `false`).
- **ColumnDateFormat**: il formato della data di input per una colonna con i tipi DATE, TIME e DATETIME e utilizzato per analizzare una stringa di dati in un oggetto data. I valori possibili includono:

```
- YYYY-MM-dd HH:mm:ss
- YYYY-MM-dd HH:mm:ss.F
- YYYY/MM/dd HH:mm:ss
- YYYY/MM/dd HH:mm:ss.F
- MM/dd/YYYY HH:mm:ss
- MM/dd/YYYY HH:mm:ss.F
- YYYYMMdd HH:mm:ss
- YYYYMMdd HH:mm:ss.F
```

- **TableColumnsTotal**: il numero totale di colonne. Questo numero deve corrispondere al numero di elementi nella matrice **TableColumns**.

Se non si specifica diversamente, AWS DMS si presuppone che **ColumnLength** sia zero.

Note

Nelle versioni supportate di AWS DMS, i dati di origine S3 possono contenere anche una colonna operativa opzionale come prima colonna prima del valore della **TableName** colonna. Questa colonna operazione identifica l'operazione (INSERT) utilizzata per migrare i dati a un endpoint di destinazione S3 durante un carico completo.

Se presente, il valore di questa colonna è il carattere iniziale della parola chiave (I) dell'operazione INSERT. Se specificato, questa colonna generalmente indica che la sorgente di S3 è stata creata da DMS come target S3 durante una migrazione precedente. Nelle versioni di DMS precedenti alla 3.4.2, questa colonna non era presente nei dati di origine S3 creati da un precedente pieno carico DMS. Aggiungere questa colonna ai dati target S3 consente al formato di tutte le righe scritte nel target S3 di essere coerenti se sono scritte durante un pieno carico o durante un carico CDC. Per ulteriori informazioni sulle opzioni per la formattazione dei dati target S3, vedere [Indicazione delle operazioni del DB di origine nei dati S3 migrati](#).

Per una colonna di tipo NUMERIC, devi specificare la precisione e la dimensione. La precisione è il numero totale di cifre in un numero e la dimensione è il numero di cifre a destra del separatore decimale. Puoi utilizzare gli elementi `ColumnScale` e `ColumnPrecision` come illustrato di seguito.

```
...
{
  "ColumnName": "HourlyRate",
  "ColumnType": "NUMERIC",
  "ColumnPrecision": "5"
  "ColumnScale": "2"
}
...
```

Per una colonna di tipo DATETIME con dati che contengono frazioni di secondo, specifica la scala. La scala è il numero di cifre per le frazioni di secondo e può variare da 0 a 9. Puoi utilizzare l'elemento `ColumnScale` per questo scopo, come illustrato di seguito.

```
...
{
  "ColumnName": "HireDate",
  "ColumnType": "DATETIME",
  "ColumnScale": "3"
}
...
```

Se non specifichi diversamente, AWS DMS assume che `ColumnScale` sia zero e tronca la frazione di secondo.

Utilizzo della CDC con Amazon S3 come origine per AWS DMS

Dopo aver AWS DMS eseguito un caricamento completo dei dati, può opzionalmente replicare le modifiche ai dati sull'endpoint di destinazione. A tale scopo, carichi i file di acquisizione dei dati di modifica (file CDC) nel tuo bucket Amazon S3. AWS DMS legge questi file CDC quando li carichi e quindi applica le modifiche all'endpoint di destinazione.

I file CDC sono denominati come segue:

```
CDC00001.csv  
CDC00002.csv  
CDC00003.csv  
...
```

Note

Per replicare i file CDC nella cartella dei dati di modifica caricarli correttamente in un ordine lessicale (sequenziale). Ad esempio, caricare il file CDC00002.csv prima del file CDC00003.csv. In caso contrario, CDC00002.csv viene ignorato e non viene replicato se lo si carica dopo CDC00003.csv. Ma il file CDC00004.csv viene replicato correttamente se caricato dopo CDC00003.csv.

Per indicare dove è AWS DMS possibile trovare i file, specificare il parametro. `cdcPath` Continuando con l'esempio precedente, se imposti `cdcPath` su *changedata*, AWS DMS legge i file CDC dal seguente percorso.

```
s3://mybucket/changedata
```

Se imposti su `cdcPath` su *changedata* e `bucketFolder` su *myFolder*, AWS DMS legge i file CDC nel seguente percorso.

```
s3://mybucket/myFolder/changedata
```

I record in un file CDC sono formattati come segue:

- Operazione: l'operazione di modifica da eseguire: INSERT o I, UPDATE o U, oppure DELETE o D. Queste parole chiave e i valori dei caratteri non fanno distinzione tra maiuscole e minuscole.

Note

Nelle AWS DMS versioni supportate, AWS DMS può identificare l'operazione da eseguire per ogni record di caricamento in due modi. AWS DMS può eseguire questa operazione dal valore della parola chiave del record (ad esempio, INSERT) o dal carattere iniziale della parola chiave (ad esempio, I). Nelle versioni precedenti, AWS DMS riconosceva l'operazione di caricamento solo dal valore completo della parola chiave.

Nelle versioni precedenti di AWS DMS, il valore completo della parola chiave veniva scritto per registrare i dati CDC. Inoltre, le versioni precedenti scrivevano il valore dell'operazione su qualsiasi destinazione S3 utilizzando solo la parola chiave iniziale.

Il riconoscimento di entrambi i formati consente di AWS DMS gestire l'operazione indipendentemente dal modo in cui viene scritta la colonna delle operazioni per creare i dati di origine S3. Questo approccio supporta l'utilizzo di dati di destinazione su S3 come sorgente per una successiva migrazione. Grazie a questo approccio, non è necessario modificare il formato di qualsiasi valore iniziale della parola chiave visualizzato nella colonna dell'operazione della successiva sorgente S3.

- Nome tabella: il nome della tabella di origine.
- Nome dello schema: il nome dello schema di origine.
- Dati: una o più colonne che rappresentano i dati da modificare.

Di seguito è riportato un esempio di un file CDC per una tabella denominata employee.

```
INSERT,employee,hr,101,Smith,Bob,2014-06-04,New York
UPDATE,employee,hr,101,Smith,Bob,2015-10-08,Los Angeles
UPDATE,employee,hr,101,Smith,Bob,2017-03-13,Dallas
DELETE,employee,hr,101,Smith,Bob,2017-03-13,Dallas
```

Prerequisiti per l'utilizzo di Amazon S3 come sorgente per AWS DMS

Per utilizzare Amazon S3 come origine per AWS DMS, il bucket S3 di origine deve trovarsi nella stessa AWS regione dell'istanza di replica DMS che migra i dati. Inoltre, l'account AWS che utilizzi per la migrazione deve disporre dell'accesso in lettura al bucket di origine.

Il ruolo AWS Identity and Access Management (IAM) assegnato all'account utente utilizzato per creare l'attività di migrazione deve avere il seguente set di autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket*/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket*"
      ]
    }
  ]
}
```

Il ruolo AWS Identity and Access Management (IAM) assegnato all'account utente utilizzato per creare l'attività di migrazione deve disporre del seguente set di autorizzazioni se il controllo delle versioni è abilitato nel bucket Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "S3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket*/*"
      ]
    },
    {
```

```

        "Effect": "Allow",
        "Action": [
            "s3:ListBucket"
        ],
        "Resource": [
            "arn:aws:s3:::mybucket*"
        ]
    }
]
}

```

Limitazioni nell'utilizzo di Amazon S3 come fonte per AWS DMS

Le seguenti limitazioni si applicano quando si utilizza Amazon S3 come origine:

- Non abilitare il controllo delle versioni per S3. Se hai bisogno del controllo delle versioni S3, utilizza le policy del ciclo di vita per eliminare attivamente le vecchie versioni. In caso contrario, è possibile che si verifichino errori della connessione di test dell'endpoint a causa del timeout della chiamata `list-object` S3. Per creare una policy del ciclo di vita per un bucket S3, consulta [Gestione del ciclo di vita dello storage](#). Per eliminare la versione di un oggetto S3, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).
- Un bucket S3 abilitato per VPC (VPC del gateway) è supportato nelle versioni 3.4.7 e successive.
- MySQL converte `time` il tipo di dati in `string`. Per visualizzare **time** i valori dei tipi di dati in MySQL, definisci la colonna nella tabella di destinazione **string** come e imposta l'impostazione della modalità di preparazione della tabella Target dell'attività su `Truncate`.
- AWS DMS utilizza il tipo di `BYTE` dati internamente per i dati di entrambi i tipi di dati. `BYTE` `BYTES`
- Gli endpoint di origine S3 non supportano la funzionalità di ricarica delle tabelle DMS.
- AWS DMS non supporta la modalità Full LOB con Amazon S3 come sorgente.

Le seguenti limitazioni si applicano all'utilizzo di file in formato Parquet in Amazon S3 come origine:

- Le date incluse o non `DDMMYYYY` sono supportate per la funzionalità di partizionamento della data di S3 Parquet Source. `MMYYYYDD`

Impostazioni degli endpoint per Amazon S3 come origine per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine Amazon S3 in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni

vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando contenuto in [AWS CLI](#), con la `--s3-settings` `'{"EndpointSetting": "value", ...}'` sintassi JSON.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Amazon S3 come origine.

Opzione	Descrizione
BucketFolder	<p>(Facoltativo) Un nome di cartella nel bucket S3. Se questo attributo è fornito, i file di dati di origine e i file CDC vengono letti dal percorso <code>s3://myBucket/bucketFolder /schemaName /tableName /</code> e <code>s3://myBucket/bucketFolder /</code> rispettivamente. Se questo attributo non è specificato, viene utilizzato il percorso <code>schemaName /tableName /</code>.</p> <pre>'{"BucketFolder": " sourceData "'</pre>
BucketName	<p>Nome del bucket S3.</p> <pre>'{"BucketName": " myBucket "'</pre>
CdcPath	<p>La posizione dei file CDC. Questo attributo è necessario se un'attività acquisisce i dati modificati; altrimenti, è facoltativo. Se <code>CdcPath</code> è presente, AWS DMS legge i file CDC da questo percorso e replica le modifiche ai dati sull'endpoint di destinazione. Per ulteriori informazioni, consulta Utilizzo della CDC con Amazon S3 come origine per AWS DMS.</p> <pre>'{"CdcPath": " changeData "'</pre>
CsvDelimiter	<p>Delimitatore utilizzato per separare le colonne nei file di origine. L'impostazione predefinita è una virgola. Di seguito è riportato un esempio.</p> <pre>'{"CsvDelimiter": ", "'</pre>
CsvNullValue	<p>Una stringa definita dall'utente che viene considerata nulla AWS DMS durante la lettura dall'origine. L'impostazione predefinita è una stringa vuota. Se non impostate questo parametro, AWS DMS considera una stringa vuota come un valore nullo. Se impostate questo parametro su</p>

Opzione	Descrizione
	una stringa come «\ N», AWS DMS tratta questa stringa come valore nullo e tratta le stringhe vuote come valore di stringa vuota.
CsvRowDelimiter	<p>Delimitatore utilizzato per separare le righe nei file di origine. L'impostazione predefinita è una nuova riga (\n).</p> <pre>'{"CsvRowDelimiter": "\n"}'</pre>
DataFormat	<p>Imposta questo valore su per leggere i dati Parquet in formato Parquet.</p> <pre>'{"DataFormat": "Parquet"}'</pre>
IgnoreHeaderRows	<p>Quando questo valore è impostato su 1, AWS DMS ignora l'intestazione della prima riga in un file.csv. Il valore 1 abilita la funzionalità, il valore 0 la disabilita.</p> <p>Il valore predefinito è 0.</p> <pre>'{"IgnoreHeaderRows": 1}'</pre>
Rfc4180	<p>Quando questo valore è impostato su true o y, le virgolette di apertura devono essere seguite dalle virgolette di chiusura. Questa formattazione è conforme a RFC 4180. Quando questo valore è impostato su false o n, i valori letterali stringa vengono copiati sulla destinazione così come sono. In questo caso, un delimitatore (riga o colonna) segnala la fine del campo. Pertanto, non è possibile utilizzare un delimitatore come parte della stringa, perché segnala la fine del valore.</p> <p>Il valore predefinito è true.</p> <p>Valori validi: true, false, y, n</p> <pre>'{"Rfc4180": false}'</pre>

Tipi di dati di origine per Amazon S3

Migrazione dei dati che utilizza Amazon S3 come fonte per AWS DMS le esigenze di mappatura dei dati da Amazon S3 AWS DMS ai tipi di dati. Per ulteriori informazioni, consulta [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#).

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, consulta. [Tipi di dati per AWS Database Migration Service](#)

I seguenti tipi di AWS DMS dati vengono utilizzati con Amazon S3 come fonte:

- BYTE: richiede ColumnLength. Per ulteriori informazioni, consulta [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#).
- DATE
- TIME
- DATETIME: per ulteriori informazioni e un esempio, consulta il tipo DATETIME in [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#).
- INT1
- INT2
- INT4
- INT8
- NUMERIC: richiede ColumnPrecision e ColumnScale AWS DMS supporta i seguenti valori massimi:
 - ColumnPrecision: 38
 - ColumnScale: 31

Per ulteriori informazioni e un esempio, consulta il tipo NUMERIC in [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#).

- REAL4
- REAL8
- STRING: richiede ColumnLength. Per ulteriori informazioni, consulta [Definizione di tabelle esterne per Amazon S3 come origine per AWS DMS](#).

- UINT1
- UINT2
- UINT4
- UINT8
- BLOB
- CLOB
- BOOLEAN

Utilizzo di file in formato Parquet in Amazon S3 come origine per AWS DMS

Nella AWS DMS versione 3.5.3 e successive, è possibile utilizzare i file in formato Parquet in un bucket S3 come origine per la replica Full-Load o CDC.

DMS supporta solo i file in formato Parquet come origine generata da DMS migrando i dati su un endpoint di destinazione S3. I nomi dei file devono essere nel formato supportato, altrimenti DMS non li includerà nella migrazione.

Per i file di dati di origine in formato Parquet, devono trovarsi nella seguente cartella e convenzione di denominazione.

```
schema/table1/LOAD00001.parquet  
schema/table2/LOAD00002.parquet  
schema/table2/LOAD00003.parquet
```

Per i file di dati di origine per i dati CDC in formato Parquet, denominateli e memorizzateli utilizzando la seguente convenzione di cartella e denominazione.

```
schema/table/20230405-094615814.parquet  
schema/table/20230405-094615853.parquet  
schema/table/20230405-094615922.parquet
```

Per accedere ai file in formato Parquet, impostate le seguenti impostazioni dell'endpoint:

- Imposta `DataFormat` su `Parquet`.
- Non impostate l'`cdcPath` impostazione. Assicuratevi di creare i file in formato Parquet nelle cartelle `schema/tabella` specificate.

[Per ulteriori informazioni sulle impostazioni per gli endpoint S3, consulta S3Settings nell'API Reference.AWS Database Migration Service](#)

Tipi di dati supportati per i file in formato Parquet

AWS DMS supporta i seguenti tipi di dati di origine e destinazione durante la migrazione di dati da file in formato Parquet. Assicurati che la tabella di destinazione contenga colonne con i tipi di dati corretti prima della migrazione.

Tipo di dati origine	Tipo di dati di destinazione
BYTE	BINARY
DATE	DATE32
TIME	TIME32
DATETIME	TIMESTAMP
INT1	INT8
INT2	INT16
INT4	INT32
INT8	INT64
NUMERIC	DECIMAL
REAL4	FLOAT
REAL8	DOUBLE
STRING	STRING
UINT1	UINT8
UINT2	UINT16
UINT4	UINT32
UINT8	UINT

Tipo di dati origine	Tipo di dati di destinazione
WSTRING	STRING
BLOB	BINARY
NCLOB	STRING
CLOB	STRING
BOOLEAN	BOOL

Utilizzo di IBM Db2 per Linux, Unix, Windows e database Amazon RDS (Db2 LUW) come origine per AWS DMS

Puoi migrare i dati da un database IBM Db2 per Linux, Unix, Windows e Amazon RDS (Db2 LUW) a qualsiasi database di destinazione supportato utilizzando (). AWS Database Migration Service AWS DMS

Per informazioni sulle versioni di Db2 su Linux, Unix, Windows e RDS supportate come sorgente, consulta. AWS DMS [Fonti per AWS DMS](#)

Puoi utilizzare il protocollo Secure Sockets Layer (SSL) per crittografare le connessioni tra l'endpoint Db2 LUW e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint Db2 LUW, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Prerequisiti per l'utilizzo di Db2 LUW come sorgente per AWS DMS

I seguenti prerequisiti sono necessari prima di poter utilizzare un database Db2 LUW come origine.

Per abilitare la replica continua, denominata anche CDC (Change Data Capture), eseguire le seguenti operazioni:

- Imposta il database in modo che sia recuperabile, il che AWS DMS richiede l'acquisizione delle modifiche. Un database è recuperabile se uno o entrambi i parametri di configurazione del database LOGARCHMETH1 e LOGARCHMETH2 sono impostati su ON.

Se il database è recuperabile, AWS DMS può accedere a Db2 se necessario. ARCHIVE LOG

- Assicurati che i log delle transazioni DB2 siano disponibili, con un periodo di conservazione sufficiente entro il quale elaborarli. AWS DMS
- DB2 richiede l'autorizzazione SYSADM o DBADM per estrarre i record del log delle transazioni. Concedi all'account utente le autorizzazioni seguenti:
 - SYSADM o DBADM
 - DATAACCESS

Note

Per le attività solo pieno carico, l'account utente DMS necessita dell'autorizzazione DATAACCESS.

- Quando utilizzi IBM DB2 for LUW versione 9.7 come origine, imposta l'attributo aggiuntivo di connessione `CurrentLSN` come segue:

`CurrentLSN=LSN` dove `LSN` specifica un numero di sequenza del log (LSN) in cui desideri avviare la replica. In alternativa, imposta `CurrentLSN=scan`.

Limitazioni nell'utilizzo di Db2 LUW come fonte per AWS DMS

AWS DMS non supporta database in cluster. Tuttavia, è possibile definire un Db2 LUW separato per ciascun endpoint di un cluster. Ad esempio, è possibile creare un'attività di migrazione pieno carico con uno qualsiasi dei nodi del cluster, quindi creare attività separate per ogni nodo.

AWS DMS non supporta il tipo di B00LEAN dati nel database Db2 LUW di origine.

Quando si utilizza la replica continua (CDC), si applicano le seguenti limitazioni:

- Quando una tabella con più partizioni viene troncata, il numero di eventi DDL visualizzati nella AWS DMS console è uguale al numero di partizioni. Questo perché Db2 LUW registra una DDL separata per ciascuna partizione.
- Le seguenti operazioni DDL non sono supportate sulle tabelle partizionate:
 - ALTER TABLE ADD PARTITION
 - ALTER TABLE DETACH PARTITION
 - ALTER TABLE ATTACH PARTITION
- AWS DMS non supporta una migrazione di replica continua da un'istanza di standby di DB2 High Availability Disaster Recovery (HADR). L'istanza di standby è inaccessibile.

- Il tipo di dati DECFLOAT non è supportato. Di conseguenza, le modifiche alle colonne DECFLOAT vengono ignorate durante la replica continua.
- L'istruzione RENAME COLUMN non è supportata.
- Quando si eseguono aggiornamenti alle tabelle Multi-Dimensional Clustering (MDC), ogni aggiornamento viene visualizzato nella console come INSERT + DELETE. AWS DMS
- Quando l'impostazione dell'attività Include LOB columns in replication (Includi le colonne LOB nella replica) non è disabilitata, qualsiasi tabella con colonne LOB viene sospesa durante la replica continua.
- Per le versioni Db2 LUW 10.5 e successive, le colonne di stringhe a lunghezza variabile con dati archiviati vengono ignorate. out-of-row Questa limitazione si applica solo alle tabelle create con dimensioni di riga estese per colonne con tipi di dati come VARCHAR e VARGRAPHIC. Per ovviare a questa limitazione, sposta la tabella in uno spazio con una dimensione di pagina maggiore. Per ulteriori informazioni, consulta [What can I do if I want to change the pagesize of DB2 tablespaces](#).
- Per la replica continua, DMS non supporta la migrazione dei dati caricati a livello di pagina dall'utilità DB2 LOAD. Utilizza invece l'utilità IMPORT che usa inserimenti SQL. Per ulteriori informazioni, consulta [Differences between the import and load utility](#).
- Durante l'esecuzione di un'attività di replica, DMS acquisisce le DDL CREATE TABLE solo se le tabelle sono state create con l'attributo DATA CAPTURE CHANGE.
- DMS presenta le seguenti limitazioni quando si utilizza la Db2 Database Partition Feature (DPF):
 - DMS non è in grado di coordinare le transazioni tra i nodi Db2 in un ambiente DPF. Ciò è dovuto ai vincoli all'interno dell'interfaccia API IBM DB2READLOG. In DPF, le transazioni possono estendersi su più nodi Db2, a seconda di come DB2 partiziona i dati. Di conseguenza, la soluzione DMS deve acquisire le transazioni da ciascun nodo Db2 in modo indipendente.
 - DMS può acquisire transazioni locali da ogni nodo Db2 nel cluster DPF connectNode impostando 1 su più endpoint di origine DMS. Questa configurazione corrisponde ai numeri di nodi logici definiti nel file di configurazione del server DB2. db2nodes . c f g
 - Le transazioni locali su singoli nodi Db2 possono far parte di una transazione globale più ampia. DMS applica ogni transazione locale in modo indipendente sulla destinazione, senza coordinamento con le transazioni su altri nodi Db2. Questa elaborazione indipendente può portare a complicazioni, specialmente quando le righe vengono spostate tra le partizioni.
 - Quando DMS esegue la replica da più nodi Db2, non vi è alcuna garanzia del corretto ordine delle operazioni sulla destinazione, poiché DMS applica le operazioni in modo indipendente

per ogni nodo Db2. È necessario assicurarsi che l'acquisizione delle transazioni locali indipendentemente da ciascun nodo Db2 funzioni per il caso d'uso specifico.

- Quando si esegue la migrazione da un ambiente DPF, si consiglia di eseguire prima un'attività Full Load senza eventi memorizzati nella cache e quindi eseguire attività solo CDC. Consigliamo di eseguire un'attività per nodo Db2, a partire dal timestamp di inizio Full Load o dal LRI (log record identifier) impostato utilizzando l'impostazione dell'endpoint. `StartFromContext` Per informazioni sulla determinazione del punto di inizio della replica, consulta [Finding the LSN o LRI value for replication start](#) nella documentazione di IBM Support.
- Per la replica continua (CDC), se prevedi di avviare la replica da un timestamp specifico, dovrai impostare l'attributo di connessione `StartFromContext` sul timestamp richiesto.
- Attualmente, DMS non supporta la funzionalità Db2 PureScale, un'estensione di DB2 LUW che è possibile utilizzare per dimensionare la soluzione di database.
- AWS DMS non supporta CDC quando utilizza Db2 for Amazon RDS come sorgente.

Impostazioni degli endpoint quando si utilizza Db2 LUW come sorgente per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di origine Db2 LUW in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di origine utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in [AWS CLI](#), con la sintassi JSON. `--ibm-db2-settings '{"EndpointSetting": "value", ...}'`

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Db2 LUW come origine.

Nome	Descrizione
<code>CurrentLSN</code>	Per la replica in corso (CDC), utilizzare <code>CurrentLSN</code> per specificare un numero di sequenza di log (LSN) in cui si desidera che la replica inizi.
<code>MaxKBytesPerRead</code>	Il numero massimo di byte per lettura, come un valore <code>NUMBER</code> . Il valore predefinito è 64 KB.
<code>SetDataCaptureChanges</code>	Abilita la replica in corso (CDC) come valore <code>BOOLEAN</code> . Il valore predefinito è <code>true</code> .

Nome	Descrizione
StartFromContext	<p>Per la replica continua (CDC), utilizza <code>StartFromContext</code> per specificare il limite minimo di un log da cui iniziare la replica. <code>StartFromContext</code> accetta diverse forme di valori. I valori validi includono:</p> <ul style="list-style-type: none">• <code>timestamp</code> (UTC). Per esempio: <pre>'{"StartFromContext": "timestamp:2021-09-21T13:00:00"}'</pre>• <code>NOW</code> Per IBM DB2 LUW 10.5 e versioni successive, <code>NOW</code> combinato con <code>CurrentLSN: scan</code>, avvia l'attività dal più recente LSO. Per esempio: <pre>'{"CurrentLSN": "scan", "StartFromContext": "NOW"}'</pre>• Un LRI specifico. Per esempio: <pre>'{"StartFromContext": "0100000000000022C000000000004FB13"}'</pre> <p>Per determinare l'intervallo LRI/LSN di un file di log, esegui il comando <code>db2f1sn</code> come illustrato nell'esempio seguente.</p> <pre>db2f1sn -db <i>SAMPLE</i> -lri range 2</pre> <p>L'output dell'esempio è simile al seguente.</p>

Nome	Descrizione
	<p data-bbox="704 212 1446 359">S0000002.LOG: has LRI range 000000000000000010000000000002254000000000004F9A6 to 0000000000000000100000000000022CC000000000004FB13</p> <p data-bbox="688 426 1507 552">In tale output, il file di registro è S0000002.LOG e il valore StartFromContextLRI è costituito dai 34 byte alla fine dell'intervallo.</p> <p data-bbox="704 615 1252 642">0100000000000000022CC000000000004FB13</p>

Tipi di dati di origine per IBM Db2 LUW

La migrazione dei dati che utilizza Db2 LUW come fonte AWS DMS supporta la maggior parte dei tipi di dati Db2 LUW. La tabella seguente mostra i tipi di dati di origine Db2 LUW supportati durante l'utilizzo AWS DMS e la mappatura predefinita dei tipi di dati. AWS DMS Per ulteriori informazioni sui tipi di dati di Db2 LUW, consulta la [documentazione di Db2 LUW](#).

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere. [Tipi di dati per AWS Database Migration Service](#)

Tipi di dati Db2 LUW	AWS DMS tipi di dati
INTEGER	INT4
SMALLINT	INT2
BIGINT	INT8
DECIMAL (p,s)	NUMERIC (p,s)
FLOAT	REAL8
DOUBLE	REAL8

Tipi di dati Db2 LUW	AWS DMS tipi di dati
REAL	REAL4
DECFLOAT (p)	Se la precisione è 16, REAL8; se la precisione è 34, STRING
GRAPHIC (n)	WSTRING, per stringhe di grafici a lunghezza fissa di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 127
VARGRAPHIC (n)	WSTRING, per stringhe di grafici a lunghezza variabile con lunghezza maggiore di 0 e minore o uguale a 16352 caratteri a due byte
LONG VARGRAPHIC (n)	CLOB, per stringhe di grafici a lunghezza variabile con lunghezza maggiore di 0 e minore o uguale a 16352 caratteri a due byte
CHARACTER (n)	STRING, per stringhe a lunghezza fissa di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 255
VARCHAR (n)	STRING, per stringhe a lunghezza variabile di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 32704
LONG VARCHAR (n)	CLOB, per stringhe a lunghezza variabile di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 32704
CHAR (n) FOR BIT DATA	BYTES
VARCHAR (n) FOR BIT DATA	BYTES
LONG VARCHAR FOR BIT DATA	BYTES
DATE	DATE
TIME	TIME

Tipi di dati Db2 LUW	AWS DMS tipi di dati
TIMESTAMP	DATETIME
BLOB(n)	BLOB La lunghezza massima è 2.147.483.647 byte
CLOB(n)	CLOB La lunghezza massima è 2.147.483.647 byte
DBCLOB (n)	CLOB La lunghezza massima: 1.073.741.824 caratteri a due byte
XML	CLOB

Utilizzo dei database IBM Db2 for z/OS come origine per AWS DMS

È possibile migrare i dati da un database IBM for z/OS a qualsiasi database di destinazione supportato utilizzando AWS Database Migration Service (AWS DMS).

Per informazioni sulle versioni di Db2 for z/OS supportate da AWS DMS come origine, consulta [Fonti per AWS DMS](#).

Prerequisiti per utilizzare Db2 for z/OS come origine per AWS DMS

Per utilizzare un database Db2 for z/OS come origine in AWS DMS, fornisci i privilegi seguenti all'utente Db2 for z/OS specificato nelle impostazioni di connessione dell'endpoint di origine.

```
GRANT SELECT ON SYSIBM.SYSTABLES TO Db2USER;
GRANT SELECT ON SYSIBM.SYSTABLESPACE TO Db2USER;
GRANT SELECT ON SYSIBM.SYSTABLEPART TO Db2USER;
GRANT SELECT ON SYSIBM.SYSCOLUMNS TO Db2USER;
GRANT SELECT ON SYSIBM.SYSDATABASE TO Db2USER;
GRANT SELECT ON SYSIBM.SYSDUMMY1 TO Db2USER
```

Fornisci anche `SELECT ON user defined` per le tabelle di origine.

Un endpoint di origine AWS DMS IBM Db2 for z/OS utilizza IBM Data Server Driver for ODBC per accedere ai dati. Il server di database deve disporre di una licenza IBM ODBC Connect valida per consentire a DMS di connettersi a questo endpoint.

Limitazioni relative all'utilizzo di Db2 for z/OS come origine per AWS DMS

Quando si utilizza un database IBM Db2 for z/OS come origine per AWS DMS, si applicano le seguenti limitazioni:

- Sono supportate solo le attività di replica pieno carico. Il CDC (Change Data Capture) non è supportato.
- Il caricamento parallelo non è supportato.
- La convalida dei dati delle viste non è supportata.
- I nomi di schemi, tabelle e colonne devono essere specificati in lettere MAIUSCOLE nelle mappature delle tabelle per le trasformazioni a livello di colonna/tabella e i filtri di selezione a livello di riga.

Tipi di dati di origine per IBM Db2 for z/OS

Le migrazioni di dati che utilizzano Db2 for z/OS come origine per AWS DMS supportano la maggior parte dei tipi di dati Db2 for z/OS. La tabella seguente mostra i tipi di dati di origine di Db2 for z/OS supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati su AWS DMS.

Per ulteriori informazioni sui tipi di dati di Db2 for z/OS, consulta la [documentazione di IBM Db2 for z/OS](#).

Per informazioni su come visualizzare il tipo di dati mappato nella destinazione, consulta la sezione relativa all'endpoint di destinazione che stai utilizzando.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati di Db2 for z/OS	Tipi di dati AWS DMS
INTEGER	INT4
SMALLINT	INT2
BIGINT	INT8

Tipi di dati di Db2 for z/OS	Tipi di dati AWS DMS
DECIMAL (p,s)	NUMERIC (p,s) Se il separatore decimale è impostato su una virgola (,) nella configurazione DB2, configura Replicate per supportare l'impostazione DB2.
FLOAT	REAL8
DOUBLE	REAL8
REAL	REAL4
DECFLOAT (p)	Se la precisione è 16, REAL8; se la precisione è 34, STRING
GRAPHIC (n)	If $n \geq 127$ then WSTRING, per stringhe di grafici a lunghezza fissa di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 127
VARGRAPHIC (n)	WSTRING, per stringhe di grafici a lunghezza variabile con lunghezza maggiore di 0 e minore o uguale a 16352 caratteri a due byte
LONG VARGRAPHIC (n)	CLOB, per stringhe di grafici a lunghezza variabile con lunghezza maggiore di 0 e minore o uguale a 16352 caratteri a due byte
CHARACTER (n)	STRING, per stringhe a lunghezza fissa di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 255
VARCHAR (n)	STRING, per stringhe a lunghezza variabile di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 32704

Tipi di dati di Db2 for z/OS	Tipi di dati AWS DMS
LONG VARCHAR (n)	CLOB, per stringhe a lunghezza variabile di caratteri a due byte con lunghezza maggiore di 0 e minore o uguale a 32704
CHAR (n) FOR BIT DATA	BYTES
VARCHAR (n) FOR BIT DATA	BYTES
LONG VARCHAR FOR BIT DATA	BYTES
DATE	DATE
TIME	TIME
TIMESTAMP	DATETIME
BLOB(n)	BLOB La lunghezza massima è 2.147.483.647 byte
CLOB(n)	CLOB La lunghezza massima è 2.147.483.647 byte
DBCLOB (n)	CLOB La lunghezza massima: 1.073.741.824 caratteri a due byte
XML	CLOB
BINARY	BYTES
VARBINARY	BYTES
ROWID	BYTES. Per ulteriori informazioni sull'utilizzo di ROWID, consulta i seguenti argomenti.
TIMESTAMP WITH TIME ZONE	Non supportato.

Le colonne ROWID vengono migrate per impostazione predefinita quando la modalità di preparazione della tabella di destinazione per l'attività è impostata su `DROP_AND_CREATE` (impostazione predefinita). La convalida dei dati ignora queste colonne perché le righe sono prive di significato al di fuori del database e della tabella specifici. Per disattivare la migrazione di queste colonne, è possibile procedere in uno dei seguenti modi preparatori:

- Crea in anticipo la tabella di destinazione senza queste colonne. Quindi, imposta la modalità di preparazione della tabella di destinazione dell'attività su `DO_NOTHING` o `TRUNCATE_BEFORE_LOAD`. È possibile utilizzare AWS Schema Conversion Tool (AWS SCT) per creare in anticipo la tabella di destinazione senza le colonne.
- Aggiungi una regola di mappatura delle tabelle a un'attività che filtra queste colonne in modo che vengano ignorate. Per ulteriori informazioni, consulta [Operazioni e regole di trasformazione](#).

Regole di confronto EBCDIC in PostgreSQL per il servizio Modernizzazione del mainframe AWS

Il servizio Modernizzazione del mainframe AWS ti aiuta a modernizzare le applicazioni mainframe in ambienti di runtime gestiti AWS. Offre strumenti e risorse per aiutarti a pianificare e implementare i progetti di migrazione e modernizzazione. Per ulteriori informazioni sulla modernizzazione e sulla migrazione del mainframe, consulta [Mainframe Modernization with AWS](#).

Alcuni set di dati IBM Db2 for z/OS sono codificati nel set di caratteri EBCDIC (Extended Binary Coded Decimal Interchange). Si tratta di un set di caratteri sviluppato prima che l'ASCII (American Standard Code for Information Interchange) diventasse comunemente usato. Una tabella codici associa ogni carattere di testo ai caratteri di un set di caratteri. Una tabella codici tradizionale contiene le informazioni di mappatura tra un punto di codice e un ID di carattere. Un ID di carattere è una stringa di dati di caratteri a 8 byte. Un punto di codice è un numero binario a 8 bit che rappresenta un carattere. I punti di codice vengono generalmente visualizzati come rappresentazioni esadecimali dei relativi valori binari.

Se attualmente utilizzi il componente Micro Focus o BluAge del servizio di Modernizzazione del mainframe, è necessario indicare ad AWS DMS di cambiare (tradurre) determinati punti di codice. È possibile utilizzare le impostazioni delle attività AWS DMS per eseguire i cambiamenti. L'esempio seguente mostra come utilizzare l'operazione AWS DMS `CharacterSetSettings` per mappare i cambiamenti in un'impostazione di attività DMS.

```
"CharacterSetSettings": {
  "CharacterSetSupport": null,
```

```

    "CharacterReplacements": [
      {"SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180"}
      , {"SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0160"}
      , {"SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "0161"}
      , {"SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017D"}
      , {"SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "017E"}
      , {"SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0152"}
      , {"SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0153"}
      , {"SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0178"}
    ]
  }
}

```

Esistono già alcune regole di confronto EBCDIC per PostgreSQL che comprendono i cambiamenti necessari. Sono supportate diverse tabelle codici. Le sezioni seguenti forniscono esempi JSON di ciò che è necessario cambiare per tutte le tabelle codici supportate. Puoi semplicemente copiare e incollare il codice JSON necessario nella tua attività DMS.

Regole di confronto EBCDIC specifiche per Micro Focus

Per Micro Focus, cambia un sottoinsieme di caratteri in base alle necessità per le seguenti regole di confronto.

```

da-DK-cp1142m-x-icu
de-DE-cp1141m-x-icu
en-GB-cp1146m-x-icu
en-US-cp1140m-x-icu
es-ES-cp1145m-x-icu
fi-FI-cp1143m-x-icu
fr-FR-cp1147m-x-icu
it-IT-cp1144m-x-icu
nl-BE-cp1148m-x-icu

```

Example Cambiamenti di dati Micro Focus per regola di confronto:

en_us_cp1140m

Cambiamento di codice:

```
0000    0180
```

00A6	0160
00B8	0161
00BC	017D
00BD	017E
00BE	0152
00A8	0153
00B4	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0153" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1141m

Cambiamento di codice:

0000	0180
00B8	0160
00BC	0161
00BD	017D
00BE	017E
00A8	0152
00B4	0153
00A6	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0153" }
```



```
,{"SourceCharacterCodePoint": "00A6","TargetCharacterCodePoint": "0178"}
```

en_us_cp1142m

Cambiamento di codice:

0000	0180
00A6	0160
00B8	0161
00BC	017D
00BD	017E
00BE	0152
00A8	0153
00B4	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0153" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1143m

Cambiamento di codice:

0000	0180
00B8	0160
00BC	0161
00BD	017D
00BE	017E
00A8	0152
00B4	0153

```
00A6    0178
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }  
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0160" }  
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "0161" }  
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017D" }  
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "017E" }  
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0152" }  
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0153" }  
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1144m

Cambiamento di codice:

```
0000    0180  
00B8    0160  
00BC    0161  
00BD    017D  
00BE    017E  
00A8    0152  
00B4    0153  
00A6    0178
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }  
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0160" }  
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "0161" }  
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017D" }  
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "017E" }  
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0152" }  
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0153" }  
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1145m

Cambiamento di codice:

0000	0180
00A6	0160
00B8	0161
00A8	017D
00BC	017E
00BD	0152
00BE	0153
00B4	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }  
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0160" }  
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0161" }  
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "017D" }  
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017E" }  
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "0152" }  
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0153" }  
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1146m

Cambiamento di codice:

0000	0180
00A6	0160
00B8	0161
00BC	017D
00BD	017E
00BE	0152
00A8	0153
00B4	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0153" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1147m

Cambiamento di codice:

0000	0180
00B8	0160
00A8	0161
00BC	017D
00BD	017E
00BE	0152
00B4	0153
00A6	0178

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0153" }
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0178" }
```

en_us_cp1148m

Cambiamento di codice:

0000	0180
------	------

```
00A6    0160
00B8    0161
00BC    017D
00BD    017E
00BE    0152
00A8    0153
00B4    0178
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0000", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "00A6", "TargetCharacterCodePoint": "0160" }
, { "SourceCharacterCodePoint": "00B8", "TargetCharacterCodePoint": "0161" }
, { "SourceCharacterCodePoint": "00BC", "TargetCharacterCodePoint": "017D" }
, { "SourceCharacterCodePoint": "00BD", "TargetCharacterCodePoint": "017E" }
, { "SourceCharacterCodePoint": "00BE", "TargetCharacterCodePoint": "0152" }
, { "SourceCharacterCodePoint": "00A8", "TargetCharacterCodePoint": "0153" }
, { "SourceCharacterCodePoint": "00B4", "TargetCharacterCodePoint": "0178" }
```

Regole di confronto EBCDIC specifiche per BluAge

Per BluAge, cambia tutti i seguenti valori bassi e valori alti secondo necessità. Queste regole di confronto devono essere utilizzate solo per supportare il servizio di migrazione del mainframe BluAge.

```
da-DK-cp1142b-x-icu
da-DK-cp277b-x-icu
de-DE-cp1141b-x-icu
de-DE-cp273b-x-icu
en-GB-cp1146b-x-icu
en-GB-cp285b-x-icu
en-US-cp037b-x-icu
en-US-cp1140b-x-icu
es-ES-cp1145b-x-icu
es-ES-cp284b-x-icu
fi-FI-cp1143b-x-icu
fi-FI-cp278b-x-icu
fr-FR-cp1147b-x-icu
fr-FR-cp297b-x-icu
it-IT-cp1144b-x-icu
```

```
it-IT-cp280b-x-icu  
nl-BE-cp1148b-x-icu  
nl-BE-cp500b-x-icu
```

Example Cambiamenti di dati BluAge:

da-DK-cp277b e da-DK-cp1142b

Cambiamento di codice:

```
0180    0180  
0001    0181  
0002    0182  
0003    0183  
009C    0184  
0009    0185  
0086    0186  
007F    0187  
0097    0188  
008D    0189  
008E    018A  
000B    018B  
000C    018C  
000D    018D  
000E    018E  
000F    018F  
0010    0190  
0011    0191  
0012    0192  
0013    0193  
009D    0194  
0085    0195  
0008    0196  
0087    0197  
0018    0198  
0019    0199  
0092    019A  
008F    019B  
001C    019C  
001D    019D  
001E    019E  
001F    019F  
0080    01A0
```

```
0081    01A1
0082    01A2
0083    01A3
0084    01A4
000A    01A5
0017    01A6
001B    01A7
0088    01A8
0089    01A9
008A    01AA
008B    01AB
008C    01AC
0005    01AD
0006    01AE
0007    01AF
0090    01B0
0091    01B1
0016    01B2
0093    01B3
0094    01B4
0095    01B5
0096    01B6
0004    01B7
0098    01B8
0099    01B9
009A    01BA
009B    01BB
0014    01BC
0015    01BD
009E    01BE
001A    01BF
009F    027F
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181" }
, { "SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182" }
, { "SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183" }
, { "SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184" }
, { "SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185" }
, { "SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186" }
```

```
,{"SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"}
,{"SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"}
,{"SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"}
,{"SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"}
,{"SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"}
,{"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
,{"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
,{"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
,{"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
,{"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
,{"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
,{"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
,{"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
,{"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
,{"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
,{"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
,{"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
,{"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
,{"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
,{"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
,{"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
,{"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
,{"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
,{"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
,{"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
,{"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
,{"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
,{"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
,{"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
,{"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
,{"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
,{"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
,{"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
,{"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
,{"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
,{"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
,{"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
,{"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
,{"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
,{"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
,{"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
,{"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
,{"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
,{"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
```



```
,{"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}  
,{"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}  
,{"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}  
,{"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}  
,{"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}  
,{"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}  
,{"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}  
,{"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}  
,{"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}  
,{"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}  
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}  
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}  
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}  
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

de-DE-273b e de-DE-1141b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196

0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF
0090	01B0
0091	01B1
0016	01B2
0093	01B3
0094	01B4
0095	01B5
0096	01B6
0004	01B7
0098	01B8
0099	01B9
009A	01BA
009B	01BB
0014	01BC
0015	01BD
009E	01BE
001A	01BF
009F	027F

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181" }
, { "SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182" }
, { "SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183" }
, { "SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184" }
, { "SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185" }
, { "SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186" }
, { "SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187" }
, { "SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188" }
, { "SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189" }
, { "SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A" }
, { "SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B" }
, { "SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C" }
, { "SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D" }
, { "SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E" }
, { "SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F" }
, { "SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190" }
, { "SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191" }
, { "SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192" }
, { "SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193" }
, { "SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194" }
, { "SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195" }
, { "SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196" }
, { "SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197" }
, { "SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198" }
, { "SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199" }
, { "SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A" }
, { "SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B" }
, { "SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C" }
, { "SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D" }
, { "SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E" }
, { "SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F" }
, { "SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0" }
, { "SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1" }
, { "SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2" }
, { "SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3" }
, { "SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4" }
, { "SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5" }
, { "SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6" }
, { "SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7" }
, { "SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8" }
, { "SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9" }
```

```
, {"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
, {"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
, {"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
, {"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
, {"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
, {"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
, {"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
, {"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
, {"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
, {"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
, {"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
, {"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
, {"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
, {"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
, {"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
, {"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
, {"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
, {"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
, {"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
, {"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
, {"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
, {"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
, {"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

en-GB-285b e en-GB-1146b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D

000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF
0090	01B0
0091	01B1
0016	01B2
0093	01B3
0094	01B4
0095	01B5
0096	01B6
0004	01B7
0098	01B8
0099	01B9

009A	01BA
009B	01BB
0014	01BC
0015	01BD
009E	01BE
001A	01BF
009F	027F

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{
  "SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180"
}, {
  "SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181"
}, {
  "SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182"
}, {
  "SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183"
}, {
  "SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184"
}, {
  "SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185"
}, {
  "SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186"
}, {
  "SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"
}, {
  "SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"
}, {
  "SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"
}, {
  "SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"
}, {
  "SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"
}, {
  "SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"
}, {
  "SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"
}, {
  "SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"
}, {
  "SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"
}, {
  "SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"
}, {
  "SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"
}, {
  "SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"
}, {
  "SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"
}, {
  "SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"
}, {
  "SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"
}, {
  "SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"
}, {
  "SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"
}, {
  "SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"
}, {
  "SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"
}, {
  "SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"
}, {
  "SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"
}, {
  "SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"
}, {
  "SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"
}, {
  "SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"
}, {
  "SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"
}
```

```

,{"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
,{"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
,{"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
,{"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
,{"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
,{"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
,{"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
,{"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
,{"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
,{"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
,{"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
,{"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
,{"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
,{"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
,{"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
,{"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
,{"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
,{"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
,{"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
,{"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
,{"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
,{"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
,{"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
,{"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
,{"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
,{"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
,{"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
,{"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
,{"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}

```

en-us-037b e en-us-1140b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183

009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF


```
0090    01B0
0091    01B1
0016    01B2
0093    01B3
0094    01B4
0095    01B5
0096    01B6
0004    01B7
0098    01B8
0099    01B9
009A    01BA
009B    01BB
0014    01BC
0015    01BD
009E    01BE
001A    01BF
009F    027F
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{"SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180"}
, {"SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181"}
, {"SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182"}
, {"SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183"}
, {"SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184"}
, {"SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185"}
, {"SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186"}
, {"SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"}
, {"SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"}
, {"SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"}
, {"SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"}
, {"SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"}
, {"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
, {"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
, {"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
, {"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
, {"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
, {"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
, {"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
, {"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
, {"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
, {"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
```

```
, {"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
, {"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
, {"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
, {"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
, {"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
, {"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
, {"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
, {"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
, {"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
, {"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
, {"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
, {"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
, {"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
, {"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
, {"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
, {"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
, {"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
, {"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
, {"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
, {"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
, {"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
, {"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
, {"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
, {"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
, {"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
, {"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
, {"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
, {"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
, {"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
, {"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
, {"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
, {"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
, {"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
, {"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
, {"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
, {"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
, {"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
, {"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
, {"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
, {"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
, {"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
, {"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
, {"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

es-ES-284b e es-ES-1145b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5

```
0017    01A6
001B    01A7
0088    01A8
0089    01A9
008A    01AA
008B    01AB
008C    01AC
0005    01AD
0006    01AE
0007    01AF
0090    01B0
0091    01B1
0016    01B2
0093    01B3
0094    01B4
0095    01B5
0096    01B6
0004    01B7
0098    01B8
0099    01B9
009A    01BA
009B    01BB
0014    01BC
0015    01BD
009E    01BE
001A    01BF
009F    027F
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181" }
, { "SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182" }
, { "SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183" }
, { "SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184" }
, { "SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185" }
, { "SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186" }
, { "SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187" }
, { "SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188" }
, { "SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189" }
, { "SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A" }
, { "SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B" }
```

```
, {"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
, {"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
, {"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
, {"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
, {"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
, {"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
, {"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
, {"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
, {"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
, {"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
, {"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
, {"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
, {"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
, {"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
, {"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
, {"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
, {"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
, {"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
, {"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
, {"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
, {"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
, {"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
, {"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
, {"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
, {"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
, {"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
, {"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
, {"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
, {"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
, {"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
, {"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
, {"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
, {"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
, {"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
, {"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
, {"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
, {"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
, {"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
, {"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
, {"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
, {"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
, {"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
, {"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
, {"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
```

```
,{"SourceCharacterCodePoint": "0098","TargetCharacterCodePoint": "01B8"}  
,{"SourceCharacterCodePoint": "0099","TargetCharacterCodePoint": "01B9"}  
,{"SourceCharacterCodePoint": "009A","TargetCharacterCodePoint": "01BA"}  
,{"SourceCharacterCodePoint": "009B","TargetCharacterCodePoint": "01BB"}  
,{"SourceCharacterCodePoint": "0014","TargetCharacterCodePoint": "01BC"}  
,{"SourceCharacterCodePoint": "0015","TargetCharacterCodePoint": "01BD"}  
,{"SourceCharacterCodePoint": "009E","TargetCharacterCodePoint": "01BE"}  
,{"SourceCharacterCodePoint": "001A","TargetCharacterCodePoint": "01BF"}  
,{"SourceCharacterCodePoint": "009F","TargetCharacterCodePoint": "027F"}
```

fi_FI-278b e fi-FI-1143b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B

001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF
0090	01B0
0091	01B1
0016	01B2
0093	01B3
0094	01B4
0095	01B5
0096	01B6
0004	01B7
0098	01B8
0099	01B9
009A	01BA
009B	01BB
0014	01BC
0015	01BD
009E	01BE
001A	01BF
009F	027F

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{"SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180"}  
, {"SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181"}
```

```
,{"SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182"}
,{"SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183"}
,{"SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184"}
,{"SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185"}
,{"SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186"}
,{"SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"}
,{"SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"}
,{"SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"}
,{"SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"}
,{"SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"}
,{"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
,{"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
,{"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
,{"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
,{"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
,{"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
,{"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
,{"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
,{"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
,{"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
,{"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
,{"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
,{"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
,{"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
,{"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
,{"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
,{"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
,{"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
,{"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
,{"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
,{"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
,{"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
,{"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
,{"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
,{"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
,{"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
,{"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
,{"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
,{"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
,{"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
,{"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
,{"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
,{"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
,{"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
```



```
,{"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
,{"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
,{"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
,{"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
,{"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
,{"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
,{"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
,{"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
,{"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
,{"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
,{"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
,{"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
,{"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
,{"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
,{"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

fr-FR-297b e fr-FR-1147b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192

0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF
0090	01B0
0091	01B1
0016	01B2
0093	01B3
0094	01B4
0095	01B5
0096	01B6
0004	01B7
0098	01B8
0099	01B9
009A	01BA
009B	01BB
0014	01BC
0015	01BD
009E	01BE

```
001A    01BF
009F    027F
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{"SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180"}
, {"SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181"}
, {"SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182"}
, {"SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183"}
, {"SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184"}
, {"SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185"}
, {"SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186"}
, {"SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"}
, {"SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"}
, {"SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"}
, {"SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"}
, {"SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"}
, {"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
, {"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
, {"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
, {"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
, {"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
, {"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
, {"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
, {"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
, {"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
, {"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
, {"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
, {"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
, {"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
, {"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
, {"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
, {"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
, {"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
, {"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
, {"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
, {"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
, {"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
, {"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
, {"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
, {"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
, {"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
```

```
,{"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
,{"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
,{"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
,{"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
,{"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
,{"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
,{"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
,{"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
,{"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
,{"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
,{"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
,{"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
,{"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
,{"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
,{"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
,{"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
,{"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
,{"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
,{"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
,{"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
,{"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
,{"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
,{"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
,{"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

it-IT-280b e it-IT-1144b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188

008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA
008B	01AB
008C	01AC
0005	01AD
0006	01AE
0007	01AF
0090	01B0
0091	01B1
0016	01B2
0093	01B3
0094	01B4

```

0095    01B5
0096    01B6
0004    01B7
0098    01B8
0099    01B9
009A    01BA
009B    01BB
0014    01BC
0015    01BD
009E    01BE
001A    01BF
009F    027F

```

Mappatura degli input corrispondente per un'attività AWS DMS:

```

{"SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180"}
, {"SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181"}
, {"SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182"}
, {"SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183"}
, {"SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184"}
, {"SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185"}
, {"SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186"}
, {"SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187"}
, {"SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188"}
, {"SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189"}
, {"SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A"}
, {"SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B"}
, {"SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C"}
, {"SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D"}
, {"SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E"}
, {"SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F"}
, {"SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190"}
, {"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
, {"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
, {"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
, {"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
, {"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
, {"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
, {"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
, {"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
, {"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
, {"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}

```

```
,{"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
,{"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
,{"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
,{"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
,{"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
,{"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
,{"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
,{"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
,{"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
,{"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
,{"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
,{"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
,{"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
,{"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
,{"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
,{"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
,{"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
,{"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
,{"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
,{"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
,{"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
,{"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
,{"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
,{"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
,{"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
,{"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
,{"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
,{"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
,{"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
,{"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
,{"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
,{"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
,{"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
,{"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

nl-BE-500b e nl-BE-1148b

Cambiamento di codice:

0180	0180
0001	0181
0002	0182
0003	0183
009C	0184
0009	0185
0086	0186
007F	0187
0097	0188
008D	0189
008E	018A
000B	018B
000C	018C
000D	018D
000E	018E
000F	018F
0010	0190
0011	0191
0012	0192
0013	0193
009D	0194
0085	0195
0008	0196
0087	0197
0018	0198
0019	0199
0092	019A
008F	019B
001C	019C
001D	019D
001E	019E
001F	019F
0080	01A0
0081	01A1
0082	01A2
0083	01A3
0084	01A4
000A	01A5
0017	01A6
001B	01A7
0088	01A8
0089	01A9
008A	01AA


```
008B    01AB
008C    01AC
0005    01AD
0006    01AE
0007    01AF
0090    01B0
0091    01B1
0016    01B2
0093    01B3
0094    01B4
0095    01B5
0096    01B6
0004    01B7
0098    01B8
0099    01B9
009A    01BA
009B    01BB
0014    01BC
0015    01BD
009E    01BE
001A    01BF
009F    027F
```

Mappatura degli input corrispondente per un'attività AWS DMS:

```
{ "SourceCharacterCodePoint": "0180", "TargetCharacterCodePoint": "0180" }
, { "SourceCharacterCodePoint": "0001", "TargetCharacterCodePoint": "0181" }
, { "SourceCharacterCodePoint": "0002", "TargetCharacterCodePoint": "0182" }
, { "SourceCharacterCodePoint": "0003", "TargetCharacterCodePoint": "0183" }
, { "SourceCharacterCodePoint": "009C", "TargetCharacterCodePoint": "0184" }
, { "SourceCharacterCodePoint": "0009", "TargetCharacterCodePoint": "0185" }
, { "SourceCharacterCodePoint": "0086", "TargetCharacterCodePoint": "0186" }
, { "SourceCharacterCodePoint": "007F", "TargetCharacterCodePoint": "0187" }
, { "SourceCharacterCodePoint": "0097", "TargetCharacterCodePoint": "0188" }
, { "SourceCharacterCodePoint": "008D", "TargetCharacterCodePoint": "0189" }
, { "SourceCharacterCodePoint": "008E", "TargetCharacterCodePoint": "018A" }
, { "SourceCharacterCodePoint": "000B", "TargetCharacterCodePoint": "018B" }
, { "SourceCharacterCodePoint": "000C", "TargetCharacterCodePoint": "018C" }
, { "SourceCharacterCodePoint": "000D", "TargetCharacterCodePoint": "018D" }
, { "SourceCharacterCodePoint": "000E", "TargetCharacterCodePoint": "018E" }
, { "SourceCharacterCodePoint": "000F", "TargetCharacterCodePoint": "018F" }
, { "SourceCharacterCodePoint": "0010", "TargetCharacterCodePoint": "0190" }
```

```
, {"SourceCharacterCodePoint": "0011", "TargetCharacterCodePoint": "0191"}
, {"SourceCharacterCodePoint": "0012", "TargetCharacterCodePoint": "0192"}
, {"SourceCharacterCodePoint": "0013", "TargetCharacterCodePoint": "0193"}
, {"SourceCharacterCodePoint": "009D", "TargetCharacterCodePoint": "0194"}
, {"SourceCharacterCodePoint": "0085", "TargetCharacterCodePoint": "0195"}
, {"SourceCharacterCodePoint": "0008", "TargetCharacterCodePoint": "0196"}
, {"SourceCharacterCodePoint": "0087", "TargetCharacterCodePoint": "0197"}
, {"SourceCharacterCodePoint": "0018", "TargetCharacterCodePoint": "0198"}
, {"SourceCharacterCodePoint": "0019", "TargetCharacterCodePoint": "0199"}
, {"SourceCharacterCodePoint": "0092", "TargetCharacterCodePoint": "019A"}
, {"SourceCharacterCodePoint": "008F", "TargetCharacterCodePoint": "019B"}
, {"SourceCharacterCodePoint": "001C", "TargetCharacterCodePoint": "019C"}
, {"SourceCharacterCodePoint": "001D", "TargetCharacterCodePoint": "019D"}
, {"SourceCharacterCodePoint": "001E", "TargetCharacterCodePoint": "019E"}
, {"SourceCharacterCodePoint": "001F", "TargetCharacterCodePoint": "019F"}
, {"SourceCharacterCodePoint": "0080", "TargetCharacterCodePoint": "01A0"}
, {"SourceCharacterCodePoint": "0081", "TargetCharacterCodePoint": "01A1"}
, {"SourceCharacterCodePoint": "0082", "TargetCharacterCodePoint": "01A2"}
, {"SourceCharacterCodePoint": "0083", "TargetCharacterCodePoint": "01A3"}
, {"SourceCharacterCodePoint": "0084", "TargetCharacterCodePoint": "01A4"}
, {"SourceCharacterCodePoint": "000A", "TargetCharacterCodePoint": "01A5"}
, {"SourceCharacterCodePoint": "0017", "TargetCharacterCodePoint": "01A6"}
, {"SourceCharacterCodePoint": "001B", "TargetCharacterCodePoint": "01A7"}
, {"SourceCharacterCodePoint": "0088", "TargetCharacterCodePoint": "01A8"}
, {"SourceCharacterCodePoint": "0089", "TargetCharacterCodePoint": "01A9"}
, {"SourceCharacterCodePoint": "008A", "TargetCharacterCodePoint": "01AA"}
, {"SourceCharacterCodePoint": "008B", "TargetCharacterCodePoint": "01AB"}
, {"SourceCharacterCodePoint": "008C", "TargetCharacterCodePoint": "01AC"}
, {"SourceCharacterCodePoint": "0005", "TargetCharacterCodePoint": "01AD"}
, {"SourceCharacterCodePoint": "0006", "TargetCharacterCodePoint": "01AE"}
, {"SourceCharacterCodePoint": "0007", "TargetCharacterCodePoint": "01AF"}
, {"SourceCharacterCodePoint": "0090", "TargetCharacterCodePoint": "01B0"}
, {"SourceCharacterCodePoint": "0091", "TargetCharacterCodePoint": "01B1"}
, {"SourceCharacterCodePoint": "0016", "TargetCharacterCodePoint": "01B2"}
, {"SourceCharacterCodePoint": "0093", "TargetCharacterCodePoint": "01B3"}
, {"SourceCharacterCodePoint": "0094", "TargetCharacterCodePoint": "01B4"}
, {"SourceCharacterCodePoint": "0095", "TargetCharacterCodePoint": "01B5"}
, {"SourceCharacterCodePoint": "0096", "TargetCharacterCodePoint": "01B6"}
, {"SourceCharacterCodePoint": "0004", "TargetCharacterCodePoint": "01B7"}
, {"SourceCharacterCodePoint": "0098", "TargetCharacterCodePoint": "01B8"}
, {"SourceCharacterCodePoint": "0099", "TargetCharacterCodePoint": "01B9"}
, {"SourceCharacterCodePoint": "009A", "TargetCharacterCodePoint": "01BA"}
, {"SourceCharacterCodePoint": "009B", "TargetCharacterCodePoint": "01BB"}
, {"SourceCharacterCodePoint": "0014", "TargetCharacterCodePoint": "01BC"}
```

```
,{"SourceCharacterCodePoint": "0015", "TargetCharacterCodePoint": "01BD"}  
,{"SourceCharacterCodePoint": "009E", "TargetCharacterCodePoint": "01BE"}  
,{"SourceCharacterCodePoint": "001A", "TargetCharacterCodePoint": "01BF"}  
,{"SourceCharacterCodePoint": "009F", "TargetCharacterCodePoint": "027F"}
```

Destinazioni per la migrazione dei dati

AWS Database Migration Service (AWS DMS) può utilizzare molti dei più noti database come destinazione per la replica dei dati. La destinazione può trovarsi su un'istanza Amazon Elastic Compute Cloud (Amazon EC2), un'istanza Amazon Relational Database Service (Amazon RDS) o un database on-premise.

Per l'elenco completo delle destinazioni valide, consulta [Destinazioni per AWS DMS](#).

Note

AWS DMS non supporta la migrazione tra regioni AWS per i seguenti tipi di endpoint di destinazione:

- Amazon DynamoDB
- Servizio OpenSearch di Amazon
- Flusso di dati Amazon Kinesis

Argomenti

- [Utilizzo di un database Oracle come destinazione per AWS Database Migration Service](#)
- [Utilizzo di un database Microsoft SQL Server come destinazione per AWS Database Migration Service](#)
- [Utilizzo di un database PostgreSQL come destinazione per AWS Database Migration Service](#)
- [Utilizzo di un database compatibile con MySQL come destinazione per AWS Database Migration Service](#)
- [Utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service](#)
- [Utilizzo di un database SAP ASE come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon S3 come destinazione per AWS Database Migration Service](#)

- [Utilizzo di un database Amazon DynamoDB come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon Kinesis Data Streams come destinazione per AWS Database Migration Service](#)
- [Usare Apache Kafka come obiettivo per AWS Database Migration Service](#)
- [Utilizzo di un cluster del servizio OpenSearch di Amazon come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon Neptune come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Redis come destinazione per AWS Database Migration Service](#)
- [Uso di Babelfish come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service](#)
- [Utilizzo di Amazon RDS per Db2 e IBM Db2 LUW come destinazione per AWS DMS](#)

Utilizzo di un database Oracle come destinazione per AWS Database Migration Service

È possibile migrare i dati verso le destinazioni del database Oracle utilizzando AWS DMS, da un altro database Oracle o da uno degli altri database supportati. Puoi utilizzare il protocollo Secure Sockets Layer (SSL) per crittografare le connessioni tra l'endpoint Oracle e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint Oracle, vedere [Utilizzo di SSL con AWS Database Migration Service](#). AWS DMS supporta anche l'uso di Oracle Transparent Data Encryption (TDE) per crittografare i dati inattivi nel database di destinazione, poiché Oracle TDE non richiede una chiave di crittografia o una password per scrivere sul database.

Per informazioni sulle versioni di Oracle AWS DMS supportate come destinazione, vedere [Obiettivi per AWS DMS](#).

Quando si utilizza Oracle come destinazione, presupponiamo che i dati debbano essere migrati nello schema o nell'utente utilizzato per la connessione alla destinazione. Se desideri migrare i dati a un altro schema, utilizza una trasformazione dello schema. Ad esempio, supponiamo che l'endpoint di destinazione si connetta all'utente RDSMASTER e che tu intenda migrare dall'utente PERFDATA1 a PERFDATA2. In questo caso, crea una trasformazione come la seguente.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "rename",
  "rule-target": "schema",
  "object-locator": {
    "schema-name": "PERFDATA1"
  },
  "value": "PERFDATA2"
}
```

Quando si utilizza Oracle come destinazione, AWS DMS migra tutte le tabelle e gli indici nelle tablespace di tabelle e indici predefinite nella destinazione. Se desideri migrare tabelle e indici a spazi di tabella e indice diversi, utilizza a questo scopo una trasformazione di spazio di tabella. Ad esempio, supponi di disporre di un set di tabelle nello schema INVENTORY assegnato ad alcuni spazi tabella nell'origine Oracle. Per la migrazione, vuoi assegnare tutte queste tabelle a un singolo spazio tabella INVENTORYSPACE nella destinazione. In questo caso, crea una trasformazione come la seguente.

```
{
  "rule-type": "transformation",
  "rule-id": "3",
  "rule-name": "3",
  "rule-action": "rename",
  "rule-target": "table-tablespace",
  "object-locator": {
    "schema-name": "INVENTORY",
    "table-name": "%",
    "table-tablespace-name": "%"
  },
  "value": "INVENTORYSPACE"
}
```

Per ulteriori informazioni sulle trasformazioni, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).

Se Oracle è sia origine che destinazione, è possibile mantenere le assegnazioni di tablespace tabella o indice esistenti impostando l'attributo di connessione extra di origine Oracle, `enableHomogenousTablespace=true`. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#)

Per ulteriori dettagli sull'utilizzo dei database Oracle come destinazione per AWS DMS, consulta le seguenti sezioni:

Argomenti

- [Limitazioni relative a Oracle come destinazione per AWS Database Migration Service](#)
- [Privilegi dell'account utente necessari per l'utilizzo di Oracle come destinazione](#)
- [Configurazione di un database Oracle come destinazione per AWS Database Migration Service](#)
- [Impostazioni degli endpoint quando si utilizza Oracle come destinazione per AWS DMS](#)
- [Tipi di dati di destinazione per Oracle](#)

Limitazioni relative a Oracle come destinazione per AWS Database Migration Service

Di seguito sono riportate le limitazioni quando si utilizza Oracle come destinazione per la migrazione dei dati:

- AWS DMS non crea uno schema sul database Oracle di destinazione. Gli eventuali schemi devono essere creati sul database Oracle di destinazione. Il nome dello schema deve esistere già per la destinazione di Oracle. Le tabelle dallo schema di origine vengono importate nell'utente o nello schema, che AWS DMS utilizza per connettersi all'istanza di destinazione. Per migrare più schemi, puoi creare più attività di replica. Inoltre puoi migrare i dati in schemi diversi di una destinazione. A tale scopo, è necessario utilizzare le regole di trasformazione dello schema sulle mappature delle AWS DMS tabelle.
- AWS DMS non supporta l'opzione `Use direct path full load` per le tabelle con `INDEXTYPE CONTEXT`. Come soluzione alternativa, puoi utilizzare il caricamento della matrice.
- Con l'opzione di applicazione ottimizzata in batch, il caricamento nella tabella delle modifiche utilizza un percorso diretto che non supporta il tipo XML. Come soluzione alternativa, è possibile utilizzare la modalità di applicazione transazionale.
- Le stringhe vuote migrate dai database di origine possono essere trattate in modo diverso dalla destinazione Oracle (ad esempio, convertite in stringhe di uno spazio). Ciò può comportare la AWS DMS segnalazione di una mancata corrispondenza nella convalida.
- È possibile esprimere il numero totale di colonne per tabella supportate nella modalità di applicazione ottimizzata in batch, utilizzando la seguente formula:

$$2 * \text{columns_in_original_table} + \text{columns_in_primary_key} \leq 999$$

Ad esempio, se la tabella originale ha 25 colonne e la chiave primaria è composta da 5 colonne, il numero totale di colonne è 55. Se una tabella supera il numero di colonne supportato, tutte le modifiche vengono applicate in modalità one-by-one

- AWS DMS non supporta Autonomous DB su Oracle Cloud Infrastructure (OCI).

Privilegi dell'account utente necessari per l'utilizzo di Oracle come destinazione

Per utilizzare un target Oracle in un AWS Database Migration Service task, concedi i seguenti privilegi nel database Oracle. Concedere tali privilegi all'account utente specificato nelle definizioni del database Oracle per AWS DMS.

- SELECT ANY TRANSACTION
- SELECT su V\$NLS_PARAMETERS
- SELECT su V\$TIMEZONE_NAMES
- SELECT su ALL_INDEXES
- SELECT su ALL_OBJECTS
- SELECT su DBA_OBJECTS
- SELECT su ALL_TABLES
- SELECT su ALL_USERS
- SELECT su ALL_CATALOG
- SELECT su ALL_CONSTRAINTS
- SELECT su ALL_CONS_COLUMNS
- SELECT su ALL_TAB_COLS
- SELECT su ALL_IND_COLUMNS
- DROP ANY TABLE
- SELECT ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE
- CREATE ANY VIEW
- DROP ANY VIEW
- CREATE ANY PROCEDURE

- ALTER ANY PROCEDURE
- DROP ANY PROCEDURE
- CREATE ANY SEQUENCE
- ALTER ANY SEQUENCE
- DROP ANY SEQUENCE
- DELETE ANY TABLE

Per i seguenti requisiti concedi questi privilegi aggiuntivi:

- Per utilizzare un elenco specifico di tabelle, concedi SELECT su qualsiasi tabella replicata e anche ALTER su qualsiasi tabella replicata.
- Per consentire a un utente di creare una tabella in uno spazio tabella predefinito, concedi il privilegio GRANT UNLIMITED TABLESPACE.
- Per l'accesso, concedi il privilegio CREATE SESSION.
- Se stai utilizzando un percorso diretto (che è l'impostazione predefinita per il pieno carico), GRANT LOCK ANY TABLE to *dms_user*;
- Se lo schema è diverso quando si utilizza la modalità di preparazione della tabella "DROP and CREATE", GRANT CREATE ANY INDEX to *dms_user*;
- Per alcuni scenari di caricamento completo, è possibile scegliere le opzioni "DROP and CREATE table" o "TRUNCATE before loading" in cui uno schema della tabella di destinazione è diverso da quello dell'utente DMS. In questo caso, concedere DROP ANY TABLE.
- Per archiviare le modifiche in tabelle di modifica o in una tabella di audit in cui lo schema della tabella di destinazione è diverso da quello dell'utente DMS, concedere CREATE ANY TABLE e CREATE ANY INDEX.

Privilegi di lettura richiesti per AWS Database Migration Service il database di destinazione

All'account AWS DMS utente devono essere concesse le autorizzazioni di lettura per le seguenti tabelle DBA:

- SELECT su DBA_USERS
- SELECT su DBA_TAB_PRIVS
- SELECT su DBA_OBJECTS
- SELECT su DBA_SYNONYMS

- SELECT su DBA_SEQUENCES
- SELECT su DBA_TYPES
- SELECT su DBA_INDEXES
- SELECT su DBA_TABLES
- SELECT su DBA_TRIGGERS
- SELECT su SYS.DBA_REGISTRY

Se uno o più privilegi necessari non possono essere concessi a V\$xxx, concedili a V_\$xxx.

Valutazioni preliminari alla migrazione

Per utilizzare le valutazioni di premigrazione elencate in [Valutazioni Oracle](#) Oracle as a Target, è necessario aggiungere le seguenti autorizzazioni all'utente del dms_user database sul database di destinazione:

```
GRANT SELECT ON V_$INSTANCE TO dms_user;
```

Configurazione di un database Oracle come destinazione per AWS Database Migration Service

Prima di utilizzare un database Oracle come obiettivo di migrazione dei dati, è necessario fornire un account utente Oracle a AWS DMS. L'account utente deve disporre dei privilegi di lettura/scrittura sul database Oracle, come specificato in [Privilegi dell'account utente necessari per l'utilizzo di Oracle come destinazione](#).

Impostazioni degli endpoint quando si utilizza Oracle come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione Oracle in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la AWS DMS console o utilizzando il create-endpoint comando in [AWS CLI](#), con la sintassi --oracle-settings '{"EndpointSetting": "value", ...}' JSON.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Oracle come destinazione.

Nome	Descrizione
EscapeCharacter	<p>Imposta questo attributo su un carattere di escape. Il carattere di escape consente che un singolo carattere jolly si comporti come un normale carattere nelle espressioni di mappatura delle tabelle. Per ulteriori informazioni, consulta Caratteri jolly nella mappatura delle tabelle.</p> <p>Valore predefinito: Null</p> <p>Valori validi: qualsiasi carattere diverso da un carattere jolly</p> <p>Esempio: <code>--oracle-settings '{"EscapeCharacter": "#"}'</code></p>
UseDirectPathFullLoad	<p>Se impostato su Y, AWS DMS utilizza un percorso diretto a pieno carico. Specificare questo valore per abilitare il protocollo di percorso diretto in Oracle Call Interface (OCI). Questo protocollo OCI consente il caricamento in blocco delle tabelle di destinazione Oracle durante un caricamento completo.</p> <p>Valore predefinito: true</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"UseDirectPathFullLoad": false}'</code></p>
DirectPathParallelLoad	<p>Se impostato su true, questo attributo specifica un caricamento parallelo quando UseDirectPathFullLoad è impostato su Y. Questo attributo si applica anche solo quando si utilizza la funzione di caricamento AWS DMS parallelo. Per ulteriori informazioni, vedere la descrizione dell'operazione parallel-load in Regole e operazioni delle impostazioni di tabella e raccolta.</p>

Nome	Descrizione
	<p>Una limitazione della specificazione di questa impostazione di caricamento parallelo è che la tabella di destinazione non può avere vincoli o indici. Per ulteriori informazioni su questa limitazione, vedere Abilitazione dei vincoli dopo un caricamento parallelo con percorso diretto. Se i vincoli o gli indici sono abilitati, l'impostazione di questo attributo non ha alcun effetto su <code>true</code>.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"Direct PathParallelLoad": true}'</code></p>
DirectPathNoLog	<p>Se impostato su <code>true</code>, questo attributo consente di aumentare la velocità di commit nel database di destinazione Oracle scrivendo direttamente nelle tabelle e non scrivendo un trail ai log del database. Per ulteriori informazioni, vedere INSERT a caricamento diretto. Inoltre, questo attributo si applica solo quando si imposta <code>UseDirectPathFullLoad</code> su <code>Y</code>.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio: <code>--oracle-settings '{"Direct PathNoLog": true}'</code></p>

Nome	Descrizione
CharLengthSemantics	<p>Specifica se la lunghezza di una colonna di caratteri è espressa in byte o in caratteri. Per indicare che la lunghezza della colonna dei caratteri è in caratteri, impostare questo attributo su CHAR. In caso contrario, la lunghezza della colonna dei caratteri è espressa in byte.</p> <p>Valore predefinito: non impostato su CHAR</p> <p>Valori validi: CHAR</p> <p>Esempio: <code>--oracle-settings '{"CharLengthSemantics": "CHAR"}'</code></p>
AlwaysReplaceEmptyString	<p>AWS DMS aggiunge uno spazio aggiuntivo per replicare una stringa vuota durante la migrazione verso un target Oracle. In generale, Oracle non dispone di una notazione per una stringa vuota. Quando si inserisce una stringa vuota in varchar2, le stringhe vuote vengono caricate come NULL. Se desideri inserire i dati come NULL su Oracle, imposta questo attributo su FALSE.</p> <p>Valore predefinito: true</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--oracle-settings '{"AlwaysReplaceEmptyString": false}'</code></p>

Tipi di dati di destinazione per Oracle

Un database Oracle di destinazione utilizzato con AWS DMS supporta la maggior parte dei tipi di dati Oracle. La tabella seguente mostra i tipi di dati di destinazione Oracle supportati durante l'utilizzo AWS DMS e la mappatura predefinita AWS DMS dei tipi di dati. Per ulteriori informazioni su come visualizzare il tipo di dati mappato dall'origine, consulta la sezione relativa all'origine che stai utilizzando.

AWS DMS tipo di dati	Tipo di dati Oracle
BOOLEAN	NUMBER (1)
BYTES	RAW (lunghezza)
DATE	DATETIME
TIME	TIMESTAMP (0)
DATETIME	TIMESTAMP (dimensionamento)
INT1	NUMBER (3)
INT2	NUMBER (5)
INT4	NUMBER (10)
INT8	NUMBER (19)
NUMERIC	NUMBER (p,s)
REAL4	FLOAT
REAL8	FLOAT
STRING	<p>Con indicazione di data: DATE</p> <p>Con indicazione di ora: TIMESTAMP</p> <p>Con indicazione di timestamp: TIMESTAMP</p> <p>Con indicazione timestamp_with_timezone: TIMESTAMP WITH TIMEZONE</p> <p>Con indicazione timestamp_with_local_timezone: TIMESTAMP WITH LOCAL TIMEZONE</p> <p>Con indicazione interval_year_to_month: INTERVAL YEAR TO MONTH</p> <p>Con indicazione interval_day_to_second: INTERVAL DAY TO SECOND</p>

AWS DMS tipo di dati	Tipo di dati Oracle
	<p>Se la lunghezza è > 4000: CLOB</p> <p>In all other cases: VARCHAR2 (lunghezza)</p>
UINT1	NUMBER (3)
UINT2	NUMBER (5)
UINT4	NUMBER (10)
UINT8	NUMBER (19)
WSTRING	<p>Se la lunghezza è > 2000: NCLOB</p> <p>In tutti gli altri casi: NVARCHAR2 (lunghezza)</p>
BLOB	<p>BLOB</p> <p>Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei BLOB per un'attività specifica. I tipi di dati BLOB sono supportati solo nelle tabelle che includono una chiave primaria</p>
CLOB	<p>CLOB</p> <p>Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso dei CLOB per un'attività specifica. Durante il Change Data Capture (CDC), i tipi di dati CLOB sono supportati solo nelle tabelle che includono una chiave primaria.</p> <p>STRING</p> <p>Un tipo di dati Oracle VARCHAR2 sull'origine con una dimensione dichiarata superiore a 4000 byte viene mappato tramite AWS DMS CLOB a una STRING sulla destinazione Oracle.</p>

AWS DMS tipo di dati	Tipo di dati Oracle
NCLOB	<p data-bbox="544 226 656 258">NCLOB</p> <p data-bbox="544 310 1477 485">Per utilizzare questo tipo di dati con AWS DMS, è necessario abilitare l'uso di NCLOBs per un'attività specifica. Durante il CDC, i tipi di dati NCLOB sono supportati solo nelle tabelle che includono una chiave primaria.</p> <p data-bbox="544 531 695 562">WSTRING</p> <p data-bbox="544 611 1485 737">Un tipo di dati Oracle VARCHAR2 sull'origine con una dimensione dichiarata superiore a 4000 byte viene mappato tramite AWS DMS NCLOB a un WSTRING sulla destinazione Oracle.</p>
XMLTYPE	<p data-bbox="544 785 1485 869">Il tipo di dati di destinazione XMLTYPE è rilevante solo in attività di replica da Oracle a Oracle.</p> <p data-bbox="544 915 1474 1089">Quando il database di origine è Oracle, i tipi di dati di origine vengono replicati così come sono sulla destinazione di Oracle. Ad esempio, un tipo di dati XMLTYPE sull'origine viene creato come tipo di dati XMLTYPE sulla destinazione.</p>

Utilizzo di un database Microsoft SQL Server come destinazione per AWS Database Migration Service

Puoi eseguire la migrazione dei dati ai database Microsoft SQL Server mediante AWS DMS. Con un database SQL Server come destinazione, puoi eseguire la migrazione dei dati da un altro database SQL Server o da uno degli altri database supportati.

Per informazioni sulle versioni di SQL Server supportate da AWS DMS come destinazione, consulta [Obiettivi per AWS DMS](#).

AWS DMS supporta le edizioni di Amazon RDS on-premise ed Enterprise, Standard, Workgroup e Developer.

Per ulteriori dettagli sull'utilizzo dei database di destinazione SQL Server e AWS DMS, consulta [quanto segue](#).

Argomenti

- [Limitazioni relative all'utilizzo di SQL Server come destinazione per AWS Database Migration Service](#)
- [Requisiti di sicurezza quando si utilizza SQL Server come destinazione per AWS Database Migration Service](#)
- [Impostazioni degli endpoint quando si utilizza SQL Server come destinazione per AWS DMS](#)
- [Tipi di dati di destinazione per Microsoft SQL Server](#)

Limitazioni relative all'utilizzo di SQL Server come destinazione per AWS Database Migration Service

Quando si utilizza un database SQL Server come destinazione per AWS DMS, si applicano le seguenti limitazioni:

- Quando crei manualmente una tabella di destinazione di SQL Server con una colonna calcolata, la replica del caricamento completo non è supportata se utilizzi l'utilità di copia bulk BCP. Per utilizzare la replica di pieno carico, disabilita il caricamento BCP impostando l'attributo aggiuntivo di connessione 'useBCPFullLoad=false' sull'endpoint. Per informazioni sulla configurazione degli attributi aggiuntivi di connessione sugli endpoint, consulta [Creazione di endpoint di origine e destinazione](#). Per ulteriori informazioni sull'utilizzo di BCP, consulta la [documentazione di Microsoft SQL Server](#).
- Quando si esegue la replica di tabelle con tipi di dati spaziali SQL Server (GEOMETRY e GEOGRAPHY), AWS DMS sostituisce qualsiasi identificatore di riferimento spaziale (SRID, Spatial Reference Identifier) inserito con il valore SRID predefinito. Il valore SRID predefinito è 0 per GEOMETRY e 4326 per GEOGRAPHY.
- Le tabelle temporali non sono supportate. La migrazione di tabelle temporali può funzionare con un'attività di sola replica in modalità di applicazione transazionale se tali tabelle sono create manualmente sulla destinazione.
- Attualmente, i tipi di dati boolean in un'origine PostgreSQL vengono migrati a una destinazione SQLServer come tipo di dati bit con valori incoerenti.

Per ovviare, esegui le seguenti operazioni:

- Crea in anticipo la tabella con un tipo di dati VARCHAR(1) per la colonna (o lascia che sia AWS DMS a creare la tabella). Quindi fai in modo che l'elaborazione a valle tratti una «F» come False e una «T» come True.

- Per evitare di dover cambiare l'elaborazione a valle, aggiungi una regola di trasformazione all'attività per modificare i valori "F" in "0" e i valori "T" in "1" e memorizzali come tipo di dati bit di SQL Server.
- AWS DMS non supporta l'elaborazione delle modifiche per impostare l'annullabilità delle colonne (tramite la clausola ALTER COLUMN [SET|DROP] NOT NULL nelle istruzioni ALTER TABLE).
- L'autenticazione Windows non è supportata.

Requisiti di sicurezza quando si utilizza SQL Server come destinazione per AWS Database Migration Service

Di seguito sono descritti i requisiti di sicurezza per l'utilizzo di AWS DMS con una destinazione di Microsoft SQL Server:

- L'account utente AWS DMS deve disporre almeno del ruolo utente db_owner nel database SQL Server a cui si effettua la connessione.
- Un amministratore di sistema di SQL Server deve fornire questa autorizzazione a tutti gli account utente AWS DMS.

Impostazioni degli endpoint quando si utilizza SQL Server come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione SQL Server in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando create-endpoint nella [AWS CLI](#), con la sintassi JSON --microsoft-sql-server-settings '{"EndpointSetting": "value", ...}'.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con SQL Server come destinazione.

Nome	Description
ControlTablesFileGroup	Specificare un gruppo di file per le tabelle interne di AWS DMS. Quando l'attività di replica viene avviata, tutte le tabelle di controllo interne di AWS DMS (awsdms_

Nome	Description
	<p>apply_exception, awsdms_apply, awsdms_changes) vengono create sul gruppo di file specificato.</p> <p>Valore predefinito: n/d</p> <p>Valori validi: stringa</p> <p>Esempio: --microsoft-sql-server-settings '{"ControlTablesFileGroup": "filegroup1"}'</p> <p>Di seguito è riportato un esempio di un comando per la creazione di un gruppo di file.</p> <pre data-bbox="690 793 1507 1388">ALTER DATABASE replicate ADD FILEGROUP Test1FG1; GO ALTER DATABASE replicate ADD FILE (NAME = test1dat5, FILENAME = 'C:\temp\DATA\t1dat5.ndf', SIZE = 5MB, MAXSIZE = 100MB, FILEGROWTH = 5MB) TO FILEGROUP Test1FG1; GO</pre>
ExecuteTimeout	<p>Utilizza questo attributo aggiuntivo di connessione per impostare il timeout in secondi dell'istruzione client per l'istanza SQL Server. Il valore predefinito è 60 secondi.</p> <p>Esempio: '{"ExecuteTimeout": 100}'</p>

Nome	Description
UseBCPFullLoad	<p>Usale per attribuire i dati di trasferimento per le operazioni di pieno carico utilizzando BCP. Quando la tabella di destinazione contiene una colonna di identità che non esiste nella tabella di origine, è necessario disabilitare l'opzione Utilizza BCP per il caricamento della tabella.</p> <p>Valore predefinito: true</p> <p>Valori validi: true/false</p> <p>Esempio: <code>--microsoft-sql-server-settings '{"UseBCPFullLoad": false}'</code></p>

Tipi di dati di destinazione per Microsoft SQL Server

La tabella seguente mostra i tipi di dati di destinazione di Microsoft SQL Server supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati AWS DMS. Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipo di dati AWS DMS	Tipo di dati SQL Server
BOOLEAN	TINYINT
BYTES	VARBINARY (lunghezza)
DATE	<p>Per SQL Server 2008 e versioni successive, utilizza DATE.</p> <p>Per le versioni precedenti, se il dimensionamento è pari o inferiore a 3, utilizzare DATETIME. In tutti gli altri casi, utilizzare VARCHAR (37).</p>
TIME	Per SQL Server 2008 e versioni successive, utilizza DATETIME2 (%d).

Tipo di dati AWS DMS	Tipo di dati SQL Server
	Per le versioni precedenti, se il dimensionamento è pari o inferiore a 3, utilizzare DATETIME. In tutti gli altri casi, utilizzare VARCHAR (37).
DATETIME	<p>Per SQL Server 2008 e versioni successive, utilizza DATETIME2 (dimensionamento).</p> <p>Per le versioni precedenti, se il dimensionamento è pari o inferiore a 3, utilizzare DATETIME. In tutti gli altri casi, utilizzare VARCHAR (37).</p>
INT1	SMALLINT
INT2	SMALLINT
INT4	INT
INT8	BIGINT
NUMERIC	NUMERIC (p,s)
REAL4	REAL
REAL8	FLOAT
STRING	<p>Se la colonna è di ora o data, effettuare le seguenti operazioni:</p> <ul style="list-style-type: none"> • Per SQL Server 2008 e versioni successive, utilizza DATETIME2. • Per le versioni precedenti, se il dimensionamento è pari o inferiore a 3, utilizzare DATETIME. In tutti gli altri casi, utilizzare VARCHAR (37). <p>Se la colonna non è di ora o data, utilizzare VARCHAR (lunghezza).</p>
UINT1	TINYINT
UINT2	SMALLINT

Tipo di dati AWS DMS	Tipo di dati SQL Server
UINT4	INT
UINT8	BIGINT
WSTRING	NVARCHAR (lunghezza)
BLOB	<p>VARBINARY(max)</p> <p>IMAGE</p> <p>Per utilizzare questo tipo di dati con AWS DMS, devi abilitare l'utilizzo dei BLOB per un'attività specifica. AWS DMS supporta i tipi di dati BLOB solo nelle tabelle che includono una chiave primaria.</p>
CLOB	<p>VARCHAR(max)</p> <p>Per utilizzare questo tipo di dati con AWS DMS, devi abilitare l'utilizzo di CLOB per un'attività specifica. Durante il Change Data Capture (CDC), AWS DMS supporta i tipi di dati CLOB solo nelle tabelle che includono una chiave primaria.</p>
NCLOB	<p>NVARCHAR(max)</p> <p>Per utilizzare questo tipo di dati con AWS DMS, devi abilitare l'utilizzo di NCLOB per un'attività specifica. Durante il CDC, AWS DMS supporta i tipi di dati NCLOB solo nelle tabelle che includono una chiave primaria.</p>

Utilizzo di un database PostgreSQL come destinazione per AWS Database Migration Service

È possibile migrare i dati ai database PostgreSQL utilizzando AWS DMS, da un altro database PostgreSQL o da uno degli altri database supportati.

Per informazioni sulle versioni di PostgreSQL supportate come destinazione, AWS DMS consulta.

[Obiettivi per AWS DMS](#)

Note

- Amazon Aurora Serverless è disponibile come destinazione per Amazon Aurora con compatibilità PostgreSQL. Per ulteriori informazioni su Amazon Aurora Serverless, consulta Using [Amazon Aurora Serverless v2 nella Amazon Aurora User Guide](#).
- I cluster di database Aurora serverless possono essere utilizzati solo da un Amazon VPC e non possono usare un [indirizzo IP pubblico](#). Quindi, se l'istanza di replica è in una regione diversa da quella di Aurora PostgreSQL serverless, devi configurare il [peering vpc](#). In alternativa, verifica la disponibilità delle [regioni](#) Aurora PostgreSQL serverless e decidi di utilizzarne una per Aurora PostgreSQL serverless e per l'istanza di replica.
- La funzionalità Babelfish è integrata in Amazon Aurora senza costi aggiuntivi. Per ulteriori informazioni, consulta [Utilizzo di Babelfish per Aurora PostgreSQL come destinazione per AWS Database Migration Service](#).

AWS DMS adotta un table-by-table approccio per la migrazione dei dati dall'origine alla destinazione nella fase di caricamento completo. L'ordine delle tabelle durante la fase di caricamento completo non può essere garantita. Le tabelle non sono sincronizzate durante la fase di caricamento completo e durante l'applicazione di transazioni memorizzate nella cache per singole tabelle. Di conseguenza, i vincoli di integrità referenziale attivi possono causare un errore dell'attività durante la fase di caricamento completo.

In PostgreSQL, le chiavi esterne (vincoli di integrità referenziale) sono implementate mediante trigger. Durante la fase di pieno caricamento, AWS DMS carica ogni tabella una alla volta. Consigliamo vivamente di disabilitare i vincoli delle chiavi esterne durante un caricamento completo, utilizzando uno dei seguenti metodi:

- Disabilitare temporaneamente tutti i trigger dall'istanza, quindi terminare il caricamento completo.
- Utilizzare il parametro `session_replication_role` in PostgreSQL.

In qualsiasi momento, un trigger può trovarsi in uno dei seguenti stati: `origin`, `replica`, `always` o `disabled`. Quando il parametro `session_replication_role` è impostato su `replica`, solo i trigger nello stato `replica` sono attivi e vengono attivati quando sono chiamati. In caso contrario, i trigger rimangono inattivi.

PostgreSQL dispone di un meccanismo di sicurezza per evitare che una tabella venga troncata, anche quando `session_replication_role` è impostato. Puoi utilizzare tale opzione come alternativa alla disabilitazione dei trigger, per facilitare il completamento dell'esecuzione del caricamento completo. Per eseguire questa operazione, imposta la modalità di preparazione della tabella di destinazione su `D0_NOTHING`. In caso contrario, le operazioni `DROP` e `TRUNCATE` avranno esito negativo in presenza di vincoli delle chiavi esterne.

In Amazon RDS, puoi controllare l'impostazione di questo parametro mediante un gruppo di parametri. Per un'istanza PostgreSQL in esecuzione su Amazon EC2, puoi impostare il parametro direttamente.

Per ulteriori dettagli sull'utilizzo di un database PostgreSQL come destinazione AWS DMS per, consulta le seguenti sezioni:

Argomenti

- [Limitazioni all'uso di PostgreSQL come destinazione per AWS Database Migration Service](#)
- [Requisiti di sicurezza quando si utilizza un database PostgreSQL come destinazione per AWS Database Migration Service](#)
- [Impostazioni degli endpoint e attributi di connessione aggiuntivi \(ECA\) quando si utilizza PostgreSQL come destinazione per AWS DMS](#)
- [Tipi di dati di destinazione per PostgreSQL](#)
- [Usare Babelfish per Aurora PostgreSQL come destinazione per AWS Database Migration Service](#)

Limitazioni all'uso di PostgreSQL come destinazione per AWS Database Migration Service

Quando si utilizza un database PostgreSQL come destinazione per AWS DMS, si applicano le seguenti limitazioni:

- Per le migrazioni eterogenee, il tipo di dati JSON viene convertito internamente nel tipo di dati CLOB nativo.
- In una migrazione da Oracle a PostgreSQL, se una colonna in Oracle contiene un carattere NULL (valore esadecimale `U+0000`), converte il carattere NULL in uno spazio (valore esadecimale `U+0020`) AWS DMS. Ciò si verifica a causa di una limitazione di PostgreSQL.
- AWS DMS non supporta la replica su una tabella con un indice univoco creato con la funzione `coalesce`.

- Se le tabelle utilizzano sequenze, aggiorna il valore di NEXTVAL per ogni sequenza nel database di destinazione dopo aver interrotto la replica dal database di origine. AWS DMS copia i dati dal database di origine, ma non migra le sequenze verso il target durante la replica in corso.

Requisiti di sicurezza quando si utilizza un database PostgreSQL come destinazione per AWS Database Migration Service

Per motivi di sicurezza, l'account utente utilizzato per la migrazione dei dati deve corrispondere a un utente registrato in qualsiasi database PostgreSQL utilizzato come destinazione.

L'endpoint di destinazione PostgreSQL richiede autorizzazioni utente minime per eseguire AWS DMS una migrazione, vedi gli esempi seguenti.

```
CREATE USER newuser WITH PASSWORD 'your-password';
ALTER SCHEMA schema_name OWNER TO newuser;
```

Oppure

```
GRANT USAGE ON SCHEMA schema_name TO myuser;
GRANT CONNECT ON DATABASE postgres TO myuser;
GRANT CREATE ON DATABASE postgres TO myuser;
GRANT CREATE ON SCHEMA schema_name TO myuser;
GRANT UPDATE, INSERT, SELECT, DELETE, TRUNCATE ON ALL TABLES IN SCHEMA schema_name
TO myuser;
GRANT TRUNCATE ON schema_name."BasicFeed" TO myuser;
```

Impostazioni degli endpoint e attributi di connessione aggiuntivi (ECA) quando si utilizza PostgreSQL come destinazione per AWS DMS


È possibile utilizzare le impostazioni degli endpoint e gli attributi di connessione aggiuntivi (ECA) per configurare il database di destinazione PostgreSQL.

Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in, con la sintassi JSON. [AWS CLI](#) -- `postgres-sql-settings '{"EndpointSetting": "value", ...}'`

È possibile specificare le ECA utilizzando il `ExtraConnectionAttributes` parametro per l'endpoint.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con PostgreSQL come destinazione.

Nome	Descrizione
<code>MaxFileSize</code>	<p>Specifica le dimensioni massime (in KB) di qualsiasi file .csv utilizzato per il trasferimento dei dati su PostgreSQL.</p> <p>Valore predefinito: 32.768 KB (32 MB)</p> <p>Valori validi: 1-1.048.576 KB (fino a 1,1 GB)</p> <p>Esempio: <code>--postgres-sql-settings '{"MaxFileSize": 512}'</code></p>
<code>ExecuteTimeout</code>	<p>Imposta il timeout dell'istruzione del client per l'istanza PostgreSQL in secondi. Il valore predefinito è 60 secondi.</p> <p>Esempio: <code>--postgres-sql-settings '{"ExecuteTimeout": 100}'</code></p>
<code>AfterConnectScript= SET session_replication_role = replica</code>	<p>Questo attributo AWS DMS ignora le chiavi esterne e i trigger utente per ridurre il tempo necessario per caricare in blocco i dati.</p>
<code>MapUnboundedNumericAsString</code>	<p>Questo parametro tratta le colonne con tipi di dati NUMERIC illimitati come STRING per eseguire correttamente la migrazione senza perdere la precisione del valore numerico. Usa questo parametro solo per la replica dall'origine PostgreSQL alla destinazione PostgreSQL o ai database con compatibilità PostgreSQL.</p> <p>Valore predefinito: false</p> <p>Valori validi: false/true</p>

Nome	Descrizione
	<p>Esempio: <code>--postgresql-settings '{"MapUnboundedNumericAsString": "true"}</code></p> <p>L'utilizzo di questo parametro può comportare un peggioramento delle prestazioni di replica a causa della trasformazione da valore numerico a stringa e di nuovo a valore numerico. Questo parametro è supportato per l'uso da DMS versione 3.4.4 e successive</p> <div data-bbox="688 604 1507 1255" style="border: 1px solid #ccc; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note</p> <p>Utilizza <code>MapUnboundedNumericAsString</code> solo negli endpoint di origine e di destinazione PostgreSQL insieme.</p> <p>L'uso di <code>MapUnboundedNumericAsString</code> su endpoint PostgreSQL di origine limita la precisione a 28 durante la CDC. L'uso di <code>MapUnboundedNumericAsString</code> su endpoint di destinazione, migra i dati con precisione 28 scala 6.</p> <p>Non utilizzare <code>MapUnboundedNumericAsString</code> con destinazioni non PostgreSQL.</p> </div>
loadUsingCSV	<p>Utilizzate questo attributo di connessione aggiuntivo (ECA) per trasferire i dati per le operazioni di caricamento completo utilizzando il comando <code>\COPY</code>.</p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>true/false</code></p> <p>Esempio ECA: <code>loadUsingCSV=true;</code></p> <p>Nota: l'impostazione di questo ECA su <code>false</code> potrebbe comportare un peggioramento delle prestazioni di replica a causa dell'esecuzione diretta degli <code>INSERT</code>.</p>

Nome	Descrizione
DatabaseMode	<p>Utilizza questo attributo per modificare il comportamento predefinito della gestione da parte della replica degli endpoint compatibili con PostgreSQL che richiedono una configurazione aggiuntiva, come gli endpoint Babelfish.</p> <p>Valore predefinito: DEFAULT</p> <p>Valori validi: DEFAULT, BABELFISH</p> <p>Esempio: DatabaseMode=default;</p>
BabelfishDatabaseName	<p>Utilizza questo attributo per specificare il nome del database T-SQL Babelfish di destinazione in cui eseguire la migrazione. Questo è necessario se DatabaseMode è impostato su Babelfish . Questo non è il database babelfish_db riservato.</p> <p>Esempio: BabelfishDatabaseName=TargetDb;</p>

Tipi di dati di destinazione per PostgreSQL

L'endpoint del database PostgreSQL per AWS DMS supporta la maggior parte dei tipi di dati del database PostgreSQL. La tabella seguente mostra i tipi di dati di destinazione del database PostgreSQL supportati durante l' AWS DMS utilizzo e la mappatura predefinita dei tipi di dati. AWS DMS

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere. [Tipi di dati per AWS Database Migration Service](#)

AWS DMS tipo di dati	Tipo di dati PostgreSQL
BOOLEAN	BOOLEAN
BLOB	BYTEA
BYTES	BYTEA

AWS DMS tipo di dati	Tipo di dati PostgreSQL
DATE	DATE
TIME	TIME
DATETIME	<p>Se il dimensionamento è compreso tra 0 e 6, utilizzare TIMESTAMP .</p> <p>Se il dimensionamento è compreso tra 7 e 9, utilizzare VARCHAR (37).</p>
INT1	SMALLINT
INT2	SMALLINT
INT4	INTEGER
INT8	BIGINT
NUMERIC	DECIMAL (P,S)
REAL4	FLOAT4
REAL8	FLOAT8
STRING	<p>Se la lunghezza è compresa tra 1 e 21.845, utilizzare VARCHAR (lunghezza in byte).</p> <p>Se la lunghezza è compresa tra 21.846 e 2.147.483.647, utilizzare VARCHAR (65535).</p>
UINT1	SMALLINT
UINT2	INTEGER
UINT4	BIGINT
UINT8	BIGINT

AWS DMS tipo di dati	Tipo di dati PostgreSQL
WSTRING	Se la lunghezza è compresa tra 1 e 21.845, utilizzare VARCHAR (lunghezza in byte). Se la lunghezza è compresa tra 21.846 e 2.147.483.647, utilizzare VARCHAR (65535).
NCLOB	TEXT
CLOB	TEXT

Note

Quando si esegue la replica da un'origine PostgreSQL AWS DMS, crea la tabella di destinazione con gli stessi tipi di dati per tutte le colonne, ad eccezione delle colonne con tipi di dati definiti dall'utente. In questi casi, il tipo di dati viene creato come "carattere variabile" nella destinazione.

Usare Babelfish per Aurora PostgreSQL come destinazione per AWS Database Migration Service

È possibile migrare le tabelle di origine SQL Server in una destinazione Babelfish per Amazon Aurora PostgreSQL mediante AWS Database Migration Service. Con Babelfish, Aurora PostgreSQL comprende T-SQL, il linguaggio SQL di proprietà di Microsoft SQL Server, e supporta lo stesso protocollo di comunicazione. Pertanto, le applicazioni scritte per SQL Server possono ora funzionare con Aurora con meno modifiche al codice. La funzionalità Babelfish è integrata in Amazon Aurora senza costi aggiuntivi. Puoi attivare Babelfish sul tuo cluster Amazon Aurora dalla console Amazon RDS.

Quando crei l'endpoint di AWS DMS destinazione utilizzando la AWS DMS console, l'API o i comandi CLI, specifica il motore di destinazione Amazon Aurora PostgreSQL e assegna un nome al database `babelfish_db`. Nella sezione Impostazione dell'endpoint aggiungi le impostazioni per configurare `DatabaseMode` su `Babelfish` e `BabelfishDatabaseName` sul nome del database T-SQL Babelfish di destinazione.

Aggiunta delle regole di trasformazione all'attività di migrazione

Quando definisci un'attività di migrazione per una destinazione Babelfish, è necessario includere le regole di trasformazione che assicurino che DMS utilizzi le tabelle T-SQL Babelfish già create nel database di destinazione.

Innanzitutto, aggiungi all'attività di migrazione una regola di trasformazione che renda tutti i nomi delle tabelle in minuscolo. Babelfish memorizza i nomi delle tabelle create utilizzando T-SQL in lettere minuscole nel catalogo `pg_class` PostgreSQL. Tuttavia, quando le tabelle SQL Server includono nomi in maiuscolo e minuscolo, DMS crea le tabelle utilizzando i tipi di dati nativi PostgreSQL anziché i tipi di dati compatibili con T-SQL. Per questo motivo, assicurati di aggiungere una regola di trasformazione che renda tutti i nomi delle tabelle in minuscolo. I nomi delle colonne non devono essere trasformati in lettere minuscole.

Successivamente, se hai utilizzato la modalità di migrazione di più database quando hai definito il cluster, aggiungi una regola di trasformazione che rinomina lo schema SQL Server originale. Assicurati di rinominare il nome dello schema SQL Server per includere il nome del database T-SQL. Ad esempio, se il nome dello schema SQL Server originale è `dbo` e il nome del database T-SQL è `mydb`, rinomina lo schema in `mydb_dbo` utilizzando una regola di trasformazione.

Se usi la modalità di un database singolo, non è necessaria una regola di trasformazione per rinominare i nomi degli schemi. I nomi degli schemi hanno una mappatura con il database T-SQL di destinazione in Babelfish. one-to-one

La seguente regola di trasformazione di esempio rende tutti i nomi delle tabelle in minuscolo e rinomina il nome dello schema SQL Server originale da `dbo` in `mydb_dbo`.

```
{
  "rules": [
    {
      "rule-type": "transformation",
      "rule-id": "566251737",
      "rule-name": "566251737",
      "rule-target": "schema",
      "object-locator": {
        "schema-name": "dbo"
      },
      "rule-action": "rename",
      "value": "mydb_dbo",
      "old-value": null
    }
  ]
}
```

```
},
{
  "rule-type": "transformation",
  "rule-id": "566139410",
  "rule-name": "566139410",
  "rule-target": "table",
  "object-locator": {
    "schema-name": "%",
    "table-name": "%"
  },
  "rule-action": "convert-lowercase",
  "value": null,
  "old-value": null
},
{
  "rule-type": "selection",
  "rule-id": "566111704",
  "rule-name": "566111704",
  "object-locator": {
    "schema-name": "dbo",
    "table-name": "%"
  },
  "rule-action": "include",
  "filters": []
}
]
}
```

Limitazioni all'utilizzo di un endpoint di destinazione PostgreSQL con le tabelle Babelfish

Le seguenti limitazioni si applicano quando si utilizza un endpoint di destinazione PostgreSQL con tabelle Babelfish:

- Per Modalità di preparazione della tabella di destinazione usa solo le modalità Nessuna operazione o Tronca. Non utilizzare la modalità Rilascia tabelle nella destinazione. In questa modalità, DMS crea le tabelle come tabelle PostgreSQL che T-SQL potrebbe non riconoscere.
- AWS DMS non supporta il tipo di dati `sql_variant`.
- Babelfish non supporta i tipi di dati `HEIRARCHYID`, `GEOMETRY` e `GEOGRAPHY`. Per migrare questi tipi di dati, puoi aggiungere le regole di trasformazione per cui convertire il tipo di dati in `wstring(250)`.

- Babelfish supporta solo la migrazione di tipi di dati BINARY, VARBINARY e IMAGE che utilizzano il tipo di dati BYTEA. Per le versioni precedenti di Aurora PostgreSQL, puoi utilizzare DMS per migrare queste tabelle su un [endpoint di destinazione Babelfish](#). Non è necessario specificare la lunghezza per il tipo di dati BYTEA, come mostrato nell'esempio seguente.

```
[Picture] [VARBINARY](max) NULL
```

Modifica il tipo di dati T-SQL precedente con il tipo di dati BYTEA supportato da T-SQL.

```
[Picture] BYTEA NULL
```

- Per le versioni precedenti di Aurora PostgreSQL Babelfish, se si crea un'attività di migrazione per la replica continua da SQL Server a Babelfish utilizzando l'endpoint di destinazione PostgreSQL, è necessario assegnare il tipo di dati SERIAL a tutte le tabelle che utilizzano colonne IDENTITY. A partire da Aurora PostgreSQL (versione 15.3/14.8 e successive) e Babelfish (versione 3.2.0 e successive), la colonna identity è supportata e non è più necessario assegnare il tipo di dati SERIAL. Per ulteriori informazioni, consulta [SERIAL Usage](#) nella sezione Sequences and Identity in SQL Server to Aurora PostgreSQL Migration Playbook. Quindi, quando crei la tabella in Babelfish, modifica la definizione della colonna come segue.

```
[IDCo1] [INT] IDENTITY(1,1) NOT NULL PRIMARY KEY
```

Cambia la definizione precedente come segue.

```
[IDCo1] SERIAL PRIMARY KEY
```

Aurora PostgreSQL compatibile con Babelfish crea una sequenza utilizzando la configurazione predefinita e aggiunge un vincolo NOT NULL alla colonna. La sequenza appena creata si comporta come una sequenza normale (con incrementi di 1) e non include alcuna opzione SERIAL composita.

- Dopo aver migrato i dati di tabelle con le colonne IDENTITY o il tipo di dati SERIAL, reimposta l'oggetto sequenza basato su PostgreSQL in base al valore massimo per la colonna. Dopo aver eseguito il pieno carico delle tabelle, usa la seguente query T-SQL per generare le istruzioni per inizializzare l'oggetto sequenza associato.

```
DECLARE @schema_prefix NVARCHAR(200) = ''
```



```

IF current_setting('babelfishpg_tsql.migration_mode') = 'multi-db'
    SET @schema_prefix = db_name() + '_'

SELECT 'SELECT setval(pg_get_serial_sequence('' + @schema_prefix +
    schema_name.tables.schema_id) + '.' + tables.name + '', '' + columns.name + '')
    ,(select max(' + columns.name + ') from ' +
    schema_name.tables.schema_id) + '.' + tables.name + ');'
FROM sys.tables tables
JOIN sys.columns columns ON tables.object_id = columns.object_id
WHERE columns.is_identity = 1

UNION ALL

SELECT 'SELECT setval(pg_get_serial_sequence('' + @schema_prefix + table_schema +
    '.' + table_name + '',
    '' + column_name + ''),(select max(' + column_name + ') from ' + table_schema + '.'
    + table_name + '));'
FROM information_schema.columns
WHERE column_default LIKE 'nextval(%;

```

La query genera una serie di istruzioni SELECT da eseguire in ordine per aggiornare i valori massimi di IDENTITY e SERIAL.

- Per le versioni di Babelfish precedenti alla 3.2, la Modalità LOB completa potrebbe causare un errore di tabella. In tal caso, crea un'attività separata per le tabelle che non sono state caricate. Utilizza quindi la Modalità LOB limitata per specificare il valore appropriato per Dimensione massima dei LOB (KB). Un'altra opzione consiste nell'impostare l'attributo di connessione dell'endpoint ForceFullLob=True di SQL Server.
- Per le versioni di Babelfish precedenti alla 3.2, l'esecuzione della convalida dei dati per tabelle Babelfish che non utilizzano chiavi primarie basate su numeri interi genera un messaggio che indica che non è possibile trovare una chiave univoca adatta. A partire da Aurora PostgreSQL (versione 15.3/14.8 e successive) e Babelfish (versione 3.2.0 e successive), è supportata la convalida dei dati per chiavi primarie basate su numeri non interi.
- A causa delle differenze di precisione nel numero di cifre decimali per i secondi, DMS segnala gli errori di convalida dei dati per le tabelle Babelfish che utilizzano tipi di dati DATETIME. Per correggere questi errori, puoi aggiungere il seguente tipo di regola di convalida per i tipi di dati DATETIME.

```

{
    "rule-type": "validation",

```

```
"rule-id": "3",
"rule-name": "3",
"rule-target": "column",
"object-locator": {
  "schema-name": "dbo",
  "table-name": "%",
  "column-name": "%",
  "data-type": "datetime"
},
"rule-action": "override-validation-function",
"source-function": "case when ${column-name} is NULL then NULL else 0 end",
"target-function": "case when ${column-name} is NULL then NULL else 0 end"
}
```

Utilizzo di un database compatibile con MySQL come destinazione per AWS Database Migration Service

È possibile migrare i dati su qualsiasi database compatibile con MySQL utilizzando uno qualsiasi dei AWS DMS motori di dati di origine supportati. AWS DMS Se si esegue la migrazione a un database locale compatibile con MySQL, è AWS DMS necessario che il motore di origine risieda all'interno dell'ecosistema. AWS Il motore può essere su un servizio AWS gestito come Amazon RDS, Amazon Aurora o Amazon S3. In alternativa, il motore può trovarsi su un database autogestito in Amazon EC2.

Puoi utilizzare il protocollo SSL per crittografare le connessioni tra l'endpoint compatibile con MySQL e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint compatibile con MySQL, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Per informazioni sulle versioni di MySQL supportate come AWS DMS destinazione, vedere. [Obiettivi per AWS DMS](#)

È possibile utilizzare i seguenti database compatibili con MySQL come destinazioni per: AWS DMS

- MySQL Community Edition
- MySQL Standard Edition
- MySQL Enterprise Edition
- MySQL Cluster Carrier Grade Edition
- MariaDB Community Edition

- MariaDB Enterprise Edition
- MariaDB Column Store
- Amazon Aurora MySQL

Note

Indipendentemente dal motore di storage di origine (MyISAM, MEMORY e così via), AWS DMS crea una tabella di destinazione compatibile con MySQL come tabella InnoDB per impostazione predefinita.

Se ti occorre una tabella che utilizza un motore di storage diverso da InnoDB, puoi creare manualmente la tabella sulla destinazione compatibile con MySQL e migrare la tabella utilizzando l'opzione Nessuna azione. Per ulteriori informazioni, consulta [Impostazioni delle attività di caricamento completo](#).

Per ulteriori dettagli sull'utilizzo di un database compatibile con MySQL come destinazione per AWS DMS, consulta le sezioni seguenti.

Argomenti

- [Utilizzo di qualsiasi database compatibile con MySQL come destinazione per AWS Database Migration Service](#)
- [Limitazioni all'utilizzo di un database compatibile con MySQL come destinazione per AWS Database Migration Service](#)
- [Impostazioni degli endpoint quando si utilizza un database compatibile con MySQL come destinazione per AWS DMS](#)
- [Tipi di dati di destinazione per MySQL](#)

Utilizzo di qualsiasi database compatibile con MySQL come destinazione per AWS Database Migration Service

Prima di iniziare a utilizzare un database compatibile con MySQL come destinazione per AWS DMS, accertati di aver soddisfatto i seguenti prerequisiti:

- Fornisci un account utente con AWS DMS privilegi di lettura/scrittura per il database compatibile con MySQL. Per creare i privilegi necessari, esegui i seguenti comandi.

```
CREATE USER '<user acct>'@'%' IDENTIFIED BY '<user password>';
GRANT ALTER, CREATE, DROP, INDEX, INSERT, UPDATE, DELETE, SELECT ON <schema>.* TO
'<user acct>'@'%' ;
GRANT ALL PRIVILEGES ON awsdms_control.* TO '<user acct>'@'%' ;
```

- Durante la fase di migrazione del caricamento completo, devi disabilitare le chiavi esterne sulle tabelle di destinazione. Per disabilitare i controlli delle chiavi esterne su un database compatibile con MySQL durante un caricamento completo, puoi aggiungere il seguente comando alla sezione Attributi di connessione aggiuntivi della AWS DMS console per l'endpoint di destinazione.

```
Initstmt=SET FOREIGN_KEY_CHECKS=0;
```

- Imposta il parametro del database `local_infile = 1` per consentire a AWS DMS di caricare i dati nel database di destinazione.

Limitazioni all'utilizzo di un database compatibile con MySQL come destinazione per AWS Database Migration Service

Quando si utilizza un database MySQL come destinazione AWS DMS , non supporta quanto segue:

- Le istruzioni DDL (Data Definition Language) TRUNCATE PARTITION, DROP TABLE e RENAME TABLE.
- L'utilizzo di un'istruzione ALTER TABLE *table_name* ADD COLUMN *column_name* per aggiungere colonne all'inizio o al centro di una tabella.
- Quando si caricano dati su una destinazione compatibile con MySQL in un'attività a caricamento completo, AWS DMS non riporta gli errori causati da vincoli nei registri delle attività, che possono causare errori di chiave duplicati o mancate corrispondenze con il numero di record. Questo comportamento è riconducibile al modo in cui MySQL gestisce i dati locali con il comando LOAD DATA. Effettua le seguenti operazioni durante la fase di pieno carico:
 - Disabilita le limitazioni.
 - Utilizza AWS DMS la convalida per assicurarti che i dati siano coerenti.
- Quando si aggiorna il valore di una colonna al valore esistente, i database compatibili con MySQL restituiscono un avviso `0 rows affected`. Sebbene questo comportamento non sia tecnicamente un errore, la situazione è gestita diversamente in altri motori di database. Ad

esempio, Oracle esegue un aggiornamento di una riga. Per i database compatibili con MySQL, AWS DMS genera una voce nella tabella di controllo `awsdms_apply_exceptions` e registra il seguente avviso.

```
Some changes from the source database had no impact when applied to
the target database. See awsdms_apply_exceptions table for details.
```

- Aurora serverless è disponibile come destinazione per Amazon Aurora versione 2, compatibile con MySQL versione 5.7. Seleziona Aurora MySQL versione 2.07.1 per utilizzare Aurora serverless compatibile con MySQL 5.7. Per ulteriori informazioni su Aurora Serverless, consulta Using [Aurora Serverless v2 nella Amazon Aurora User Guide](#).
- AWS DMS non supporta l'utilizzo di un endpoint reader per Aurora o Amazon RDS, a meno che le istanze non siano in modalità scrivibile, `read_only` ovvero i parametri `innodb_read_only` and non siano impostati su o. `0 OFF` Per ulteriori informazioni sull'utilizzo di Amazon RDS e Aurora come destinazioni, consulta gli argomenti seguenti:
 - [Determinazione dell'istanza database a cui si è connessi](#)
 - [Aggiornamento di repliche di lettura con MySQL](#)

Impostazioni degli endpoint quando si utilizza un database compatibile con MySQL come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione compatibile con MySQL in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la AWS DMS console o utilizzando il `create-endpoint` comando in, con la sintassi JSON. [AWS CLI](#) `--my-sql-settings '{"EndpointSetting": "value", ...}'`

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con MySQL come destinazione.

Nome	Descrizione
TargetDbType	Specifica la posizione in cui migrare le tabelle di origine sulla destinazione, su un singolo database o su più

Nome	Descrizione
	<p>database. Se si specifica <code>SPECIFIC_DATABASE</code> , è necessario specificare il nome del database, quando si utilizza il o il AWS CLI . AWS Management Console</p> <p>Valore predefinito: <code>MULTIPLE_DATABASES</code></p> <p>Valori validi: <code>{SPECIFIC_DATABASE , MULTIPLE_DATABASES }</code></p> <p>Esempio: <code>--my-sql-settings '{"TargetDbType": "MULTIPLE_DATABASES"}'</code></p>
<code>ParallelLoadThreads</code>	<p>Migliora le prestazioni durante il caricamento dei dati nel database di destinazione compatibile con MySQL. Specifica il numero di thread da utilizzare per caricare i dati nel database di destinazione compatibile con MySQL. L'impostazione di un numero elevato di thread può avere ripercussioni negative sulle prestazioni del database, perché è necessaria una connessione separata per ciascun thread.</p> <p>Valore predefinito: 1</p> <p>Valori validi: 1-5</p> <p>Esempio: <code>--my-sql-settings '{"ParallelLoadThreads": 1}'</code></p>

Nome	Descrizione
AfterConnectScript	<p>Specifica uno script da eseguire immediatamente dopo la connessione di AWS DMS all'endpoint.</p> <p>Ad esempio, puoi specificare che la destinazione compatibile con MySQL deve convertire le istruzioni ricevute nel set di caratteri latin1, ovvero il set di caratteri compilato predefinito del database. In genere, questo parametro migliora le prestazioni quando si esegue la conversione da client UTF8.</p> <p>Esempio: <code>--my-sql-settings '{"AfterConnectScript": "SET character_set_connection='latin1''}"</code></p>
MaxFileSize	<p>Specifica le dimensioni massime (in KB) di qualsiasi file .csv utilizzato per il trasferimento dei dati su database compatibile con MySQL.</p> <p>Valore predefinito: 32.768 KB (32 MB)</p> <p>Valori validi: 1-1.048.576</p> <p><code>--my-sql-settings '{"MaxFileSize": 512}'</code></p>
CleanSrcMetadataOnMismatch	<p>Esegue la pulizia e crea nuovamente le informazioni dei metadati delle tabelle sull'istanza di replica se si verifica una mancata corrispondenza. Un esempio è una situazione in cui l'esecuzione di un'istruzione di modifica di DDL sulla tabella potrebbe avere come risultato informazioni diverse relative alla tabella memorizzata nella cache nell'istanza di replica. booleano.</p> <p>Valore predefinito: false</p> <p>Esempio: <code>--my-sql-settings '{"CleanSrcMetadataOnMismatch": false}'</code></p>

Puoi anche utilizzare gli attributi aggiuntivi di connessione per configurare il database di destinazione compatibile con MySQL.

Nella seguente tabella vengono indicati gli attributi aggiuntivi di connessione utilizzabili con MySQL come destinazione.

Nome	Descrizione
<code>Initstmt=SET FOREIGN_KEY_CHECKS=0;</code>	<p>Disabilita i controlli delle chiavi esterne.</p> <p>Esempio: <code>--extra-connection-attributes "Initstmt=SET FOREIGN_KEY_CHECKS=0;"</code></p>
<code>Initstmt=SET time_zone</code>	<p>Specifica il fuso orario per il database di destinazione compatibile con MySQL.</p> <p>Valore predefinito: UTC</p> <p>Valori validi: i nomi dei fusi orari disponibili nel database MySQL di destinazione.</p> <p>Esempio: <code>--extra-connection-attributes "Initstmt=SET time_zone= <i>US/Pacific</i> ;"</code></p>

In alternativa, è possibile utilizzare il parametro `AfterConnectScript` del comando `--mysql-settings` per disabilitare i controlli delle chiavi esterne e specificare il fuso orario del database.

Tipi di dati di destinazione per MySQL

La tabella seguente mostra i tipi di dati di destinazione del database MySQL supportati durante l'AWS DMS utilizzo e la AWS DMS mappatura predefinita dei tipi di dati.

Per ulteriori informazioni sui tipi di AWS DMS dati, vedere. [Tipi di dati per AWS Database Migration Service](#)

AWS DMS tipi di dati	Tipi di dati MySQL
BOOLEAN	BOOLEAN

AWS DMS tipi di dati	Tipi di dati MySQL
BYTES	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizzare VARBINARY (lunghezza).</p> <p>Se la lunghezza è compresa tra 65.536 e 2.147.483.647, utilizzare LONGLOB.</p>
DATE	DATE
TIME	TIME
TIMESTAMP	<p>"Se il dimensionamento è => 0 e =< 6, DATETIME (dimensionamento)</p> <p>Se il dimensionamento è => 7 e =< 9, VARCHAR (37)"</p>
INT1	TINYINT
INT2	SMALLINT
INT4	INTEGER
INT8	BIGINT
NUMERIC	DECIMAL (p,s)
REAL4	FLOAT
REAL8	DOUBLE PRECISION
STRING	<p>Se la lunghezza è compresa tra 1 e 21.845, utilizzare VARCHAR (lunghezza).</p> <p>Se la lunghezza è compresa tra 21.846 e 2.147.483.647, utilizzare LONGTEXT.</p>
UINT1	UNSIGNED TINYINT
UINT2	UNSIGNED SMALLINT

AWS DMS tipi di dati	Tipi di dati MySQL
UINT4	UNSIGNED INTEGER
UINT8	UNSIGNED BIGINT
WSTRING	<p>Se la lunghezza è compresa tra 1 e 32.767, utilizzare VARCHAR (lunghezza).</p> <p>Se la lunghezza è compresa tra 32.768 e 2.147.483.647, utilizzare LONGTEXT.</p>
BLOB	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizzare BLOB.</p> <p>Se la lunghezza è compresa tra 65.536 e 2.147.483.647, utilizzare LONGBLOB.</p> <p>Se la lunghezza è 0, utilizzare LONGBLOB (supporto LOB completo).</p>
NCLOB	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizzare TEXT.</p> <p>Se la lunghezza è compresa tra 65.536 a 2.147.483.647, utilizzare LONGTEXT con ucs2 per CHARACTER SET.</p> <p>Se la lunghezza è 0, utilizzare LONGTEXT (supporto LOB completo) con ucs2 per CHARACTER SET.</p>
CLOB	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizzare TEXT.</p> <p>Se la lunghezza è compresa tra 65.536 e 2147483647, utilizzare LONGTEXT.</p> <p>Se la lunghezza è 0, utilizzare LONGTEXT (supporto LOB completo).</p>

Utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service

Puoi migrare i dati nei database Amazon Redshift utilizzando AWS Database Migration Service. Amazon Redshift è un servizio di data warehouse nel cloud in scala petabyte interamente gestito. Con un database Amazon Redshift come destinazione, puoi eseguire la migrazione dei dati da tutti gli altri database di origine supportati.

Puoi utilizzare Amazon Redshift serverless come destinazione per AWS DMS. Per ulteriori informazioni, consulta la sezione seguente: [Utilizzo di AWS DMS con Amazon Redshift serverless come destinazione](#).

Il cluster Amazon Redshift deve trovarsi nello stesso account AWS e nella stessa regione AWS dell'istanza di replica.

Durante la migrazione di un database a Amazon Redshift, AWS DMS sposta innanzitutto i dati in un bucket Amazon S3. Quando i file risiedono in un bucket Amazon S3, AWS DMS li trasferisce alle tabelle appropriate nel data warehouse Amazon Redshift. AWS DMS crea il bucket S3 nella stessa regione AWS del database Amazon Redshift. L'istanza di replica AWS DMS deve trovarsi in quella stessa regione AWS.

Se utilizzi la AWS CLI oppure l'API DMS per eseguire la migrazione dei dati ad Amazon Redshift, devi configurare un ruolo AWS Identity and Access Management (IAM) per consentire l'accesso a S3. Per ulteriori informazioni sulla creazione di questo ruolo IAM, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

L'endpoint Amazon Redshift fornisce l'automazione completa per le operazioni seguenti:

- Generazione dello schema e mappatura dei tipi di dati
- Caricamento completo delle tabelle di database di origine
- Caricamento incrementale delle modifiche apportate alle tabelle di origine
- Applicazione delle modifiche dello schema nel DDL (Data Definition Language) effettuate sulle tabelle di origine
- Sincronizzazione tra il caricamento completo e i processi Change Data Capture (CDC).

AWS Database Migration Service supporta le operazioni di caricamento completo e di elaborazione delle modifiche. AWS DMS legge i dati dal database di origine e crea una serie di file con valori

separati da virgole (.csv). Per le operazioni di pieno carico, AWS DMS crea i file per ciascuna tabella. Quindi, AWS DMS copia i file per ciascuna tabella in una cartella separata in Amazon S3. Quando i file vengono caricati su Amazon S3, AWS DMS invia un comando di copia e i dati nei file vengono copiati in Amazon Redshift. Per le operazioni di elaborazione delle modifiche, AWS DMS copia le modifiche della rete nei file .csv. Quindi, AWS DMS carica i file delle modifiche di rete su Amazon S3 e copia i dati in Amazon Redshift.

Per ulteriori dettagli sull'utilizzo di Amazon Redshift come destinazione per AWS DMS, consulta le seguenti sezioni:

Argomenti

- [Prerequisiti per l'utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service](#)
- [Privilegi richiesti per l'utilizzo di Redshift come destinazione](#)
- [Limitazioni all'utilizzo di Amazon Redshift come destinazione per AWS Database Migration Service](#)
- [Configurazione di un database Amazon Redshift come destinazione per AWS Database Migration Service](#)
- [Utilizzo del routing VPC avanzato con Amazon Redshift come destinazione per AWS Database Migration Service](#)
- [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#)
- [Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS](#)
- [Utilizzo di una chiave di crittografia dei dati e di un bucket Amazon S3 come storage intermedio](#)
- [Impostazioni delle attività multithread per Amazon Redshift](#)
- [Tipi di dati di destinazione per Amazon Redshift.](#)
- [Utilizzo di AWS DMS con Amazon Redshift serverless come destinazione](#)

Prerequisiti per l'utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service

Di seguito sono descritti i prerequisiti necessari per l'utilizzo di Amazon Redshift come destinazione per la migrazione dei dati:

- Utilizza la Console di gestione AWS per avviare un cluster Amazon Redshift. Prendi nota delle informazioni di base sull'account AWS e sul cluster Amazon Redshift, ad esempio la password, il

nome utente e il nome del database. Tali valori sono necessari durante la creazione dell'endpoint di destinazione Amazon Redshift.

- Il cluster Amazon Redshift deve trovarsi nello stesso account AWS e nella stessa regione AWS dell'istanza di replica.
- L'istanza di replica AWS DMS richiede la connettività di rete sull'endpoint Amazon Redshift (nome host e porta) utilizzato dal cluster.
- AWS DMS usa un bucket Amazon S3 per trasferire i dati al database Amazon Redshift. Per consentire a AWS DMS di creare il bucket, la console utilizza un ruolo IAM, `dms-access-for-endpoint`. Se utilizzi la AWS CLI o l'API DMS per creare una migrazione di database con Amazon Redshift come database di destinazione, devi creare questo ruolo IAM. Per ulteriori informazioni sulla creazione di questo ruolo, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).
- AWS DMS converte BLOB, CLOB e NCLOB in un valore VARCHAR nell'istanza di destinazione Amazon Redshift. Amazon Redshift non supporta tipi di dati VARCHAR di dimensioni superiori a 64 KB, quindi non puoi archiviare i LOB tradizionali in Amazon Redshift.
- Imposta l'attività dei metadati di destinazione [BatChapplyEnabled](#) su `true` per AWS DMS per gestire le modifiche alle tabelle target Amazon Redshift durante il CDC. È necessaria una chiave primaria nella tabella di origine e nella tabella di destinazione. Senza una chiave primaria, le modifiche vengono applicate istruzione dopo istruzione. E ciò può influire negativamente sulle prestazioni delle attività durante il CDC causando latenza di destinazione e influenzando sulla coda di commit del cluster.

Privilegi richiesti per l'utilizzo di Redshift come destinazione

Utilizza il comando GRANT per definire i privilegi di accesso per un utente o un gruppo di utenti. I privilegi includono opzioni di accesso come la possibilità di leggere i dati in tabelle e viste, scrivere dati e creare tabelle. Per ulteriori informazioni sull'utilizzo di GRANT con Amazon Redshift, consulta [GRANT](#) nella Guida per gli sviluppatori di database Amazon Redshift.

Di seguito è riportata la sintassi per assegnare privilegi specifici per una tabella, un database, uno schema, una funzione, una procedura o privilegi a livello di lingua su tabelle e viste Amazon Redshift.

```
GRANT { { SELECT | INSERT | UPDATE | DELETE | REFERENCES } [,...] | ALL
  [ PRIVILEGES ] }
  ON { [ TABLE ] table_name [, ...] | ALL TABLES IN SCHEMA schema_name [, ...] }
  TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]
```

```

GRANT { { CREATE | TEMPORARY | TEMP } [,...] | ALL [ PRIVILEGES ] }
    ON DATABASE db_name [, ...]
    TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]

GRANT { { CREATE | USAGE } [,...] | ALL [ PRIVILEGES ] }
    ON SCHEMA schema_name [, ...]
    TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]

GRANT { EXECUTE | ALL [ PRIVILEGES ] }
    ON { FUNCTION function_name ( [ [ argname ] argtype [, ...] ] ) [, ...] | ALL
    FUNCTIONS IN SCHEMA schema_name [, ...] }
    TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]

GRANT { EXECUTE | ALL [ PRIVILEGES ] }
    ON { PROCEDURE procedure_name ( [ [ argname ] argtype [, ...] ] ) [, ...] | ALL
    PROCEDURES IN SCHEMA schema_name [, ...] }
    TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]

GRANT USAGE
    ON LANGUAGE language_name [, ...]
    TO { username [ WITH GRANT OPTION ] | GROUP group_name | PUBLIC } [, ...]

```

Di seguito è riportata la sintassi per i privilegi a livello di colonna su tabelle e viste Amazon Redshift.

```

GRANT { { SELECT | UPDATE } ( column_name [, ...] ) [, ...] | ALL [ PRIVILEGES ]
    ( column_name [, ...] ) }
    ON { [ TABLE ] table_name [, ...] }
    TO { username | GROUP group_name | PUBLIC } [, ...]

```

Di seguito è riportata la sintassi per il privilegio ASSUMEROLE concesso a utenti e gruppi con un ruolo specificato.

```

GRANT ASSUMEROLE
    ON { 'iam_role' [, ...] | ALL }
    TO { username | GROUP group_name | PUBLIC } [, ...]
    FOR { ALL | COPY | UNLOAD } [, ...]

```

Limitazioni all'utilizzo di Amazon Redshift come destinazione per AWS Database Migration Service

Le seguenti limitazioni si applicano quando si utilizza un database Amazon Redshift come destinazione:

- Non abilitare il controllo delle versioni per il bucket S3 che usi come storage intermedio per la destinazione Amazon Redshift. Se hai bisogno del controllo delle versioni S3, utilizza le policy del ciclo di vita per eliminare attivamente le vecchie versioni. In caso contrario, è possibile che si verifichino errori della connessione di test dell'endpoint a causa del timeout della chiamata `list-object` S3. Per creare una policy del ciclo di vita per un bucket S3, consulta [Gestione del ciclo di vita dello storage](#). Per eliminare la versione di un oggetto S3, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).

- Il seguente DDL non è supportato:

```
ALTER TABLE table name MODIFY COLUMN column name data type;
```

- AWS DMS non può migrare o replicare le modifiche in uno schema con un nome che inizia con un carattere di sottolineatura (`_`). Se disponi di schemi con un nome che inizia con un carattere di sottolineatura, utilizza le trasformazioni di mappatura per rinominare lo schema sulla destinazione.
- Amazon Redshift non supporta valori VARCHAR di dimensioni superiori a 64 KB. I LOB provenienti dai database tradizionali non possono essere archiviati in Amazon Redshift.
- L'applicazione di un'istruzione DELETE a una tabella con una chiave primaria a più colonne non è supportata quando uno dei nomi di colonna della chiave primaria utilizza una parola riservata. Vai [qui](#) per vedere un elenco di parole riservate Amazon Redshift.
- Potrebbero verificarsi problemi di prestazioni se il sistema di origine esegue operazioni UPDATE sulla chiave primaria di una tabella di origine. Questi problemi di prestazioni si verificano quando si applicano modifiche alla destinazione. Ciò accade perché le operazioni UPDATE (e DELETE) dipendono dal valore della chiave primaria per identificare la riga di destinazione. Se aggiorni la chiave primaria di una tabella di origine, il log delle attività conterrà messaggi come i seguenti:

```
Update on table 1 changes PK to a PK that was previously updated in the same bulk update.
```

- DMS non supporta nomi DNS personalizzati per la configurazione di un endpoint di un cluster Redshift ed è necessario utilizzare il nome DNS fornito da Amazon. Poiché il cluster Amazon

Redshift deve trovarsi nello stesso account e nella stessa regione AWS dell'istanza di replica, la convalida non riesce se si utilizza un endpoint DNS personalizzato.

- Amazon Redshift prevede un timeout di sessione inattiva predefinito di 4 ore. Quando non c'è alcuna esecuzione all'interno dell'attività di replica DMS, Redshift disconnette la sessione dopo 4 ore. Gli errori possono derivare dall'impossibilità di DMS di connettersi e dalla potenziale necessità di riavviare il sistema. Come soluzione alternativa, imposta per SESSION TIMEOUT un limite superiore a 4 ore per l'utente della replica DMS. In alternativa, consulta la descrizione di [ALTER USER](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Quando AWS DMS replica i dati della tabella di origine senza una chiave primaria o univoca, la latenza del CDC può essere elevata con conseguente livello di prestazioni inaccettabile.

Configurazione di un database Amazon Redshift come destinazione per AWS Database Migration Service

AWS Database Migration Service deve essere configurato per l'utilizzo dell'istanza Amazon Redshift. Nella tabella seguente vengono descritte le proprietà di configurazione disponibili per l'endpoint Amazon Redshift.

Proprietà	Description
server	Il nome del cluster Amazon Redshift in uso.
port	Il numero di porta per Amazon Redshift. Il valore predefinito è 5439.
username	Il nome utente Amazon Redshift di un utente registrato.
password	La password per l'utente denominato nella proprietà username.
database	Il nome del data warehouse (servizio) Amazon Redshift in uso.

Se desideri aggiungere ulteriori attributi della stringa di connessione all'endpoint Amazon Redshift, puoi specificare `maxFileSize` e `fileTransferUploadStreams`. Per ulteriori informazioni su questi attributi, consulta [Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS](#).

Utilizzo del routing VPC avanzato con Amazon Redshift come destinazione per AWS Database Migration Service

Se usi il routing VPC avanzato con la destinazione Amazon Redshift, tutto il traffico di tipo COPY tra il cluster Amazon Redshift e i repository di dati passa attraverso il VPC. Poiché il routing VPC avanzato influisce sul modo in cui Amazon Redshift accede ad altre risorse, i comandi COPY potrebbero avere esito negativo se non hai configurato correttamente il VPC.

AWS DMS può essere influenzato da questo comportamento perché utilizza il comando COPY per spostare i dati in S3 su un cluster Amazon Redshift.

Di seguito sono riportate le fasi intraprese da AWS DMS per il caricamento dei dati in una destinazione Amazon Redshift:

1. AWS DMS copia i dati dall'origine ai file .csv sul server di replica.
2. AWS DMS utilizza AWS SDK per copiare i file .csv in un bucket S3 sull'account.
3. AWS DMS utilizza quindi il comando COPY in Amazon Redshift per copiare i dati dai file .csv in S3 su una tabella appropriata in Amazon Redshift.

Se il routing VPC avanzato non è abilitato, Amazon Redshift instrada il traffico tramite Internet, incluso il traffico verso altri servizi nella rete AWS. Se la caratteristica non è abilitata, non è necessario configurare il percorso di rete. Se la caratteristica è abilitata, è necessario creare un percorso di rete tra il VPC del cluster e le risorse di dati. Per ulteriori informazioni sulla configurazione necessaria, consulta [Routing VPC avanzato](#) nella documentazione di Amazon Redshift.

Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift

È possibile crittografare i dati di destinazione trasmessi ad Amazon S3 prima di copiarli in Amazon Redshift. A questo scopo, puoi creare e utilizzare chiavi AWS KMS personalizzate. Puoi utilizzare la chiave creata per crittografare i dati di destinazione usando uno dei seguenti meccanismi al momento della creazione dell'endpoint di destinazione Amazon Redshift:

- Utilizza la seguente opzione quando esegui il comando `create-endpoint` utilizzando la AWS CLI.

```
--redshift-settings '{"EncryptionMode": "SSE_KMS", "ServerSideEncryptionKmsKeyId":  
"your-kms-key-ARN"}
```

Qui, *your-kms-key-ARN* è l'ARN (Amazon Resource Name) per la chiave KMS. Per ulteriori informazioni, consulta [Utilizzo di una chiave di crittografia dei dati e di un bucket Amazon S3 come storage intermedio](#).

- Imposta l'attributo di connessione aggiuntivo `encryptionMode` sul valore `SSE_KMS` e l'attributo della connessione aggiuntiva `serverSideEncryptionKmsKeyId` per l'ARN per la chiave KMS. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS](#).

Per crittografare i dati di destinazione Amazon Redshift utilizzando una chiave KMS, è necessario disporre di un ruolo AWS Identity and Access Management (IAM) che abbia le autorizzazioni per accedere ai dati Amazon Redshift. È possibile accedere a questo ruolo IAM in una policy (policy della chiave) collegata alla chiave di crittografia creata. È possibile farlo nella console IAM creando quanto segue:

- Un ruolo IAM con una policy gestita da AWS.
- Una chiave di crittografia KMS con la policy della chiave che fa riferimento a questo ruolo.

Nelle seguenti procedure viene descritto come procedere.

Per creare un ruolo IAM con la policy gestita da AWS richiesta

1. Apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione, seleziona Ruoli. Viene visualizzata la pagina Roles (Ruoli).
3. Scegli Crea ruolo. Viene visualizzata la pagina Create role (Crea ruolo).
4. Dopo aver selezionato Servizio AWS come entità attendibile, scegli DMS come servizio per l'utilizzo del ruolo.
5. Scegli Successivo: Autorizzazioni. Verrà visualizzata la pagina Attach permissions policies (Collega policy di autorizzazioni).
6. Trova e seleziona la policy `AmazonDMSRedshiftS3Role`.
7. Scegliere Successivo: Tag. Viene visualizzata la pagina Aggiungi tag. Qui è possibile aggiungere i tag desiderati.
8. Seleziona Next: Review (Successivo: Rivedi) ed esamina i risultati.
9. Se le impostazioni sono quelle desiderate, immetti un nome per il ruolo (ad esempio, `DMS-Redshift-endpoint-access-role`) e qualsiasi ulteriore descrizione, quindi scegli Create

role (Crea ruolo). Viene visualizzata la pagina Roles (Ruoli) con un messaggio che indica che il ruolo è stato creato.

Ora il nuovo ruolo per accedere alle risorse di Amazon Redshift per la crittografia con un nome specifico, ad esempio `DMS-Redshift-endpoint-access-role`, è stato creato.

Per creare una chiave crittografica AWS KMS con una policy della chiave che faccia riferimento al ruolo IAM

Note

Per ulteriori informazioni sul funzionamento di AWS DMS con le chiavi di crittografia AWS KMS, consulta [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#).

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo <https://console.aws.amazon.com/kms>.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave). Verrà visualizzata la pagina Configure key (Configura chiave).
5. Alla voce Key type (Tipo di chiave), scegliere Symmetric (Simmetrica).

Note

È possibile creare solo una chiave simmetrica, poiché tutti i servizi AWS, ad esempio Amazon Redshift, funzionano solo con chiavi di crittografia simmetriche.

6. Scegliere Advanced Options (Opzioni avanzate). Alla voce Key material origin (Origine del materiale della chiave), assicurarsi che sia selezionata la voce KMS quindi scegliere Next (Avanti). Verrà visualizzata la pagina Add labels (Aggiungi etichette).
7. Alla voce Create alias and description (Crea alias e descrizione), inserire un alias per la chiave (ad esempio `DMS-Redshift-endpoint-encryption-key`) e qualsiasi descrizione aggiuntiva.

8. Alla voce Tag, aggiungere tutti i tag desiderati per identificare la chiave e monitorarne l'utilizzo, quindi scegliere Next (Avanti). Verrà visualizzata la pagina Define key administrative permissions (Definisci autorizzazioni amministrative della chiave) che mostra un elenco di utenti e ruoli tra cui è possibile scegliere.
9. Aggiungi gli utenti e i ruoli che desideri gestiscano la chiave. Assicurati che questi utenti e ruoli dispongano delle autorizzazioni necessarie per gestire la chiave.
10. Alla voce Key deletion (Eliminazione chiave), scegliere se gli amministratori della chiave possono eliminarla, quindi scegliere Next (Avanti). Verrà visualizzata la pagina Define key usage permissions (Definisci autorizzazioni di utilizzo della chiave) che mostra un elenco aggiuntivo di utenti e ruoli tra cui è possibile scegliere.
11. Per Questo account scegli tra gli utenti disponibili quelli che dovranno eseguire operazioni di crittografia sulle destinazioni Amazon Redshift. Scegli in Ruoli il ruolo creato in precedenza per abilitare l'accesso alla crittografia degli oggetti di destinazione Amazon Redshift, ad esempio DMS-Redshift-endpoint-access-role.
12. Se desideri aggiungere altri account non elencati affinché abbiano lo stesso accesso, per Altri account AWS, scegli Aggiungi un altro account AWS, quindi seleziona Successivo. Verrà visualizzata la pagina Review and edit key policy (Rivedi e modifica la policy della chiave) che mostra il JSON associato alla policy della chiave, che è possibile rivedere e modificare digitando all'interno del testo esistente. Qui è possibile visualizzare il punto in cui la policy della chiave fa riferimento al ruolo e agli utenti (ad esempio, Admin e User1) selezionati nella fase precedente. È anche possibile visualizzare le diverse operazioni di chiave consentite per i diversi principali (utenti e ruoli), come mostrato nel seguente esempio.

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
  ],
}
```

```
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/Admin"
    ]
  },
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms>Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::111122223333:role/DMS-Redshift-endpoint-access-role",
      "arn:aws:iam::111122223333:role/Admin",
      "arn:aws:iam::111122223333:role/User1"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
}
```

```

    },
    {
      "Sid": "Allow attachment of persistent resources",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/DMS-Redshift-endpoint-access-role",
          "arn:aws:iam::111122223333:role/Admin",
          "arn:aws:iam::111122223333:role/User1"
        ]
      },
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
      ],
      "Resource": "*",
      "Condition": {
        "Bool": {
          "kms:GrantIsForAWSResource": true
        }
      }
    }
  ]
}
]

```

13. Scegli Fine. Viene visualizzata la pagina Chiavi di crittografia con un messaggio che indica che la AWS KMS key è stata creata.

È stata creata una nuova chiave KMS con un alias specificato (ad esempio, `DMS-Redshift-endpoint-encryption-key`). Questa chiave consente ad AWS DMS di crittografare i dati di destinazione Amazon Redshift.

Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS


È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione Amazon Redshift in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--redshift-settings '{"EndpointSetting": "value", ...}'`.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Amazon Redshift come destinazione.

Nome	Description
MaxFileSize	<p>Specifica la dimensione massima (in KB) di qualsiasi file .csv utilizzato per il trasferimento dei dati ad Amazon Redshift.</p> <p>Valore predefinito: 32.768 KB (32 MB)</p> <p>Valori validi: 1-1.048.576</p> <p>Esempio: <code>--redshift-settings '{"MaxFileSize": 512}'</code></p>
FileTransferUploadStreams	<p>Specifica il numero di thread utilizzati per caricare un singolo file.</p> <p>Valore predefinito: 10</p> <p>Valori validi: 1-64</p> <p>Esempio: <code>--redshift-settings '{"FileTransferUploadStreams": 20}'</code></p>
Acceptanydate	<p>Specifica se viene accettato qualsiasi formato di data, inclusi i formati di date non validi, ad esempio 0000-00-00. Valore booleano.</p> <p>Valore predefinito: false</p> <p>Valori validi: true false</p> <p>Esempio: <code>--redshift-settings '{"Acceptanydate": true}'</code></p>
Dateformat	<p>Specifica il formato della data. Si tratta di un input di stringa e tale campo è vuoto per impostazione predefinita. Il formato predefinito è AAAA-MM-GG ma è possibile</p>

Nome	Description
	<p>modificarlo, ad esempio, GG-MM-AAAA. Se i valori di ora o data utilizzano formati diversi, utilizzare l'argomento auto con il parametro <code>Dateformat</code> . L'argomento auto riconosce diversi formati che non sono supportati quando si utilizza una stringa <code>Dateformat</code> . La parola chiave auto prevede una distinzione tra lettere maiuscole e minuscole.</p> <p>Valore predefinito: vuoto</p> <p>Valori validi: "<i>dateformat_string</i>" o auto</p> <p>Esempio:--redshift-settings '{"Dateformat": "auto"}'</p>
Timeformat	<p>Specifica il formato dell'ora. Si tratta di un input di stringa e tale campo è vuoto per impostazione predefinita. L'argomento auto riconosce diversi formati che non sono supportati quando si utilizza una stringa <code>Timeformat</code> . Se i valori di data e ora utilizzano formati diversi tra loro, utilizzare l'argomento auto con il parametro <code>Timeformat</code> .</p> <p>Valore predefinito: 10</p> <p>Valori validi: "<i>Timeformat_string</i>" "auto" "epochsecs" "epochmillisecs"</p> <p>Esempio:--redshift-settings '{"Timeformat": "auto"}'</p>

Nome	Description
Emptyasnull	<p>Specifica se AWS DMS deve migrare campi CHAR e VARCHAR vuoti come null. Il valore true imposta i campi CHAR e VARCHAR vuoti come null.</p> <p>Valore predefinito: false</p> <p>Valori validi: true false</p> <p>Esempio: <code>--redshift-settings '{"Emptyasnull": true}'</code></p>
TruncateColumns	<p>Tronca i dati nelle colonne al numero appropriato di caratteri in modo che corrispondano alle specifiche della colonna. Si applica solo alle colonne con un tipo di dati VARCHAR o CHAR e alle righe di dimensioni fino a 4 MB.</p> <p>Valore predefinito: false</p> <p>Valori validi: true false</p> <p>Esempio: <code>--redshift-settings '{"TruncateColumns": true}'</code></p>
RemoveQuotes	<p>Rimuove le virgolette intorno alle stringhe nei dati in entrata. Tutti i caratteri compresi tra le virgolette, inclusi i delimitatori, vengono mantenuti. Per ulteriori informazioni sulla rimozione delle virgolette per una destinazione Amazon Redshift, consulta la Guida per gli sviluppatori di database di Amazon Redshift.</p> <p>Valore predefinito: false</p> <p>Valori validi: true false</p> <p>Esempio: <code>--redshift-settings '{"RemoveQuotes": true}'</code></p>

Nome	Description
TrimBlanks	<p>Rimuove i caratteri di spazio finale da una stringa VARCHAR. Questo parametro è valido solo per le colonne con un tipo di dati VARCHAR.</p> <p>Valore predefinito: false</p> <p>Valori validi: true false</p> <p>Esempio: <code>--redshift-settings '{"TrimBlanks": true}'</code></p>
EncryptionMode	<p>La modalità di crittografia lato server che si desidera utilizzare per inviare i dati a S3 prima di copiarli in Amazon Redshift. I valori validi sono SSE_S3 (crittografia lato server S3) o SSE_KMS (crittografia chiave KMS). Se scegli SSE_KMS, imposta il parametro <code>ServerSid</code> e <code>EncryptionKmsKeyId</code> al valore dell'ARN (Amazon Resource Name) della chiave KMS da utilizzare per la crittografia.</p> <div data-bbox="688 1100 1507 1514"><p> Note</p><p>È inoltre possibile utilizzare il comando CLI <code>modify-endpoint</code> per modificare il valore dell'impostazione <code>EncryptionMode</code> per un endpoint esistente da SSE_KMS a SSE_S3. Tuttavia non puoi modificare il valore di <code>EncryptionMode</code> da SSE_S3 a SSE_KMS.</p></div> <p>Valore predefinito: SSE_S3</p> <p>Valori validi: SSE_S3 o SSE_KMS</p> <p>Esempio: <code>--redshift-settings '{"EncryptionMode": "SSE_S3"}</code></p>

Nome	Description
ServerSideEncryptionKmsKeyId	<p>Se hai configurato <code>EncryptionMode</code> su <code>SSE_KMS</code>, imposta questo parametro sull'ARN della chiave KMS. Puoi trovare l'ARN selezionando l'alias della chiave nell'elenco delle chiavi AWS KMS create per l'account. Quando crei la chiave, è necessario associare ad essa policy e ruoli specifici. Per ulteriori informazioni, consulta Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift.</p> <p>Esempio: <code>--redshift-settings '{"ServerSideEncryptionKmsKeyId":"arn:aws:kms:us-east-1:111122223333:key/11a1a1a1-aaaa-9999-abab-2bbbbbb222a2"}'</code></p>
EnableParallelBatchInMemoryCSVFiles	<p>L'impostazione <code>EnableParallelBatchInMemoryCSVFiles</code> migliora le prestazioni delle attività di pieno carico multithread di maggiori dimensioni grazie alla possibilità di DMS di scrivere sul disco anziché sulla memoria. Il valore predefinito è <code>false</code>.</p>
CompressCsvFiles	<p>Utilizza questo attributo per comprimere i dati inviati a una destinazione Amazon Redshift durante la migrazione. Il valore predefinito è <code>true</code> e la compressione è abilitata per impostazione predefinita.</p>

Utilizzo di una chiave di crittografia dei dati e di un bucket Amazon S3 come storage intermedio

Puoi utilizzare le impostazioni degli endpoint di destinazione Amazon Redshift per configurare:

- Una chiave di crittografia dei dati AWS KMS personalizzata. Puoi utilizzare quindi questa chiave per crittografare i dati trasmessi ad Amazon S3 prima che siano copiati su Amazon Redshift.
- Un bucket S3 personalizzato come storage intermedio per i dati migrati in Amazon Redshift.
- Mappa un booleano come tale da un'origine PostgreSQL. Per impostazione predefinita, il tipo `BOOLEAN` viene migrato come `varchar(1)`. Puoi specificare `MapBooleanAsBoolean` per

consentire alla destinazione Redshift di migrare il tipo booleano come tale, come mostrato nell'esempio seguente.

```
--redshift-settings '{"MapBooleanAsBoolean": true}'
```

Tieni presente che questa impostazione, affinché abbia effetto, deve essere configurata sia sull'endpoint di origine che su quello di destinazione.

Impostazioni delle chiavi KMS per la crittografia dei dati

I seguenti esempi mostrano la configurazione di una chiave KMS personalizzata per crittografare i dati trasmessi a S3. Per iniziare, è possibile effettuare la seguente chiamata `create-endpoint` utilizzando la AWS CLI.

```
aws dms create-endpoint --endpoint-identifier redshift-target-endpoint --endpoint-type target
--engine-name redshift --username your-username --password your-password
--server-name your-server-name --port 5439 --database-name your-db-name
--redshift-settings '{"EncryptionMode": "SSE_KMS",
"ServerSideEncryptionKmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/24c3c5a1-
f34a-4519-a85b-2debbef226d1"}'
```

Qui l'oggetto JSON specificato dall'opzione `--redshift-settings` definisce due parametri. Uno è un parametro `EncryptionMode` con il valore `SSE_KMS`. L'altro è un parametro `ServerSideEncryptionKmsKeyId` con il valore `arn:aws:kms:us-east-1:111122223333:key/24c3c5a1-f34a-4519-a85b-2debbef226d1`. Questo valore è un ARN (Amazon Resource Name) per la chiave KMS personalizzata.

Per impostazione predefinita, la crittografia dei dati di S3 viene effettuata utilizzando la crittografia lato server. Per la destinazione Amazon Redshift dell'esempio precedente, ciò equivale a specificare le impostazioni degli endpoint, come nell'esempio seguente.

```
aws dms create-endpoint --endpoint-identifier redshift-target-endpoint --endpoint-type target
--engine-name redshift --username your-username --password your-password
--server-name your-server-name --port 5439 --database-name your-db-name
--redshift-settings '{"EncryptionMode": "SSE_S3"}'
```

Per ulteriori informazioni sull'utilizzo della crittografia lato server S3, consulta [Protezione dei dati con la crittografia lato server](#) nella Guida per l'utente di Amazon Simple Storage Service.

Note

È inoltre possibile utilizzare il comando CLI `modify-endpoint` per modificare il valore del parametro `EncryptionMode` per un endpoint esistente da `SSE_KMS` a `SSE_S3`. Tuttavia non puoi modificare il valore di `EncryptionMode` da `SSE_S3` a `SSE_KMS`.

Impostazioni del bucket Amazon S3

Quando esegui la migrazione di dati su un endpoint di destinazione Amazon Redshift, AWS DMS utilizza un bucket Amazon S3 predefinito per lo storage intermedio dell'attività prima della copia dei dati migrati su Amazon Redshift. Gli esempi mostrati per la creazione di un endpoint di destinazione Amazon Redshift con una chiave di crittografia dei dati AWS KMS utilizzano questo bucket S3 predefinito (consulta [Impostazioni delle chiavi KMS per la crittografia dei dati](#)).

Puoi invece specificare un bucket S3 personalizzato da usare come area di memorizzazione intermedia includendo i seguenti parametri nel valore dell'opzione `--redshift-settings` nel comando `create-endpoint` invocato tramite AWS CLI:

- `BucketName`: una stringa che specifichi come nome dello storage del bucket S3. Se il ruolo di accesso al servizio si basa sulla policy `AmazonDMSRedshiftS3Role`, questo valore deve avere il prefisso `dms-`, ad esempio `dms-my-bucket-name`.
- `BucketFolder` (facoltativo): una stringa che è possibile indicare come nome della cartella di storage nel bucket S3 specificato.
- `ServiceAccessRoleArn`: l'ARN di un ruolo IAM che consente l'accesso amministrativo al bucket S3. Di solito, è necessario creare questo ruolo in base alla policy `AmazonDMSRedshiftS3Role`. Per un esempio, consulta la procedura per creare un ruolo IAM con la policy gestita da AWS richiesta in [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#).

Note

Se specifichi l'ARN di un altro ruolo IAM utilizzando l'opzione `--service-access-role-arn` del comando `create-endpoint`, questa opzione per il ruolo IAM ha la precedenza.

L'esempio seguente mostra come utilizzare questi parametri per specificare un bucket Amazon S3 personalizzato nella seguente chiamata `create-endpoint` utilizzando la AWS CLI.

```
aws dms create-endpoint --endpoint-identifier redshift-target-endpoint --endpoint-type
target
--engine-name redshift --username your-username --password your-password
--server-name your-server-name --port 5439 --database-name your-db-name
--redshift-settings '{"ServiceAccessRoleArn": "your-service-access-ARN",
"BucketName": "your-bucket-name", "BucketFolder": "your-bucket-folder-name"}'
```

Impostazioni delle attività multithread per Amazon Redshift

Puoi migliorare le prestazioni delle attività di pieno carico e acquisizione dei dati di modifica (CDC) per un endpoint di destinazione Amazon Redshift utilizzando le impostazioni delle attività multithread. Ti consentono di specificare il numero di thread simultanei e il numero di record da archiviare in un buffer.

Impostazioni delle attività di pieno carico multithread per Amazon Redshift

Per promuovere le prestazioni del pieno carico, puoi utilizzare le seguenti impostazioni dell'attività `ParallelLoad*`:

- `ParallelLoadThreads`: specifica il numero di thread simultanei che DMS utilizza durante un pieno carico per eseguire il push di record di dati a un endpoint di destinazione Amazon Redshift. Il valore predefinito è zero (0) e il valore massimo è 32. Per ulteriori informazioni, consulta [Impostazioni delle attività di caricamento completo](#).

Puoi impostare l'attributo `enableParallelBatchInMemoryCSVFiles` su `false` quando usi l'impostazione dell'attività `ParallelLoadThreads`. L'attributo migliora le prestazioni delle attività di pieno carico multithread di maggiori dimensioni grazie alla possibilità di DMS di scrivere sul disco anziché sulla memoria. Il valore predefinito è `true`.

- `ParallelLoadBufferSize`: specifica il numero massimo di richieste di record di dati durante l'utilizzo di thread di caricamento paralleli con la destinazione Redshift. Il valore predefinito è 100 e il valore massimo è 1.000. Si consiglia di utilizzare questa opzione quando `ParallelLoadThreads` > 1 (maggiore di uno).

Note

Il supporto per l'uso delle impostazioni dell'attività `ParallelLoad*` durante il FULL LOAD negli endpoint di destinazione Amazon Redshift è disponibile in AWS DMS 3.4.5 e versioni successive.

L'impostazione dell'endpoint `ReplaceInvalidChars` Redshift non è supportata per l'uso durante l'acquisizione dei dati di modifica (CDC) o durante un'attività di migrazione FULL LOAD abilitata al caricamento parallelo. È supportata per la migrazione FULL LOAD quando il caricamento parallelo non è abilitato. Per ulteriori informazioni, consulta [RedshiftSettings](#) nella Documentazione di riferimento delle API di AWS Database Migration Service

Impostazioni dell'attività di CDC multithread per Amazon Redshift

Per promuovere le prestazioni della CDC, puoi utilizzare le seguenti impostazioni dell'attività `ParallelApply*`.

- `ParallelApplyThreads`: specifica il numero di thread simultanei utilizzati da AWS DMS durante un carico CDC per eseguire il push di record di dati a un endpoint di destinazione Amazon Redshift. Il valore predefinito è zero (0) e il valore massimo è 32. Il valore minimo consigliato è pari al numero di sezioni del cluster.
- `ParallelApplyBufferSize`: specifica il numero massimo di richieste di record di dati durante l'utilizzo di thread di applicazione paralleli con la destinazione Redshift. Il valore predefinito è 100 e il valore massimo è 1.000. Si consiglia di utilizzare questa opzione quando `ParallelApplyThreads` > 1 (maggiore di uno).

Per ottenere il massimo vantaggio da Redshift come destinazione, è opportuno che il valore di `ParallelApplyBufferSize` sia almeno due volte (il doppio) il numero di `ParallelApplyThreads`.

Note

Il supporto per l'uso delle impostazioni dell'attività `ParallelApply*` durante CDC verso gli endpoint di destinazione Amazon Redshift è disponibile in AWS DMS 3.4.3 e versioni successive.

Il livello di parallelismo applicato dipende dalla correlazione tra la dimensione del batch totale e la dimensione massima del file utilizzato per trasferire i dati. Quando si utilizzano impostazioni dell'attività di CDC multithread con una destinazione Redshift, si ottengono vantaggi quando la dimensione del batch è elevata rispetto alla dimensione massima del file. Ad esempio, per ottimizzare le prestazioni è possibile utilizzare la seguente combinazione di impostazioni dell'endpoint e dell'attività.

```
// Redshift endpoint setting

    MaxFileSize=250000;

// Task settings

    BatchApplyEnabled=true;
    BatchSplitSize =8000;
    BatchApplyTimeoutMax =1800;
    BatchApplyTimeoutMin =1800;
    ParallelApplyThreads=32;
    ParallelApplyBufferSize=100;
```

Utilizzando le impostazioni dell'esempio precedente, un cliente con un carico di lavoro transazionale intenso trae vantaggio dal fatto che il buffer batch, contenente 8000 record, viene riempito in 1800 secondi e utilizza 32 thread paralleli con una dimensione massima del file di 250 MB.

Per ulteriori informazioni, consulta [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).

Note

Le query DMS eseguite durante la replica continua su un cluster Redshift possono condividere la stessa coda di gestione del carico di lavoro con altre query applicative in esecuzione. Pertanto, prendi in considerazione la corretta configurazione delle proprietà di gestione del carico di lavoro per influenzare le prestazioni durante la replica continua su una destinazione Redshift. Ad esempio, se sono in esecuzione altre query ETL parallele, DMS viene eseguito più lentamente e i miglioramenti delle prestazioni sono vanificati.

Tipi di dati di destinazione per Amazon Redshift.

L'endpoint Amazon Redshift per AWS DMS supporta la maggior parte dei tipi di dati Amazon Redshift. La tabella seguente mostra i tipi di dati di destinazione di Amazon Redshift supportati quando si utilizza AWS DMS e la mappatura predefinita dei tipi di dati AWS DMS.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati AWS DMS	Tipi di dati Amazon Redshift
BOOLEAN	BOOL
BYTES	VARCHAR (lunghezza)
DATE	DATE
TIME	VARCHAR(20)
DATETIME	<p>Se la scala è => 0 e =< 6, a seconda del tipo di colonna di destinazione Redshift, il valore è uno dei seguenti:</p> <p>TIMESTAMP (s)</p> <p>TIMESTAMPTZ (s): se il timestamp di origine contiene un offset di zona (come in SQL Server oppure Oracle), viene convertito in UTC al momento dell'inserimento/aggiornamento. Se non contiene un offset, l'ora viene già considerata in UTC.</p> <p>Se il dimensionamento è => 7 e =< 9:</p> <p>VARCHAR (37)</p>
INT1	INT2
INT2	INT2
INT4	INT4

Tipi di dati AWS DMS	Tipi di dati Amazon Redshift
INT8	INT8
NUMERIC	<p>Se il dimensionamento è => 0 e =< 37: NUMERIC (p,s)</p> <p>Se il dimensionamento è => 38 e =< 127: VARCHAR (lunghezza)</p>
REAL4	FLOAT4
REAL8	FLOAT8
STRING	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizza VARCHAR (lunghezza in byte)</p> <p>Se la lunghezza è compresa tra 65.536 e 2.147.483.647, utilizza VARCHAR (65535)</p>
UINT1	INT2
UINT2	INT2
UINT4	INT4
UINT8	NUMERIC (20,0)
WSTRING	<p>Se la lunghezza è compresa tra 1 e 65.535, utilizza NVARCHAR (lunghezza in byte)</p> <p>Se la lunghezza è compresa tra 65.536 e 2.147.483.647, utilizza NVARCHAR (65535)</p>

Tipi di dati AWS DMS	Tipi di dati Amazon Redshift
BLOB	VARCHAR (dimensioni massime di LOB *2) Le dimensioni massime di LOB non possono superare 31 KB. Amazon Redshift non supporta valori VARCHAR di dimensioni superiori a 64 KB.
NCLOB	NVARCHAR (dimensioni massime di LOB) Le dimensioni massime di LOB non possono superare 63 KB. Amazon Redshift non supporta valori VARCHAR di dimensioni superiori a 64 KB.
CLOB	VARCHAR (dimensioni massime di LOB) Le dimensioni massime di LOB non possono superare 63 KB. Amazon Redshift non supporta valori VARCHAR di dimensioni superiori a 64 KB.

Utilizzo di AWS DMS con Amazon Redshift serverless come destinazione

AWS DMS supporta l'utilizzo di Amazon Redshift serverless come endpoint di destinazione. Per informazioni sull'uso di Amazon Redshift serverless, consulta [Amazon Redshift serverless](#) nella [Guida alla gestione di Amazon Redshift](#).

In questo argomento viene descritto come utilizzare un endpoint Amazon Redshift serverless con AWS DMS.

Note

Quando crei un endpoint Amazon Redshift serverless per il campo DatabaseName della configurazione dell'endpoint [RedshiftSettings](#), usa il nome del data warehouse Amazon Redshift o il nome dell'endpoint del gruppo di lavoro. Per il campo ServerName, utilizza il valore dell'endpoint visualizzato nella pagina Gruppo di lavoro per il cluster serverless (ad esempio default-workgroup.093291321484.us-east-1.redshift-

serverless.amazonaws.com). Per informazioni su come creare un endpoint, vedi [Creazione di endpoint di origine e destinazione](#). Per informazioni sull'endpoint del gruppo di lavoro, consulta [Connessione ad Amazon Redshift serverless](#).

Policy di attendibilità con Amazon Redshift serverless come destinazione

Quando utilizzi Amazon Redshift serverless come endpoint di destinazione, devi aggiungere la seguente sezione evidenziata alla policy di attendibilità. Questa policy di attendibilità è associata al ruolo `dms-access-for-endpoint`.

```
{
  "PolicyVersion": {
    "CreateDate": "2016-05-23T16:29:57Z",
    "VersionId": "v3",
    "Document": {
      "Version": "2012-10-17",
      "Statement": [
        {
          "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:DescribeAvailabilityZones",
            "ec2:DescribeInternetGateways",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2>DeleteNetworkInterface",
            "ec2:ModifyNetworkInterfaceAttribute"
          ],
          "Resource": "arn:aws:service:region:account:resourcetype/id",
          "Effect": "Allow"
        },
        {
          "Sid": "",
          "Effect": "Allow",
          "Principal": {
            "Service": "redshift-serverless.amazonaws.com"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
  },
}
```

```
"IsDefaultVersion": true
}
}
```

Per ulteriori informazioni sull'uso di una policy di attendibilità con AWS DMS, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

Limitazioni all'utilizzo di Amazon Redshift serverless come destinazione

L'utilizzo di Redshift serverless come destinazione prevede le seguenti limitazioni:

- AWS DMS supporta Amazon Redshift serverless come endpoint solo nelle regioni che supportano Amazon Redshift serverless. Per informazioni sulle regioni che supportano Amazon Redshift serverless, consulta API Redshift serverless nell'argomento [Endpoint e quote di Amazon Redshift](#) della [Guida di riferimento generale di AWS](#).
- Quando utilizzi il routing VPC avanzato, assicurati di creare un endpoint Amazon S3 nello stesso VPC del cluster Redshift serverless o del cluster con provisioning Redshift. Per ulteriori informazioni, consulta [Utilizzo del routing VPC avanzato con Amazon Redshift come destinazione per AWS Database Migration Service](#).
- AWS DMS serverless non supporta Amazon Redshift serverless come destinazione.

Utilizzo di un database SAP ASE come destinazione per AWS Database Migration Service

Puoi eseguire la migrazione dei dati ai database SAP Adaptive Server Enterprise (ASE), precedentemente denominati Sybase, mediante AWS DMS da qualsiasi origine di database supportata.

Per informazioni sulle versioni di SAP ASE supportate da AWS DMS come destinazione, consulta [Obiettivi per AWS DMS](#).

Prerequisiti per l'utilizzo di un database SAP ASE come destinazione per AWS Database Migration Service

Prima di iniziare a utilizzare un database SAP ASE come destinazione per AWS DMS, accertati che siano soddisfatti i seguenti prerequisiti:

- Fornire all'account SAP ASE l'accesso all'utente AWS DMS. Questo utente deve disporre dei privilegi di lettura/scrittura nel database SAP ASE.

- In alcuni casi, è possibile eseguire la replica in SAP ASE versione 15.7 installato in un'istanza Amazon EC2 di Microsoft Windows configurata con caratteri non latini (ad esempio, cinese). In questi casi, AWS DMS richiede l'installazione di SAP ASE 15.7 SP121 sul computer SAP ASE di destinazione.

Limitazioni all'utilizzo di un database SAP ASE come destinazione per AWS DMS

Quando si utilizza un database SAP ASE come destinazione per AWS DMS, si applicano le seguenti limitazioni:

- AWS DMS non supporta tabelle che includono i campi con i seguenti tipi di dati. Le colonne replicate con questi tipi di dati vengono mostrate come null.
 - Tipo definito dall'utente (UDT, User-Defined Type)

Impostazioni degli endpoint quando si utilizza SAP ASE come destinazione per AWS DMS

È possibile utilizzare le impostazioni di endpoint per configurare il database di destinazione SAP ASE in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--sybase-settings '{"EndpointSetting": "value", ...}'`.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con SAP ASE come destinazione.

Nome	Descrizione
Driver	<p>Imposta questo attributo se desideri utilizzare TLS per le versioni di ASE 15.7 e successive.</p> <p>Valore predefinito: Adaptive Server Enterprise</p> <p>Esempio: <code>driver=Adaptive Server Enterprise 16.03.06;</code></p> <p>Valori validi: Adaptive Server Enterprise 16.03.06</p>

Nome	Descrizione
AdditionalConnectionProperties	Qualsiasi parametro di connessione ODBC aggiuntivo che si desidera specificare.

Tipi di dati di destinazione per SAP ASE

La tabella seguente mostra i tipi di dati di destinazione del database SAP ASE supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati AWS DMS.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati AWS DMS	Tipi di dati SAP ASE
BOOLEAN	BIT
BYTES	VARBINARY (lunghezza)
DATE	DATE
TIME	TIME
TIMESTAMP	Se il dimensionamento è => 0 e =< 6: BIGDATETIME Se il dimensionamento è => 7 e =< 9, VARCHAR (37)
INT1	TINYINT
INT2	SMALLINT
INT4	INTEGER
INT8	BIGINT
NUMERIC	NUMERIC (p,s)
REAL4	REAL

Tipi di dati AWS DMS	Tipi di dati SAP ASE
REAL8	DOUBLE PRECISION
STRING	VARCHAR (lunghezza)
UINT1	TINYINT
UINT2	UNSIGNED SMALLINT
UINT4	UNSIGNED INTEGER
UINT8	UNSIGNED BIGINT
WSTRING	VARCHAR (lunghezza)
BLOB	IMAGE
CLOB	UNITEXT
NCLOB	TEXT

Utilizzo di Amazon S3 come destinazione per AWS Database Migration Service

Puoi eseguire la migrazione dei dati ad Amazon S3 mediante AWS DMS da qualsiasi origine di database supportata. Quando utilizzi Amazon S3 come destinazione in un'attività AWS DMS, i dati del pieno carico e dell'acquisizione dei dati di modifica (CDC) vengono scritti per impostazione predefinita in formato .csv (valori separati da virgole). Per opzioni di storage più compatto e per query più rapide, è possibile scrivere i dati nel formato Apache Parquet (.parquet).

AWS DMS denomina i file creati durante un pieno carico utilizzando un contatore esadecimale incrementale, ad esempio LOAD00001.csv, LOAD00002..., LOAD00009, LOAD0000A e così via per i file.csv. AWS DMS denomina i file CDC utilizzando i timestamp, ad esempio 20141029-1134010000.csv. Per ciascuna tabella di origine contenente record, AWS DMS crea una cartella nella cartella di destinazione specificata (se la tabella non è vuota). AWS DMS scrive tutti i file CDC e del pieno carico nel bucket Amazon S3 specificato. È possibile controllare la dimensione dei file creati da AWS DMS utilizzando l'impostazione dell'endpoint [MaxFileSize](#).

Il parametro `bucketFolder` contiene il percorso in cui i file `.csv` o `.parquet` vengono archiviati prima di essere caricati nel bucket S3. Con i file `.csv` i dati di tabella vengono archiviati nel formato seguente nel bucket S3 con i file di pieno carico.

```
database_schema_name/table_name/LOAD00000001.csv
database_schema_name/table_name/LOAD00000002.csv
...
database_schema_name/table_name/LOAD00000009.csv
database_schema_name/table_name/LOAD0000000A.csv
database_schema_name/table_name/LOAD0000000B.csv
...database_schema_name/table_name/LOAD0000000F.csv
database_schema_name/table_name/LOAD00000010.csv
...
```

Puoi specificare il delimitatore di colonna, di riga e altri parametri utilizzando gli attributi di connessione aggiuntivi. Per ulteriori informazioni sugli attributi di connessione aggiuntivi, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#) alla fine di questa sezione.

Puoi specificare il proprietario del bucket e impedire lo sniping utilizzando l'impostazione dell'endpoint `ExpectedBucketOwner` Amazon S3, come illustrato di seguito. Quindi, quando effettui una richiesta per testare una connessione o eseguire una migrazione, S3 controlla l'ID account del proprietario del bucket rispetto al parametro specificato.

```
--s3-settings='{"ExpectedBucketOwner": "AWS_Account_ID"}
```

Quando utilizzi AWS DMS per replicare le modifiche dei dati con un'attività di CDC, la prima colonna del file di output `.csv` o `.parquet` indica il modo in cui i dati della riga sono stati modificati, come illustrato nel seguente file `.csv`.

```
I,101,Smith,Bob,4-Jun-14,New York
U,101,Smith,Bob,8-Oct-15,Los Angeles
U,101,Smith,Bob,13-Mar-17,Dallas
D,101,Smith,Bob,13-Mar-17,Dallas
```

Per questo esempio, supponiamo che vi sia una tabella `EMPLOYEE` nel database di origine. AWS DMS scrive i dati nel file `.csv` o `.parquet` in risposta ai seguenti eventi:

- Un nuovo dipendente (Bob Smith, ID dipendente 101) viene assunto il 4 giugno 2014 presso l'ufficio di New York. Nel file .csv o .parquet, il simbolo I nella prima colonna indica che una nuova riga è stata inserita con il comando INSERT nella tabella EMPLOYEE nel database di origine.
- In data 8 ottobre 2015, Bob si trasferisce all'ufficio di Los Angeles. Nel file .csv o .parquet il simbolo U indica che la riga corrispondente nella tabella EMPLOYEE è stata aggiornata con il comando UPDATE per riflettere il trasferimento di Bob nel nuovo ufficio. Il resto della riga riflette la riga nella tabella EMPLOYEE come appare dopo UPDATE.
- Il 13 marzo 2017 Bob si trasferisce di nuovo all'ufficio di Dallas. Nel file .csv o .parquet U indica che la riga è stata nuovamente aggiornata con il comando UPDATE. Il resto della riga riflette la riga nella tabella EMPLOYEE come appare dopo UPDATE.
- Dopo un periodo di tempo presso l'ufficio di Dallas, Bob lascia l'azienda. Nel file .csv o .parquet il simbolo D indica che la riga è stata eliminata con il comando DELETE nella tabella di origine. Il resto della riga riflette come la riga nella tabella EMPLOYEE appariva prima dell'eliminazione.

Tieni presente che, per impostazione predefinita, per CDC, AWS DMS memorizza le modifiche della riga per ogni tabella del database indipendentemente dall'ordine delle transazioni. Se desideri archiviare le modifiche della riga nei file CDC in base all'ordine delle transazioni, è necessario utilizzare le impostazioni dell'endpoint S3 per specificarlo e il percorso della cartella in cui desideri che i file delle transazioni CDC vengano archiviati sulla destinazione S3. Per ulteriori informazioni, consulta [Capturing Data Changes \(CDC\) incluso l'ordine di transazione sulla destinazione S3](#).

Per controllare la frequenza delle scritture su una destinazione Amazon S3 durante un'attività di replica dei dati, puoi configurare gli attributi aggiuntivi di connessione `cdcMaxBatchInterval` e `cdcMinFileSize`. In tal modo le prestazioni possono risultare migliori durante l'analisi dei dati senza ulteriori operazioni di sovraccarico. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#)

Argomenti

- [Prerequisiti per l'utilizzo di Amazon S3 come destinazione](#)
- [Limitazioni all'utilizzo di Amazon S3 come destinazione](#)
- [Sicurezza](#)
- [Utilizzo di Apache Parquet per l'archiviazione di oggetti Amazon S3](#)
- [Applicazione di tag agli oggetti Amazon S3](#)
- [Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3](#)
- [Utilizzo del partizionamento delle cartelle in base alla data](#)

- [Caricamento parallelo di origini partizionate quando si utilizza Amazon S3 come destinazione per AWS DMS](#)
- [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#)
- [Utilizzo di AWS Glue Data Catalog con una destinazione Amazon S3 per AWS DMS](#)
- [Utilizzo della crittografia dei dati, dei file parquet e della CDC sulla destinazione Amazon S3](#)
- [Indicazione delle operazioni del DB di origine nei dati S3 migrati](#)
- [Tipi di dati di destinazione per Parquet S3](#)

Prerequisiti per l'utilizzo di Amazon S3 come destinazione

Prima di utilizzare Amazon S3 come destinazione, controlla che le seguenti condizioni siano soddisfatte:

- Il bucket S3 che usi come destinazione sia nella stessa regione AWS dell'istanza di replica DMS in uso per migrare i dati.
- L'account AWS utilizzato per la migrazione deve disporre di un ruolo IAM con accesso per scrittura ed eliminazione al bucket S3 in uso come destinazione.
- In questo ruolo ha accesso con il tagging in modo da poter aggiungere tag qualsiasi oggetto S3 scritto nel bucket di destinazione.
- Il ruolo IAM è stato aggiunto da DMS (dms.amazonaws.com) come entità attendibile.

Per configurare l'accesso a questo account, assicurarsi che il ruolo assegnato all'account utente utilizzato per creare l'attività di migrazione disponga del seguente set di autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::buckettest2/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::buckettest2"
      ]
    }
  ]
}
```

Per i prerequisiti per l'utilizzo della convalida con S3 come destinazione, consulta [Prerequisiti per la convalida della destinazione S3](#).

Limitazioni all'utilizzo di Amazon S3 come destinazione

Le seguenti limitazioni si applicano quando si utilizza Amazon S3 come destinazione:

- Non abilitare il controllo delle versioni per S3. Se hai bisogno del controllo delle versioni S3, utilizza le policy del ciclo di vita per eliminare attivamente le vecchie versioni. In caso contrario, è possibile che si verifichino errori della connessione di test dell'endpoint a causa del timeout della chiamata `list-object` S3. Per creare una policy del ciclo di vita per un bucket S3, consulta [Gestione del ciclo di vita dello storage](#). Per eliminare la versione di un oggetto S3, consulta [Eliminazione di versioni di oggetti da un bucket con funzione Controllo delle versioni abilitata](#).
- Un bucket S3 abilitato per VPC (VPC del gateway) è supportato nelle versioni 3.4.7 e successive.
- Per l'acquisizione dei dati di modifica (CDC) sono supportati i seguenti comandi DDL (Data Definition Language): Truncate Table, Drop Table, Create Table, Rename Table, Add Column, Drop Column, Rename Column e Change Column Data Type. Tieni presente che quando una colonna viene aggiunta, eliminata o rinominata nel database di origine, nessuna istruzione ALTER viene registrata nel bucket S3 di destinazione e AWS DMS non altera i record creati in precedenza per adattarli alla nuova struttura. Dopo la modifica, AWS DMS crea tutti i nuovi record utilizzando la nuova struttura della tabella.

Note

Un'operazione DDL di troncamento rimuove tutti i corrispondenti file e le cartelle della tabella da un bucket S3. È possibile utilizzare le impostazioni delle attività per disabilitare tale comportamento e configurare il modo in cui DMS gestisce l'approccio DDL durante

l'acquisizione dei dati di modifica (CDC). Per ulteriori informazioni, consulta [Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche](#).

- La modalità LOB completa non è supportata.
- Le modifiche apportate alla struttura della tabella di origine durante il caricamento completo non sono supportate. Le modifiche apportate ai dati sono supportate durante il pieno carico.
- Se più attività replicano i dati dalla stessa tabella di origine allo stesso bucket dell'endpoint S3 di destinazione, tali attività scrivono sullo stesso file. Se l'origine dati proviene dalla stessa tabella, è consigliabile specificare endpoint di destinazione (bucket) diversi.
- BatchApply non è supportato per un endpoint S3. L'utilizzo dell'applicazione in batch, ad esempio l'impostazione dell'attività dei metadati di destinazione BatchApplyEnabled, per una destinazione S3 potrebbe causare la perdita di dati.
- Non puoi usare DatePartitionEnabled o addColumnName insieme con PreserveTransactions o CdcPath.
- AWS DMS non supporta la ridenominazione di più tabelle di origine nella stessa cartella di destinazione utilizzando le regole di trasformazione.
- In caso di scrittura intensiva sulla tabella di origine durante la fase di pieno carico, DMS può scrivere record duplicati nel bucket S3 o modifiche memorizzate nella cache.
- Se configuri l'attività con il TargetTablePrepMode come DO_NOTHING, DMS può scrivere record duplicati nel bucket S3 se l'attività si interrompe e riprende improvvisamente durante la fase di pieno carico.
- Se configuri l'endpoint di destinazione con PreserveTransactions impostato su true, il ricaricamento di una tabella non cancella i file CDC generati in precedenza. Per ulteriori informazioni, consulta [Capturing Data Changes \(CDC\) incluso l'ordine di transazione sulla destinazione S3](#).

Per le limitazioni all'utilizzo della convalida con S3 come destinazione, consulta [Limitazioni all'utilizzo della convalida della destinazione S3](#).

Sicurezza

Per utilizzare Amazon S3 come destinazione, l'account usato per la migrazione deve disporre dell'accesso per scrittura ed eliminazione al bucket Amazon S3 in uso come destinazione. Specifica il nome della risorsa Amazon (ARN) di un ruolo IAM che dispone delle autorizzazioni necessarie per accedere ad Amazon S3.

AWS DMS supporta un set di concessioni predefinite per Amazon S3, definite liste di controllo degli accessi (ACL) predefinite. Ogni ACL predefinita dispone di un set di assegnatari e autorizzazioni che sono utilizzabili per impostare le autorizzazioni per il bucket Amazon S3. Puoi specificare un'ACL predefinita mediante `cannedAc1For0bjects` sull'attributo della stringa di connessione per l'endpoint di destinazione S3. Per ulteriori informazioni sull'utilizzo dell'attributo di connessione aggiuntivo `cannedAc1For0bjects`, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#). Per ulteriori informazioni sulle ACL predefinite di Amazon S3, consulta [ACL predefinita](#).

Il ruolo IAM utilizzato per la migrazione deve essere in grado di eseguire l'operazione API `s3:Put0bjectAc1`.

Utilizzo di Apache Parquet per l'archiviazione di oggetti Amazon S3

Il formato valore separato da virgole (csv) è il formato di archiviazione predefinito per gli oggetti di destinazione Amazon S3. Per storage più compatto e per query più rapide, è possibile utilizzare Apache parquet (.parquet) come formato di archiviazione.

Apache Parquet è un formato di archiviazione dei file open source originariamente progettato per Hadoop. Per ulteriori informazioni su Apache Parquet, consulta <https://parquet.apache.org/>.

Per impostare .parquet come formato di storage per gli oggetti di destinazione S3 migrati, è possibile utilizzare i seguenti meccanismi:

- Le impostazioni dell'endpoint fornite come parametri di un oggetto JSON durante la creazione dell'endpoint utilizzando la AWS CLI o l'API per AWS DMS. Per ulteriori informazioni, consulta [Utilizzo della crittografia dei dati, dei file parquet e della CDC sulla destinazione Amazon S3](#).
- Gli attributi aggiuntivi di connessione forniti come un elenco separato da punti e virgola durante la creazione dell'endpoint. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#).

Applicazione di tag agli oggetti Amazon S3



È possibile applicare i tag agli oggetti Amazon S3 creati da un'istanza di replica specificando oggetti JSON appropriati come parte delle regole di mappatura attività-tabella. Per ulteriori informazioni sui requisiti e sulle opzioni per l'applicazione di tag agli oggetti S3, inclusi i nomi di tag validi, consulta [Tagging oggetti](#) nella Guida per l'utente di Amazon Simple Storage Service. Per ulteriori informazioni sulla mappatura delle tabelle mediante JSON, consulta [Specifiche della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).

Puoi aggiungere tag agli oggetti S3 creati per tabelle e schemi specifici utilizzando uno o più oggetti JSON del tipo di regola `selection`. Quindi fai seguire all'oggetto (o agli oggetti) `selection` uno o più oggetti JSON del tipo di regola `post-processing` con l'operazione `add-tag`. Tali regole di post-elaborazione identificano gli oggetti S3 a cui desideri aggiungere tag e specificano i nomi e i valori dei tag che desideri aggiungere a questi oggetti S3.

Puoi trovare i parametri da specificare negli oggetti JSON del tipo di regola `post-processing` nella tabella riportata di seguito.

Parametro	Valori possibili	Description
<code>rule-type</code>	<code>post-processing</code>	Valore che si applica alle operazioni di post-elaborazione agli oggetti di destinazione generati. Puoi specificare una o più regole di post-elaborazione per aggiungere tag agli oggetti S3 selezionati.
<code>rule-id</code>	Un valore numerico.	Un valore numerico univoco per identificare la regola.
<code>rule-name</code>	Un valore alfanumerico.	Un nome univoco per identificare la regola.
<code>rule-action</code>	<code>add-tag</code>	L'operazione di post-elaborazione che si desidera applicare all'oggetto S3. È possibile aggiungere uno o più tag utilizzando un singolo oggetto JSON di post-elaborazione per l'operazione <code>add-tag</code> .
<code>object-locator</code>	<code>schema-name</code> : il nome dello schema della tabella. <code>table-name</code> : il nome della tabella.	Il nome di ogni schema e tabella a cui si applica la regola. È possibile utilizzare il simbolo di percentuale "%" come carattere jolly per tutto o parte del valore di ciascun parametro <code>object-locator</code> . Pertanto, è

Parametro	Valori possibili	Description
		<p>possibile mettere in corrispondenza questi elementi:</p> <ul style="list-style-type: none">• Una singola tabella in un singolo schema• Una singola tabella in alcuni o in tutti gli schemi• Alcune o tutte le tabelle in un singolo schema• Alcune o tutte le tabelle in alcuni o in tutti gli schemi

Parametro	Valori possibili	Description
tag-set	<p>key: qualsiasi nome valido per un singolo tag.</p> <p>value: qualsiasi valore JSON valido per il tag.</p>	<p>I nomi e i valori per uno o più tag che si desidera impostare su ogni oggetto S3 creato che corrisponde a <code>object-locator</code> specificato. È possibile specificare fino a 10 coppie chiave-valore in un singolo oggetto parametro tag-set. Per ulteriori informazioni sull'applicazione di tag agli oggetti S3, consulta Tagging oggetti nella Guida per l'utente di Amazon Simple Storage Service.</p> <p>È anche possibile specificare un valore dinamico per tutto o parte del valore di entrambi i parametri key e value di un tag utilizzando <code>\${dyn-value}</code>. Qui, <code>\${dyn-value}</code> può essere <code>\${schema-name}</code> oppure <code>\${table-name}</code>. Pertanto, puoi inserire il nome dello schema o della tabella attualmente selezionati come tutto o parte del valore del parametro.</p> <div data-bbox="1003 1291 1507 1873"><p> Note</p><div data-bbox="1055 1407 1474 1873"><p> Important</p><p>Se inserisci un valore dinamico per il parametro key, è possibile generare i tag con nomi duplicati per un oggetto S3, a seconda del tipo di utilizzo. In questo</p></div></div>

Parametro	Valori possibili	Description
		<div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p>caso, solo una delle impostazioni di tag duplicati viene aggiunta all'oggetto.</p> </div>

Quando si specificano più tipi di regole post-processing per applicare tag a una selezione di oggetti S3, a ogni oggetto S3 vengono aggiunti tag utilizzando un solo oggetto tag-set da una regola di post-elaborazione. Il set di tag utilizzato per aggiungere tag a un determinato oggetto S3 è quello della regola di post-elaborazione il cui localizzatore di oggetti associato è maggiormente corrispondente a tale oggetto S3

Ad esempio, supponiamo che due regole di post-elaborazione identificano lo stesso oggetto S3. Supponi, inoltre, che il localizzatore di oggetti di una regola utilizza caratteri jolly e che localizzatore di oggetti dell'altra regola utilizza una corrispondenza esatta per identificare l'oggetto S3 (senza caratteri jolly). In questo caso, il set di tag associato alla regola di post-elaborazione con la corrispondenza esatta viene utilizzato per aggiungere i tag all'oggetto S3. Se più regole di post-elaborazione corrispondono a un determinato oggetto S3 in modo ugualmente valido, per aggiungere tag all'oggetto viene utilizzato il set di tag associato con la prima di tali regole di post-elaborazione.

Example Aggiunta di tag statici a un oggetto S3 creato per una singola tabella e un singolo schema

La seguente selezione e regole di post produzione aggiungono tre tag (tag_1, tag_2 e tag_3 con i corrispondenti valori statici value_1, value_2 e value_3) a un oggetto S3 creato. Questo oggetto S3 corrisponde ad una singola tabella nell'origine denominata STOCK con uno schema denominato aat2.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "5",
      "rule-name": "5",
      "object-locator": {
        "schema-name": "aat2",
        "table-name": "STOCK"
      }
    },
  ],
}
```



```
    },
    "rule-action": "include"
  },
  {
    "rule-type": "post-processing",
    "rule-id": "21",
    "rule-name": "21",
    "rule-action": "add-tag",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%",
    },
    "tag-set": [
      {
        "key": "dw-schema-name",
        "value": "${schema-name}"
      },
      {
        "key": "dw-schema-table",
        "value": "my_prefix_${table-name}"
      }
    ]
  },
  {
    "rule-type": "post-processing",
    "rule-id": "41",
    "rule-name": "41",
    "rule-action": "add-tag",
    "object-locator": {
      "schema-name": "aat",
      "table-name": "ITEM",
    },
    "tag-set": [
      {
        "key": "tag_1",
        "value": "value_1"
      },
      {
        "key": "tag_2",
        "value": "value_2"
      }
    ]
  }
]
```

```
}
```

La prima regola di post-elaborazione aggiunge due tag (`dw-schema-name` e `dw-schema-table`) con i valori dinamici corrispondenti (`${schema-name}` e `my_prefix_${table-name}`) per quasi tutti gli oggetti S3 creati nella destinazione. L'eccezione è l'oggetto S3 identificato e al quale sono applicati tag con la seconda regola di post-elaborazione. Pertanto, ogni oggetto S3 di destinazione identificato dal localizzatore di oggetti jolly viene creato con i tag che identificano lo schema e la tabella a cui corrisponde nell'origine.

La seconda regola di post-elaborazione aggiunge `tag_1` e `tag_2` con i corrispondenti valori statici `value_1` e `value_2` a un oggetto S3 creato identificato da un localizzatore di oggetti con corrispondenza esatta. Questo oggetto S3 creato corrisponde quindi alla singola tabella nell'origine denominata `ITEM` con uno schema denominato `aat`. A causa della corrispondenza esatta, questi tag sostituiscono qualsiasi tag in questo oggetto aggiunti dalla prima regola di post-elaborazione regola, che corrisponde agli oggetti S3 solo con i caratteri jolly.

Example Aggiunta di nomi di tag e valori dinamici a oggetti S3

L'esempio seguente presenta di due regole di selezione e una regola di post-elaborazione. Qui l'input dall'origine include solo la tabella `ITEM` nello schema `retail` o nello schema `wholesale`.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "retail",
        "table-name": "ITEM"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "wholesale",
        "table-name": "ITEM"
      },
    },
  ],
}
```

```

    "rule-action": "include"
  },
  {
    "rule-type": "post-processing",
    "rule-id": "21",
    "rule-name": "21",
    "rule-action": "add-tag",
    "object-locator": {
      "schema-name": "%",
      "table-name": "ITEM",
    },
    "tag-set": [
      {
        "key": "dw-schema-name",
        "value": "${schema-name}"
      },
      {
        "key": "dw-schema-table",
        "value": "my_prefix_ITEM"
      },
      {
        "key": "${schema-name}_ITEM_tag_1",
        "value": "value_1"
      },
      {
        "key": "${schema-name}_ITEM_tag_2",
        "value": "value_2"
      }
    ]
  }
]
}

```

Il set di tag della regola di post-elaborazione aggiunge due tag (dw-schema-name e dw-schema-table) a tutti gli oggetti S3 creati per la tabella ITEM nella destinazione. Il primo tag ha il valore dinamico "\${schema-name}" e il secondo tag ha un valore statico, "my_prefix_ITEM". Pertanto, ogni oggetto S3 di destinazione viene creato con i tag che identificano lo schema e la tabella a cui corrisponde nell'origine.

Inoltre, il set di tag aggiunge due ulteriori tag con nomi dinamici (\${schema-name}_ITEM_tag_1 e "\${schema-name}_ITEM_tag_2"). Questi hanno i corrispondenti valori statici value_1 e value_2. Pertanto, ognuno di questi tag viene denominato per lo schema attuale, retail o wholesale. In questo oggetto non è possibile creare un nome di tag dinamico duplicato, perché ogni

oggetto viene creato per un unico nome di schema univoco. Il nome dello schema viene utilizzato per creare un nome di tag univoco.

Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3

Puoi creare e utilizzare le chiavi AWS KMS personalizzate per crittografare gli oggetti di destinazione Amazon S3. Dopo aver creato una chiave KMS, è possibile utilizzarla per crittografare gli oggetti tramite uno dei seguenti approcci al momento della creazione dell'endpoint di destinazione S3:

- Utilizza le seguenti opzioni per gli oggetti di destinazione S3 (con l'impostazione predefinita per lo storage di file in formato .csv) quando esegui il comando `create-endpoint` utilizzando la AWS CLI.

```
--s3-settings '{"ServiceAccessRoleArn": "your-service-access-ARN",  
"CsvRowDelimiter": "\n", "CsvDelimiter": ",", "BucketFolder": "your-bucket-folder",  
"BucketName": "your-bucket-name", "EncryptionMode": "SSE_KMS",  
"ServerSideEncryptionKmsKeyId": "your-KMS-key-ARN"}'
```

Qui, *your-KMS-key-ARN* è l'ARN (Amazon Resource Name) per la chiave KMS. Per ulteriori informazioni, consulta [Utilizzo della crittografia dei dati, dei file parquet e della CDC sulla destinazione Amazon S3](#).

- Imposta l'attributo di connessione aggiuntivo `encryptionMode` sul valore `SSE_KMS` e l'attributo della connessione aggiuntiva `serverSideEncryptionKmsKeyId` per l'ARN per la chiave KMS. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#).

Per crittografare gli oggetti di destinazione Amazon S3 utilizzando una chiave KMS, è necessario disporre di un ruolo IAM che abbia le autorizzazioni per accedere al bucket Amazon S3. È possibile accedere a questo ruolo IAM in una policy (policy della chiave) collegata alla chiave di crittografia creata. È possibile farlo nella console IAM creando quanto segue:

- Una policy con le autorizzazioni ad accedere al bucket Amazon S3.
- Un ruolo IAM con la policy.
- Una chiave di crittografia KMS con una policy della chiave che fa riferimento a questo ruolo.

Nelle seguenti procedure viene descritto come procedere.

Per creare una policy IAM con le autorizzazioni ad accedere al bucket Amazon S3

1. Apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione seleziona Policies (Policy). Viene visualizzata la pagina Policies (Policy).
3. Scegli Create Policy (Crea policy). Viene visualizzata la pagina Create policy (Crea policy).
4. Scegli Service (Servizio), quindi S3. Viene visualizzato un elenco di autorizzazioni di azioni.
5. Scegli Expand all (Espandi tutto) per espandere l'elenco e scegli come minimo le seguenti autorizzazioni:
 - ListBucket
 - PutObject
 - DeleteObject

Scegli qualsiasi altra autorizzazione di cui hai bisogno, quindi scegli Collapse all (Comprimi tutto) per comprimere l'elenco.

6. Scegli Resources (Risorse) per specificare le risorse di cui desideri accedere. Come minimo, scegli Tutte le risorse per fornire l'accesso generale alle risorse Amazon S3.
7. Aggiungi tutte le altre condizioni o le autorizzazioni necessarie, quindi scegli Review policy (Esamina policy). Controlla i tuoi risultati nella pagina Review policy (Esamina policy).
8. Se le impostazioni sono quelle desiderate, immetti un nome per la policy (ad esempio, DMS-S3-endpoint-access) e qualsiasi ulteriore descrizione, quindi scegli Create policy (Crea policy). Viene visualizzata la pagina Policies (Policy) con un messaggio che indica che la policy è stata creata.
9. Ricerca e scegli il nome della policy nell'elenco Policies (Policy) Viene visualizzata la pagina Summary (Riepilogo) che visualizza il file JSON per la policy simile al seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:ListBucket",
```



```
        "s3:DeleteObject"
      ],
      "Resource": "*"
    }
  ]
}
```


È stata creata la nuova policy per accedere alle risorse Amazon S3 per la crittografia con un nome specificato, ad esempio `DMS-S3-endpoint-access`.

Per creare un ruolo IAM con questa policy

1. Nella console IAM scegli Ruoli nel riquadro di navigazione. Viene visualizzata la pagina dei dettagli Roles (Ruoli).
2. Selezionare Create role (Crea ruolo). Viene visualizzata la pagina Create role (Crea ruolo).
3. Dopo aver selezionato il servizio AWS come entità attendibile, scegli DMS come servizio per l'utilizzo del ruolo IAM.
4. Scegli Successivo: Autorizzazioni. Viene visualizzata la vista Allega policy di autorizzazione nella pagina Crea ruolo.
5. Individuare e selezionare la policy IAM per il ruolo IAM creato nella procedura precedente (`DMS-S3-endpoint-access`).
6. Scegliere Successivo: Tag. Viene visualizzata la vista Aggiungi tag nella pagina Crea ruolo. Qui è possibile aggiungere i tag desiderati.
7. Seleziona Successivo: Revisione. Viene visualizzata la vista Verifica nella pagina Crea ruolo. Qui è possibile verificare i risultati.
8. Se le impostazioni sono quelle desiderate, immetti un nome per il ruolo (richiesto, ad esempio, `DMS-S3-endpoint-access-role`) e qualsiasi ulteriore descrizione, quindi scegli Create role (Crea ruolo). Viene visualizzata la pagina dei dettagli Roles (Ruoli) con un messaggio che indica che il ruolo è stato creato.


È stato creato il nuova ruolo per accedere alle risorse Amazon S3 per la crittografia con un nome specificato, ad esempio `DMS-S3-endpoint-access-role`.

Per creare una chiave di crittografia KMS con una policy della chiave che faccia riferimento al ruolo IAM

 Note

Per ulteriori informazioni sul funzionamento di AWS DMS con le chiavi di crittografia AWS KMS, consulta [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#).

1. Accedi alla AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'indirizzo <https://console.aws.amazon.com/kms>.
2. Per modificare la Regione AWS, utilizza il Selettore di regione nell'angolo in alto a destra della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegliere Create key (Crea chiave). Verrà visualizzata la pagina Configure key (Configura chiave).
5. Alla voce Key type (Tipo di chiave), scegliere Symmetric (Simmetrica).

 Note

È possibile creare solo una chiave simmetrica, poiché tutti i servizi AWS, ad esempio Amazon S3, funzionano solo con chiavi di crittografia simmetriche.

6. Scegliere Advanced Options (Opzioni avanzate). Alla voce Key material origin (Origine del materiale della chiave), assicurarsi che sia selezionata la voce KMS quindi scegliere Next (Avanti). Verrà visualizzata la pagina Add labels (Aggiungi etichette).
7. Alla voce Create alias and description (Crea alias e descrizione), inserire un alias per la chiave (ad esempio `DMS-S3-endpoint-encryption-key`) e qualsiasi descrizione aggiuntiva.
8. Alla voce Tag, aggiungere tutti i tag desiderati per identificare la chiave e monitorarne l'utilizzo, quindi scegliere Next (Avanti). Verrà visualizzata la pagina Define key administrative permissions (Definisci autorizzazioni amministrative della chiave) che mostra un elenco di utenti e ruoli tra cui è possibile scegliere.
9. Aggiungi gli utenti e i ruoli che desideri gestiscano la chiave. Assicurati che questi utenti e ruoli dispongano delle autorizzazioni necessarie per gestire la chiave.

10. Alla voce Key deletion (Eliminazione chiave), scegliere se gli amministratori della chiave possono eliminarla, quindi scegliere Next (Avanti). Verrà visualizzata la pagina Define key usage permissions (Definisci autorizzazioni di utilizzo della chiave) che mostra un elenco aggiuntivo di utenti e ruoli tra cui è possibile scegliere.
11. Per Questo account scegli tra gli utenti disponibili quelli che dovranno eseguire operazioni di crittografia sulle destinazioni Amazon S3. Scegli in Ruoli il ruolo creato in precedenza per abilitare l'accesso alla crittografia degli oggetti di destinazione Amazon S3, ad esempio `DMS-S3-endpoint-access-role`.
12. Se desideri aggiungere altri account non elencati affinché abbiano lo stesso accesso, per Altri account AWS, scegli Aggiungi un altro account AWS, quindi seleziona Successivo. Verrà visualizzata la pagina Review and edit key policy (Rivedi e modifica la policy della chiave) che mostra il JSON associato alla policy della chiave, che è possibile rivedere e modificare digitando all'interno del testo esistente. Qui è possibile visualizzare il punto in cui la policy della chiave fa riferimento al ruolo e agli utenti (ad esempio, `Admin` e `User1`) selezionati nella fase precedente. È anche possibile visualizzare le diverse operazioni sulla chiave permesse alle diverse entità (utenti e ruoli), come mostrato nel seguente esempio.

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:role/Admin"
        ]
      },
    },
  ],
}
```

```

    "Action": [
      "kms:Create*",
      "kms:Describe*",
      "kms:Enable*",
      "kms:List*",
      "kms:Put*",
      "kms:Update*",
      "kms:Revoke*",
      "kms:Disable*",
      "kms:Get*",
      "kms>Delete*",
      "kms:TagResource",
      "kms:UntagResource",
      "kms:ScheduleKeyDeletion",
      "kms:CancelKeyDeletion"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/DMS-S3-endpoint-access-role",
        "arn:aws:iam::111122223333:role/Admin",
        "arn:aws:iam::111122223333:role/User1"
      ]
    },
    "Action": [
      "kms:Encrypt",
      "kms:Decrypt",
      "kms:ReEncrypt*",
      "kms:GenerateDataKey*",
      "kms:DescribeKey"
    ],
    "Resource": "*"
  },
  {
    "Sid": "Allow attachment of persistent resources",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/DMS-S3-endpoint-access-role",
        "arn:aws:iam::111122223333:role/Admin",

```

```
        "arn:aws:iam::111122223333:role/User1"
    ],
    },
    "Action": [
        "kms:CreateGrant",
        "kms:ListGrants",
        "kms:RevokeGrant"
    ],
    "Resource": "*",
    "Condition": {
        "Bool": {
            "kms:GrantIsForAWSResource": true
        }
    }
}
]
```

13. Scegli Fine. Viene visualizzata la pagina Chiavi di crittografia con un messaggio che indica che la chiave KMS è stata creata.

È stata creata una nuova chiave KMS con un alias specificato (ad esempio, `DMS-S3-endpoint-encryption-key`). Questa chiave consente ad AWS DMS di crittografare gli oggetti di destinazione Amazon S3.

Utilizzo del partizionamento delle cartelle in base alla data

AWS DMS supporta le partizioni delle cartelle S3 in base alla data di commit della transazione quando utilizzi Amazon S3 come endpoint di destinazione. Con il partizionamento delle cartelle in base alla data puoi scrivere dati da un'unica tabella di origine in una struttura di cartelle con la gerarchia basata sulla data di un bucket S3. Il partizionamento delle cartelle eseguito durante la creazione di un endpoint di destinazione S3 offre i seguenti vantaggi:

- Migliore gestione degli oggetti S3
- Limite della dimensione di ogni cartella S3
- Ottimizzazione delle query sul data lake o altre operazioni successive

Il partizionamento delle cartelle in base alla data si abilita quando si crea un endpoint di destinazione S3. È possibile abilitarlo quando si migrano i dati esistenti e si replicano le modifiche in corso

(pieno carico e CDC) oppure si replicano solo le modifiche ai dati (sola CDC). Utilizza le seguenti impostazioni dell'endpoint di destinazione:

- `DatePartitionEnabled`: specifica il partizionamento in base alla data. Imposta questa opzione booleana su `true` per eseguire il partizionamento delle cartelle del bucket S3 in base alla data di commit delle transazioni.

Non è possibile utilizzare questa impostazione con `PreserveTransactions` o `CdcPath`.

Il valore predefinito è `false`.

- `DatePartitionSequence`: identifica la sequenza del formato della data da utilizzare durante il partizionamento delle cartelle. Imposta questa opzione ENUM su `YYYYMMDD`, `YYYYMMDDHH`, `YYYYMM`, `MMYYYYDD` o `DDMMYYYY`. Il valore predefinito è `YYYYMMDD`. Utilizza questa impostazione quando `DatePartitionEnabled` è impostato su `true`.
- `DatePartitionDelimiter`: specifica un delimitatore di separazione della data da utilizzare durante il partizionamento delle cartelle. Imposta questa opzione ENUM su `SLASH`, `DASH`, `UNDERSCORE` o `NONE`. Il valore predefinito è `SLASH`. Utilizza questa impostazione quando `DatePartitionEnabled` è impostato su `true`.

L'esempio seguente mostra come abilitare il partizionamento delle cartelle in base alla data, con valori predefiniti per la sequenza di partizione dei dati e il delimitatore. Utilizza l'opzione `--s3-settings '{json-settings}'` del comando `AWS CLI.create-endpoint`.

```
--s3-settings '{"DatePartitionEnabled": true, "DatePartitionSequence":  
"YYYYMMDD", "DatePartitionDelimiter": "SLASH"}
```

Caricamento parallelo di origini partizionate quando si utilizza Amazon S3 come destinazione per AWS DMS

Puoi configurare un pieno carico parallelo di origini dati partizionate in destinazioni Amazon S3. Questo approccio migliora i tempi di caricamento per la migrazione dei dati partizionati dai motori di database di origine supportati alla destinazione S3. Per migliorare i tempi di caricamento dei dati di origine partizionati, crei sottocartelle di destinazione S3 mappate alle partizioni di ogni tabella del database di origine. Queste sottocartelle associate alle partizioni consentono ad AWS DMS di eseguire processi paralleli per popolare ogni sottocartella sulla destinazione.

Per configurare un pieno carico parallelo di una destinazione S3, S3 supporta tre tipi di regole `parallel-load` per la regola `table-settings` di mappatura delle tabelle:

- `partitions-auto`
- `partitions-list`
- `ranges`

Per ulteriori informazioni su questi tipi di regole di caricamento parallelo, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Per i tipi di regole `partitions-auto` e `partitions-list`, AWS DMS utilizza ogni nome di partizione dell'endpoint di origine per identificare la struttura della sottocartella di destinazione, come segue.

```
bucket_name/bucket_folder/database_schema_name/table_name/partition_name/  
LOADseq_num.csv
```

Qui, il percorso della sottocartella in cui i dati vengono migrati e archiviati sulla destinazione S3 include una sottocartella `partition_name` aggiuntiva che corrisponde a una partizione di origine con lo stesso nome. Questa sottocartella `partition_name` archivia uno o più file `LOADseq_num.csv` contenenti i dati migrati dalla partizione di origine specificata. `seq_num` è il suffisso del numero di sequenza nel nome del file.csv, ad esempio `00000001` nel file.csv denominato `LOAD00000001.csv`.

Tuttavia, alcuni motori di database, come MongoDB e DocumentDB, non supportano il concetto di partizione. Per questi motori di database, AWS DMS aggiunge l'indice del segmento di origine in esecuzione come prefisso al nome del file.csv di destinazione, come segue.

```
.../database_schema_name/table_name/SEGMENT1_LOAD00000001.csv  
.../database_schema_name/table_name/SEGMENT1_LOAD00000002.csv  
...  
.../database_schema_name/table_name/SEGMENT2_LOAD00000009.csv  
.../database_schema_name/table_name/SEGMENT3_LOAD0000000A.csv
```

Qui, i file `SEGMENT1_LOAD00000001.csv` e `SEGMENT1_LOAD00000002.csv` sono denominati con lo stesso prefisso dell'indice del segmento di origine in esecuzione `SEGMENT1`. Sono denominati così perché i dati di origine migrati per questi due file .csv sono associati allo stesso indice del segmento di origine in esecuzione. I dati migrati archiviati in ciascuno dei file `SEGMENT2_LOAD00000009.csv`

e `SEGMENT3_LOAD0000000A.csv` di destinazione sono associati a diversi indici dei segmenti di origine in esecuzione. Ogni file ha il nome preceduto dal nome dell'indice del segmento in esecuzione `SEGMENT2` e `SEGMENT3`.

Per il tipo di caricamento parallelo `ranges`, è possibile definire i nomi e i valori delle colonne utilizzando le impostazioni `columns` e `boundaries` delle regole `table-settings`. Con queste regole puoi specificare le partizioni corrispondenti ai nomi dei segmenti, come segue.

```
"parallel-load": {
  "type": "ranges",
  "columns": [
    "region",
    "sale"
  ],
  "boundaries": [
    [
      "NORTH",
      "1000"
    ],
    [
      "WEST",
      "3000"
    ]
  ],
  "segment-names": [
    "custom_segment1",
    "custom_segment2",
    "custom_segment3"
  ]
}
```

Qui, l'impostazione `segment-names` definisce i nomi di tre partizioni per migrare i dati in parallelo sulla destinazione S3. I dati migrati vengono caricati in parallelo e archiviati in file.csv nelle sottocartelle delle partizioni nell'ordine, come indicato di seguito.

```
.../database_schema_name/table_name/custom_segment1/LOAD[00000001...].csv
.../database_schema_name/table_name/custom_segment2/LOAD[00000001...].csv
.../database_schema_name/table_name/custom_segment3/LOAD[00000001...].csv
```


AWS DMS archivia una serie di file .csv in ciascuna delle tre sottocartelle di partizione. La serie di file .csv in ogni sottocartella di partizione viene denominata in modo incrementale a partire da LOAD00000001.csv fino alla migrazione di tutti i dati.

In alcuni casi, puoi non denominare in modo esplicito le sottocartelle di partizione per il tipo di caricamento parallelo ranges utilizzando l'impostazione segment-names. In questi casi, AWS DMS per impostazione predefinita crea ogni serie di file .csv nella relativa sottocartella *table_name*. Qui, AWS DMS antepone ai nomi di file di ogni serie di file .csv il nome dell'indice del segmento di origine in esecuzione, come segue.

```
.../database_schema_name/table_name/SEGMENT1_LOAD[00000001...].csv
.../database_schema_name/table_name/SEGMENT2_LOAD[00000001...].csv
.../database_schema_name/table_name/SEGMENT3_LOAD[00000001...].csv
...
.../database_schema_name/table_name/SEGMENTZ_LOAD[00000001...].csv
```

Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare la destinazione Amazon S3 in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando create-endpoint nella [AWS CLI](#), con la sintassi JSON --s3-settings '{"EndpointSetting": "value", ...}'.


La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Amazon S3 come destinazione.


Opzione	Descrizione
CsvNullValue	Un parametro facoltativo che specifica come AWS DMS considera i valori null. Durante la gestione del valore null, puoi utilizzare questo parametro per passare una stringa definita dall'utente come null durante la scrittura nella destinazione. Ad esempio, quando le colonne di destinazione sono nullable, puoi utilizzare questa opzione per distinguere tra il valore di stringa vuoto e il valore null. Quindi, se imposti questo valore di parametro sulla stringa vuota (" " o ""), AWS DMS la considera come valore null anziché NULL.


Opzione	Descrizione
	<p>Valore predefinito: NULL</p> <p>Valori validi: qualsiasi stringa valida</p> <p>Esempio: <code>--s3-settings '{"CsvNullValue": " "}'</code></p>
AddColumnName	<p>Un parametro facoltativo che, quando impostato a <code>true</code> o a <code>y</code>, è possibile utilizzare per aggiungere informazioni al nome di colonna nel file <code>.csv</code> di output.</p> <p>Non è possibile utilizzare questo parametro con <code>PreserveTransactions</code> o <code>CdcPath</code>.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"AddColumnName": true}'</code></p>
AddTrailingPaddingCharacter	<p>Usa l'impostazione dell'endpoint di destinazione S3 <code>AddTrailingPaddingCharacter</code> per aggiungere il riempimento ai dati delle stringhe. Il valore predefinito è <code>false</code>.</p> <p>Tipo: Booleano</p> <p>Esempio: <code>--s3-settings '{"AddTrailingPaddingCharacter": true}'</code></p>
BucketFolder	<p>Parametro opzionale per impostare un nome di cartella nel bucket S3. Se forniti, gli oggetti di destinazione vengono creati come file <code>.csv</code> o <code>.parquet</code> nel percorso <code>BucketFolder /schema_name /table_name /</code>. Se questo parametro non viene specificato, viene utilizzato il percorso <code>schema_name /table_name /</code>.</p> <p>Esempio: <code>--s3-settings '{"BucketFolder": "testFolder"}</code></p>


Opzione	Descrizione
BucketName	<p>Il nome del bucket S3 in cui gli oggetti di destinazione S3 vengono creati come file .csv o .parquet.</p> <p>Esempio: <code>--s3-settings '{"BucketName": "buckettest"}</code></p>
CannedAclForObjects	<p>Un valore che consente a AWS DMS di specificare una lista di controllo accessi (ACL) predefinita per gli oggetti creati nel bucket S3 come file .csv o .parquet. Per ulteriori informazioni sulle ACL predefinite di Amazon S3, consulta ACL predefinita nella Guida per gli sviluppatori di Amazon S3.</p> <p>Valore predefinito: NONE</p> <p>I valori validi per questo attributo sono: NONE; PRIVATE; PUBLIC_READ; PUBLIC_READ_WRITE; AUTHENTICATED_READ; AWS_EXEC_READ; BUCKET_OWNER_READ; BUCKET_OWNER_FULL_CONTROL.</p> <p>Esempio: <code>--s3-settings '{"CannedAclForObjects": "PUBLIC_READ"}</code></p>

Opzione	Descrizione
CdcInsertsOnly	<p>Un parametro facoltativo durante il caricamento dell'acquisizione delle modifiche dei dati (Change Data Capture, CDC) per scrivere solo le operazioni INSERT nei file di output con valori separati da virgole (.csv) o file di storage colonnare (.parquet). Per impostazione predefinita (l'impostazione <code>false</code>), il primo campo in un record .csv o .parquet record contiene la lettera I (INSERT, inserisci), U (UPDATE, aggiorna) o D (DELETE, elimina). Questa lettera indica se la riga è stata inserita, aggiornata o eliminata nel database di origine di un caricamento CDC sulla destinazione. Se <code>cdcInsertsOnly</code> è impostato su <code>true</code> o <code>y</code>, solo le istruzioni INSERT dal database di origine vengono migrate nel file .csv o .parquet.</p> <p>Solo per il formato .csv, la modalità di registrazione di queste istruzioni INSERT varia a seconda del valore di <code>IncludeOpForFullLoad</code>. Se <code>IncludeOpForFullLoad</code> è impostato su <code>true</code>, il primo campo di ogni record CDC è impostato su I per confermare l'operazione INSERT all'origine. Se <code>IncludeOpForFullLoad</code> è impostato su <code>false</code>, ogni record CDC viene scritto senza un primo campo per confermare l'operazione INSERT all'origine. Per ulteriori informazioni sul funzionamento congiunto di questi parametri, consulta Indicazione delle operazioni del DB di origine nei dati S3 migrati.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"CdcInsertsOnly": true}'</code></p>


Opzione	Descrizione
<code>CdcInsertsAndUpdates</code>	<p>Permette a una Change Data Capture (CDC) di scrivere le operazioni INSERT e UPDATE nei file di output con estensione .csv o .parquet (memorizzazione in formato colonnare). L'impostazione predefinita è <code>false</code>, ma quando <code>cdcInsertsAndUpdates</code> è impostato a <code>true</code> o <code>y</code>, le operazioni di INSERT e UPDATE provenienti dal database di origine vengono migrate verso i file con estensione .csv o .parquet.</p> <p>Solo nel caso di file in formato CSV, la registrazione di tali operazioni di INSERT e UPDATE dipende dal valore del parametro <code>includeOpForFullLoad</code>. Se <code>includeOpForFullLoad</code> è impostato su <code>true</code>, il primo campo di ogni record CDC viene impostato su <code>I</code> o <code>U</code> per indicare le operazioni INSERT e UPDATE all'origine. Ma se <code>includeOpForFullLoad</code> è impostato su <code>false</code>, i record CDC vengono scritti senza un'indicazione dell'operazione INSERT o UPDATE all'origine.</p> <p>Per ulteriori informazioni sul funzionamento congiunto di questi parametri, consulta Indicazione delle operazioni del DB di origine nei dati S3 migrati.</p> <div data-bbox="472 1087 1507 1451"><p> Note</p><p><code>CdcInsertsOnly</code> e <code>cdcInsertsAndUpdates</code> non possono essere entrambi impostati su <code>true</code> per lo stesso endpoint. Imposta uno tra <code>cdcInsertsAndUpdates</code> o <code>cdcInsertsOnly</code> su <code>true</code> per lo stesso endpoint, ma non entrambi.</p></div> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"CdcInsertsAndUpdates": true}'</code></p>

Opzione	Descrizione
CdcPath	<p>Specifica il percorso della cartella dei file CDC. Per un'origine S3, questa impostazione è necessaria se un'attività acquisisce i dati modificati; altrimenti, è facoltativa. Se è impostato CdcPath, DMS legge i file CDC da questo percorso e replica le modifiche ai dati nell'endpoint di destinazione. Se PreserveTransactions è impostato su true per una destinazione S3, DMS verifica che questo parametro sia impostato su un percorso di cartella nella destinazione S3 in cui DMS può salvare l'ordine di transazione per il caricamento CDC. DMS crea questo percorso della cartella CDC nella directory di lavoro di destinazione S3 o nella posizione di destinazione S3 specificata da BucketFolder e BucketName .</p> <p>Non è possibile utilizzare questo parametro con DatePartitionEnabled o AddColumnName .</p> <p>Tipo: string</p> <p>Ad esempio, se specifichi CdcPath come MyChangedData e BucketName come MyTargetBucket senza specificare BucketFolder , DMS crea il seguente percorso della cartella CDC: MyTargetBucket/MyChangedData .</p> <p>Se specifichi lo stesso CdcPath, quindi specifichi BucketName come MyTargetBucket e BucketFolder come MyTargetData , DMS crea il seguente percorso della cartella CDC: MyTargetBucket/MyTargetData/MyChangedData .</p> <div data-bbox="472 1388 1507 1843"><p> Note</p><p>Questa impostazione è supportata in AWS DMS 3.4.2 e versioni successive.</p><p>Durante l'acquisizione delle modifiche ai dati nell'ordine delle transazioni, DMS memorizza sempre le modifiche alle righe nei file.csv indipendentemente dal valore dell'impostazione DataFormat S3 della destinazione. DMS non salva le modifiche ai dati nell'ordine delle transazioni utilizzando i file .parquet.</p></div>

Opzione	Descrizione
<code>CdcMaxBatchInterval</code>	<p>Condizione della lunghezza massima dell'intervallo, definita in secondi, per l'output di un file in Amazon S3.</p> <p>Valore predefinito: 60 secondi</p> <p>Quando <code>CdcMaxBatchInterval</code> viene specificato insieme a <code>CdcMinFileSize</code>, la scrittura del file viene attivata dalla condizione di parametro che viene soddisfatta per prima.</p>
<code>CdcMinFileSize</code>	<p>Condizione della dimensione minima del file, espressa in kilobyte, per l'output di un file in Amazon S3.</p> <p>Valore predefinito: 32000 KB</p> <p>Quando <code>CdcMinFileSize</code> viene specificato insieme a <code>CdcMaxBatchInterval</code>, la scrittura del file viene attivata dalla condizione di parametro che viene soddisfatta per prima.</p>
<code>PreserveTransactions</code>	<p>Se questa opzione è impostata su <code>true</code>, DMS salva l'ordine di transazione per l'acquisizione dei dati di modifica (CDC) nella destinazione Amazon S3 specificata da <code>CdcPath</code>.</p> <p>Non è possibile utilizzare questo parametro con <code>DatePartitionEnabled</code> o <code>AddColumnName</code>.</p> <p>Tipo: Booleano</p> <p>Durante l'acquisizione delle modifiche ai dati nell'ordine delle transazioni, DMS memorizza sempre le modifiche alle righe nei file.csv indipendentemente dal valore dell'impostazione <code>DataFormat S3</code> della destinazione. DMS non salva le modifiche ai dati nell'ordine delle transazioni utilizzando i file .parquet.</p> <div data-bbox="472 1646 1507 1864"><p> Note</p><p>Questa impostazione è supportata in AWS DMS 3.4.2 e versioni successive.</p></div>

Opzione	Descrizione
<p><code>IncludeOpForFullLoad</code></p>	<p>Un parametro facoltativo durante il caricamento completo per scrivere le operazioni INSERT nei file di output con i valori separati da virgola (.csv).</p> <p>Per il caricamento completo, i record possono solo essere inseriti. Per impostazione predefinita (impostazione <code>false</code>), le informazioni non vengono registrate in questi file di output per un caricamento completo per indicare che le righe sono state inserite nel database di origine. Se <code>IncludeOpForFullLoad</code> è impostato su <code>true</code> o <code>y</code>, l'istruzione INSERT viene registrata come annotazione I nel primo campo del file .csv.</p> <div data-bbox="472 716 1507 1081" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>Questo parametro viene utilizzato insieme a <code>CdcInsertsOnly</code> o <code>CdcInsertsAndUpdates</code> solo per l'output verso file .csv. Per ulteriori informazioni sul funzionamento congiunto di questi parametri, consulta Indicazione delle operazioni del DB di origine nei dati S3 migrati.</p> </div> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"IncludeOpForFullLoad": true}'</code></p>
<p><code>CompressionType</code></p>	<p>Parametro facoltativo che se impostato a GZIP attiva l'utilizzo di GZIP per comprimere i file .csv o .parquet di destinazione. Quando questo parametro è impostato come predefinito, i file di dati non vengono compressi.</p> <p>Valore predefinito: <code>NONE</code></p> <p>Valori validi: <code>GZIP</code> o <code>NONE</code></p> <p>Esempio: <code>--s3-settings '{"CompressionType": "GZIP"}</code></p>

Opzione	Descrizione
<code>CsvDelimiter</code>	<p>Delimitatore utilizzato per separare le colonne nei file di origine .csv. L'impostazione predefinita è una virgola (,).</p> <p>Esempio: <code>--s3-settings '{"CsvDelimiter": ","}'</code></p>
<code>CsvRowDelimiter</code>	<p>Delimitatore utilizzato per separare le righe nei file di origine .csv. L'impostazione predefinita è una nuova riga (\n).</p> <p>Esempio: <code>--s3-settings '{"CsvRowDelimiter": "\n"}'</code></p>
<code>MaxFileSize</code>	<p>Un valore che specifica le dimensioni massime (in KB) di qualsiasi file .csv da creare durante la migrazione a una destinazione S3 durante il caricamento completo.</p> <p>Valore predefinito: 1.048.576 KB (1 GB)</p> <p>Valori validi: 1-1.048.576</p> <p>Esempio: <code>--s3-settings '{"MaxFileSize": 512}'</code></p>
<code>Rfc4180</code>	<p>Un parametro facoltativo utilizzato per impostare il comportamento di conformità a RFC per i dati migrati ad Amazon S3 utilizzando solo il formato di file .csv. Quando questo valore è impostato su <code>true</code> o su <code>y</code> con l'utilizzo di Amazon S3 come destinazione, se i dati contengono virgolette, virgole o caratteri di riga nuova, AWS DMS racchiude l'intera colonna con un'ulteriore coppia di virgolette doppie ("). Ogni virgoletta all'interno dei dati viene ripetuta due volte. Questa formattazione è conforme a RFC 4180.</p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"Rfc4180": false}'</code></p>


Opzione	Descrizione
EncryptionMode	<p>Le modalità di crittografia lato server desiderata per crittografare i file degli oggetti .csv o .parquet copiati in S3. I valori validi sono SSE_S3 (crittografia lato server S3) o SSE_KMS (crittografia chiave KMS). Se scegli SSE_KMS, imposta il parametro <code>ServerSideEncryptionKmsKeyId</code> al valore dell'ARN (Amazon Resource Name) della chiave KMS da utilizzare per la crittografia.</p> <div data-bbox="472 541 1507 907" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p> Note</p> <p>È inoltre possibile utilizzare il comando CLI <code>modify-endpoint</code> per modificare il valore dell'attributo <code>EncryptionMode</code> per un endpoint esistente da SSE_KMS a SSE_S3. Tuttavia non puoi modificare il valore di <code>EncryptionMode</code> da SSE_S3 a SSE_KMS.</p> </div> <p>Valore predefinito: SSE_S3</p> <p>Valori validi: SSE_S3 o SSE_KMS</p> <p>Esempio: <code>--s3-settings '{"EncryptionMode": SSE_S3}'</code></p>
ServerSideEncryptionKmsKeyId	<p>Se hai impostato <code>EncryptionMode</code> su SSE_KMS, configura questo parametro sul nome della risorsa Amazon (ARN) della chiave KMS. Puoi trovare l'ARN selezionando l'alias della chiave nell'elenco delle chiavi AWS KMS create per l'account. Quando crei la chiave, è necessario associare alla chiave KMS policy e ruoli specifici. Per ulteriori informazioni, consulta Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3.</p> <p>Esempio: <code>--s3-settings '{"ServerSideEncryptionKmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/11a1a1a1-aaaa-9999-abab-2bbbbbb222a2"}'</code></p>

Opzione	Descrizione
DataFormat	<p>Il formato di output per i file che AWS DMS utilizza per creare oggetti S3. Per le destinazioni Amazon S3, AWS DMS supporta i file .csv o .parquet. Il file .parquet hanno un formato binario di storage colonnare con opzioni di compressione efficaci e prestazioni delle query più veloci. Per ulteriori informazioni sui file .parquet, consulta https://parquet.apache.org/.</p> <p>Valore predefinito: csv</p> <p>Valori validi: csv o parquet</p> <p>Esempio: <code>--s3-settings '{"DataFormat": "parquet"}'</code></p>
EncodingType	<p>Il tipo di codifica Parquet. Le opzioni del tipo di codifica includono le seguenti:</p> <ul style="list-style-type: none">• <code>rle-dictionary</code> : questa codifica di dizionario utilizza una combinazione di creazione di pacchetti di bit e di codifica runlength per un'archiviazione più efficiente dei valori ripetuti.• <code>plain</code>: nessuna codifica.• <code>plain-dictionary</code> : questa codifica di dizionario crea un dizionario di valori riscontrati in una determinata colonna. Il dizionario è archiviato in una pagina del dizionario per ogni blocco di colonne. <p>Valore predefinito: <code>rle-dictionary</code></p> <p>Valori validi: <code>rle-dictionary</code> , <code>plain</code> o <code>plain-dictionary</code></p> <p>Esempio: <code>--s3-settings '{"EncodingType": "plain-dictionary"}'</code></p>

Opzione	Descrizione
DictPageSizeLimit	<p>La dimensione massima consentita, in byte, per una pagina del dizionario o in un file .parquet. Se una pagina del dizionario supera questo valore, la pagina utilizza la codifica normale.</p> <p>Valore predefinito: 1.024.000 (1 MB)</p> <p>Valori validi: qualsiasi valore intero valido</p> <p>Esempio: <code>--s3-settings '{"DictPageSizeLimit": 2,048,000}'</code></p>
RowGroupLength	<p>Il numero di righe in un gruppo di righe di un file .parquet.</p> <p>Valore predefinito: 10.024 (10 KB)</p> <p>Valori validi: qualsiasi intero valido</p> <p>Esempio: <code>--s3-settings '{"RowGroupLength": 20,048}'</code></p>
DataPageSize	<p>La dimensione massima consentita, in byte, per una pagina di dati in un file .parquet.</p> <p>Valore predefinito: 1.024.000 (1 MB)</p> <p>Valori validi: qualsiasi intero valido</p> <p>Esempio: <code>--s3-settings '{"DataPageSize": 2,048,000}'</code></p>
ParquetVersion	<p>La versione del formato del file .parquet.</p> <p>Valore predefinito: PARQUET_1_0</p> <p>Valori validi: PARQUET_1_0 o PARQUET_2_0</p> <p>Esempio: <code>--s3-settings '{"ParquetVersion": "PARQUET_2_0"}</code></p>

Opzione	Descrizione
<p><code>EnableStatistics</code></p>	<p>Impostare a <code>true</code> o <code>y</code> per abilitare le statistiche sulle pagine e sui gruppi di righe del file <code>.parquet</code>.</p> <p>Valore predefinito: <code>true</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"EnableStatistics": false}'</code></p>
<p><code>TimestampColumnName</code></p>	<p>Un parametro facoltativo per includere una colonna timestamp nei dati dell'endpoint di destinazione S3.</p> <p>AWS DMS include una colonna <code>STRING</code> aggiuntiva nel <code>.csv</code> o <code>.parquet</code> dei file di oggetti dei dati migrati quando <code>TimestampColumnName</code> viene impostato su un valore non vuoto.</p> <p>Per un caricamento completo, ogni riga della colonna timestamp contiene il timestamp del trasferimento dei dati dall'origine alla destinazione tramite DMS.</p> <p>Per un caricamento CDC, ogni riga della colonna timestamp contiene il timestamp per il commit di quella riga nel database di origine.</p> <p>Il formato di stringa per questo valore della colonna timestamp è <code>yyyy-MM-dd HH:mm:ss.SSSSSS</code> . Per impostazione predefinita, la precisione di questo valore è in microsecondi. Per un carico CDC, l'arrotondamento della precisione dipende dal timestamp di commit supportato da DMS per il database di origine.</p> <p>Quando il parametro <code>AddColumnName</code> è impostato su <code>true</code>, DMS include anche il nome per la colonna timestamp impostata con il valore non vuoto <code>TimestampColumnName</code> .</p> <p>Esempio: <code>--s3-settings '{"TimestampColumnName": "TIMESTAMP"}'</code></p>

Opzione	Descrizione
UseTaskStartTimeForFullLoadTimestamp	<p>Se impostato su <code>true</code>, questo parametro utilizza l'ora di inizio dell'attività come valore della colonna <code>timestamp</code> anziché l'ora in cui i dati vengono scritti nella destinazione. Per il caricamento completo, quando <code>UseTaskStartTimeForFullLoadTimestamp</code> è impostato su <code>true</code>, ogni riga della colonna <code>timestamp</code> contiene l'ora di inizio dell'attività. Per i caricamenti CDC, ogni riga della colonna <code>timestamp</code> contiene l'orario di esecuzione del commit della transazione.</p> <p>Quando <code>UseTaskStartTimeForFullLoadTimestamp</code> è impostato su <code>false</code>, il timestamp del caricamento completo nella colonna <code>timestamp</code> aumenta con l'ora di arrivo dei dati a destinazione.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code></p> <p>Esempio: <code>--s3-settings '{"UseTaskStartTimeForFullLoadTimestamp": true}'</code></p> <p><code>UseTaskStartTimeForFullLoadTimestamp: true</code> consente di rendere ordinabile la destinazione <code>S3 TimestampColumnName</code> per un pieno carico con <code>TimestampColumnName</code> per un carico CDC.</p>

Opzione	Descrizione
ParquetTimestampInMillisecond	<p>Un parametro opzionale che specifica la precisione di qualsiasi valore della colonna <code>TIMESTAMP</code> scritto su un file oggetto S3 in formato <code>.parquet</code>.</p> <p>Quando questo attributo è impostato su <code>true</code> o <code>y</code>, AWS DMS scrive tutte le colonne <code>TIMESTAMP</code> in un file in formato <code>.parquet</code> con la precisione e in millisecondi. In caso contrario, DMS le scrive con la precisione del microsecondo.</p> <p>Al momento, Amazon Athena e AWS Glue possono gestire solo la precisione in millisecondi per i valori <code>TIMESTAMP</code>. Imposta questo attributo su <code>true</code> per file di oggetti dell'endpoint S3 nel formato <code>.parquet</code> solo se si prevede di eseguire query o elaborare i dati con Athena o AWS Glue.</p> <div data-bbox="472 894 1507 1335" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> Note</p><ul style="list-style-type: none">• AWS DMS scrive qualsiasi valore della colonna <code>TIMESTAMP</code> scritto su un file S3 in formato <code>.csv</code> con la precisione dei microsecondi.• L'impostazione di questo attributo non ha effetto sul formato della stringa del valore della colonna <code>timestamp</code> inserito impostando l'attributo <code>TimestampColumnName</code>.</div> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code>, <code>y</code>, <code>n</code></p> <p>Esempio: <code>--s3-settings '{"ParquetTimestampInMillisecond": true}'</code></p>

Opzione	Descrizione
GlueCatalogGeneration	<p>Per generare un AWS Glue Data Catalog, configura questa impostazione dell'endpoint su <code>true</code>.</p> <p>Valore predefinito: <code>false</code></p> <p>Valori validi: <code>true</code>, <code>false</code></p> <p>Esempio: <code>--s3-settings '{"GlueCatalogGeneration": true}'</code></p> <p>Nota: non utilizzare <code>GlueCatalogGeneration</code> con <code>PreserveTransactions</code> e <code>CdcPath</code>.</p>

Utilizzo di AWS Glue Data Catalog con una destinazione Amazon S3 per AWS DMS

AWS Glue è un servizio che fornisce modi semplici per classificare i dati ed è costituito da un repository di metadati noto come AWS Glue Data Catalog. Puoi integrare AWS Glue Data Catalog con l'endpoint di destinazione Amazon S3 ed eseguire query sui dati Amazon S3 tramite altri servizi AWS, come Amazon Athena. Amazon Redshift funziona con AWS Glue, ma AWS DMS non la supporta come opzione predefinita.

Per generare il catalogo dati, imposta l'impostazione dell'endpoint `GlueCatalogGeneration` su `true`, come mostrato nell'esempio della AWS CLI seguente.

```
aws dms create-endpoint --endpoint-identifier s3-target-endpoint
                        --engine-name s3 --endpoint-type target--s3-settings
                        '{"ServiceAccessRoleArn":
                          "your-service-access-ARN", "BucketFolder": "your-bucket-folder",
                        "BucketName":
                          "your-bucket-name", "DataFormat": "parquet", "GlueCatalogGeneration":
                        true}'
```

Per un'attività di replica di pieno carico che include dati di tipo `csv`, imposta `IncludeOpForFullLoad` su `true`.

Non utilizzare `GlueCatalogGeneration` con `PreserveTransactions` e `CdcPath`. Il crawler AWS Glue non è in grado di riconciliare i diversi schemi di file archiviati nel `CdcPath` specificato.

Affinché Amazon Athena indicizzi i dati Amazon S3 per poter eseguire le query sui dati utilizzando query SQL standard tramite Amazon Athena, il ruolo IAM associato all'endpoint deve avere la seguente policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListBucketMultipartUploads",
        "s3:ListMultipartUploadParts",
        "s3:AbortMultipartUpload"
      ],
      "Resource": [
        "arn:aws:s3:::bucket123",
        "arn:aws:s3:::bucket123/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:CreateDatabase",
        "glue:GetDatabase",
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:UpdateTable",
        "glue:GetTable",
        "glue:BatchCreatePartition",
        "glue:CreatePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
      ],
      "Resource": [
        "arn:aws:glue:*:111122223333:catalog",
        "arn:aws:glue:*:111122223333:database/*",
        "arn:aws:glue:*:111122223333:table/*"
      ]
    }
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:StartQueryExecution",
        "athena:GetQueryExecution",
        "athena:CreateWorkGroup"
      ],
      "Resource": "arn:aws:athena:*:111122223333:workgroup/
glue_catalog_generation_for_task_*"
    }
  ]
}
```

Riferimenti

- Per ulteriori informazioni su AWS Glue, consulta [Concetti dell'](#) nella Guida per gli sviluppatori AWS Glue.
- Per ulteriori informazioni su AWS Glue Data Catalog, consulta [Componenti](#) nella Guida per gli sviluppatori di AWS Glue.

Utilizzo della crittografia dei dati, dei file parquet e della CDC sulla destinazione Amazon S3

Puoi utilizzare le impostazioni dell'endpoint di destinazione S3 per configurare quanto segue:

- Una chiave KMS personalizzata per crittografare gli oggetti di destinazione S3.
- File parquet come formato di storage dei file per gli oggetti di destinazione S3.
- Acquisizione dei dati di modifica (CDC) incluso l'ordine di transazione sulla destinazione S3.
- Effettua l'integrazione di AWS Glue Data Catalog con l'endpoint di destinazione Amazon S3 ed esegui le query sui dati Amazon S3 tramite altri servizi, come Amazon Athena.

Impostazioni della chiave AWS KMS per la crittografia dei dati

I seguenti esempi mostrano la configurazione di una chiave KMS personalizzata per crittografare gli oggetti di destinazione S3. Per iniziare, è possibile eseguire il comando CLI `create-endpoint` seguente.

```
aws dms create-endpoint --endpoint-identifier s3-target-endpoint --engine-name s3 --
endpoint-type target
--s3-settings '{"ServiceAccessRoleArn": "your-service-access-ARN", "CsvRowDelimiter":
"\n",
"CsvDelimiter": ",", "BucketFolder": "your-bucket-folder",
"BucketName": "your-bucket-name",
"EncryptionMode": "SSE_KMS",
"ServerSideEncryptionKmsKeyId": "arn:aws:kms:us-
east-1:111122223333:key/72abb6fb-1e49-4ac1-9aed-c803dfcc0480"}'
```

Qui l'oggetto JSON specificato dall'opzione `--s3-settings` definisce due parametri. Uno è un parametro `EncryptionMode` con il valore `SSE_KMS`. L'altro è un parametro `ServerSideEncryptionKmsKeyId` con il valore `arn:aws:kms:us-east-1:111122223333:key/72abb6fb-1e49-4ac1-9aed-c803dfcc0480`. Questo valore è un ARN (Amazon Resource Name) per la chiave KMS personalizzata. Per una destinazione S3, è anche possibile specificare impostazioni aggiuntive. Queste identificano il ruolo di accesso al server, specificano i delimitatori per il formato di memorizzazione degli oggetti CSV predefinito e forniscono il nome e la posizione del bucket per la memorizzazione degli oggetti di destinazione S3.

Per impostazione predefinita, la crittografia dei dati di S3 viene effettuata utilizzando la crittografia lato server. Per la destinazione S3 dell'esempio precedente, ciò è anche equivalente a specificare le impostazioni dell'endpoint, come nell'esempio seguente.

```
aws dms create-endpoint --endpoint-identifier s3-target-endpoint --engine-name s3 --
endpoint-type target
--s3-settings '{"ServiceAccessRoleArn": "your-service-access-ARN", "CsvRowDelimiter":
"\n",
"CsvDelimiter": ",", "BucketFolder": "your-bucket-folder",
"BucketName": "your-bucket-name",
"EncryptionMode": "SSE_S3"}'
```

Per ulteriori informazioni sulle opzioni di crittografia lato server di S3, consultare [Protezione dei dati con la crittografia lato server](#).

Note

È inoltre possibile utilizzare il comando CLI `modify-endpoint` per modificare il valore del parametro `EncryptionMode` per un endpoint esistente da `SSE_KMS` a `SSE_S3`. Tuttavia non puoi modificare il valore di `EncryptionMode` da `SSE_S3` a `SSE_KMS`.

Impostazioni per l'utilizzo di file .parquet per l'archiviazione di oggetti di destinazione S3

Il formato predefinito per la creazione di oggetti di destinazione S3 è file .csv. I seguenti esempi mostrano alcune impostazioni di endpoint per specificare i file .parquet come formato per la creazione di oggetti di destinazione S3. È possibile specificare il formato dei file .parquet con tutte le impostazioni predefinite, come nell'esempio seguente.

```
aws dms create-endpoint --endpoint-identifier s3-target-endpoint --engine-name s3 --
endpoint-type target
--s3-settings '{"ServiceAccessRoleArn": "your-service-access-ARN", "DataFormat":
"parquet"}'
```

Qui il parametro `DataFormat` è impostato su `parquet` per abilitare il formato con tutte le impostazioni predefinite di S3. Queste impostazioni predefinite includono una codifica del dizionario (`"EncodingType": "rle-dictionary"`) che utilizza una combinazione di creazione di pacchetti di bit e di codifica `runlength` per un'archiviazione più efficiente dei valori ripetuti.

È possibile aggiungere ulteriori impostazioni per opzioni diverse dalle impostazioni predefinite come nell'esempio seguente.

```
aws dms create-endpoint --endpoint-identifier s3-target-endpoint --engine-name s3 --
endpoint-type target
--s3-settings '{"ServiceAccessRoleArn": "your-service-access-ARN", "BucketFolder":
"your-bucket-folder",
"BucketName": "your-bucket-name", "CompressionType": "GZIP", "DataFormat": "parquet",
"EncodingType": "plain-dictionary", "DictPageSizeLimit": 3,072,000,
"EnableStatistics": false }'
```

Qui, oltre ai parametri per varie opzioni standard del bucket S3 e il parametro `DataFormat`, vengono impostati i seguenti parametri aggiuntivi del file .parquet:

- `EncodingType`: imposta una codifica di dizionario (`plain-dictionary`) che archivia i valori rilevati in ogni colonna in un blocco per colonna della pagina del dizionario.
- `DictPageSizeLimit`: imposta la dimensione massima della pagina del dizionario di 3 MB.
- `EnableStatistics`: disabilita l'impostazione predefinita che consente la raccolta di statistiche sulle pagine e sui gruppi di righe dei file Parquet.

Capturing Data Changes (CDC) incluso l'ordine di transazione sulla destinazione S3

Per impostazione predefinita, quando AWS DMS esegue un'attività di CDC, memorizza tutte le modifiche alle righe registrate nel database (o nei database) di origine in uno o più file per ogni tabella. Ogni set di file contenente le modifiche della stessa tabella si trova in un'unica directory di destinazione associata a quella tabella. AWS DMS crea tante directory di destinazione quante sono le tabelle del database migrate all'endpoint di destinazione Amazon S3. I file vengono archiviati sulla destinazione S3 in queste directory indipendentemente dall'ordine di transazione. Per ulteriori informazioni sulle convenzioni di denominazione dei file, sul contenuto dei dati e sul formato, consulta [Utilizzo di Amazon S3 come destinazione per AWS Database Migration Service](#).

Per acquisire le modifiche al database di origine in modo da rilevare anche l'ordine di transazione, puoi specificare le impostazioni degli endpoint S3 che consentono ad AWS DMS di memorizzare le modifiche alle righe per tutte le tabelle del database in uno o più file .csv creati in base alla dimensione della transazione. Questi file di transazione .csv contengono tutte le modifiche alle righe elencate in sequenza nell'ordine di transazione per tutte le tabelle coinvolte in ciascuna transazione. Questi file di transazione risiedono insieme in un'unica directory delle transazioni che specifichi anche sulla destinazione S3. In ogni file di transazione, l'operazione di transazione e l'identità del database e della tabella di origine per ogni modifica alla riga vengono archiviate come parte dei dati di riga, come indicato di seguito.

```
operation,table_name,database_schema_name,field_value,...
```

Qui *operation* è l'operazione di transazione sulla riga modificata, *table_name* è il nome della tabella del database in cui è stata modificata la riga, *database_schema_name* è il nome dello schema del database in cui si trova la tabella e *field_value* è il primo di uno o più valori di campo che specificano i dati per la riga.

Il seguente file di transazione di esempio mostra le righe modificate per una o più transazioni che coinvolgono due tabelle.

```
I,Names_03cdcad11a,rdsTempsdb,13,Daniel  
U,Names_03cdcad11a,rdsTempsdb,23,Kathy  
D,Names_03cdcad11a,rdsTempsdb,13,Cathy  
I,Names_6d152ce62d,rdsTempsdb,15,Jane  
I,Names_6d152ce62d,rdsTempsdb,24,Chris  
I,Names_03cdcad11a,rdsTempsdb,16,Mike
```

Qui, l'operazione di transazione su ogni riga è indicata da I (insert, inserisci), U (update, aggiorna) o D (delete, elimina) nella prima colonna. Il nome della tabella è il valore della seconda colonna (ad esempio, Names_03cdcad11a). Il nome dello schema del database è il valore della terza colonna (ad esempio, rdsTempsdb). E le colonne rimanenti vengono popolate con i propri dati della riga (ad esempio, 13, Daniel).

Inoltre, AWS DMS assegna un nome ai file di transazione che crea sulla destinazione Amazon S3 utilizzando un timestamp secondo la seguente convenzione di denominazione.

```
CDC_TXN-timestamp.csv
```

Qui *timestamp* è l'ora in cui stato creato il file di transazione, come nell'esempio seguente.

```
CDC_TXN-20201117153046033.csv
```

Questo timestamp nel nome del file assicura che i file delle transazioni vengano creati ed elencati nell'ordine di transazione nella rispettiva directory della transazione.

Note

Durante l'acquisizione delle modifiche ai dati nell'ordine delle transazioni, AWS DMS archivia sempre le modifiche alle righe nei file.csv indipendentemente dal valore dell'impostazione DataFormat S3 della destinazione. AWS DMS non salva le modifiche ai dati nell'ordine di transazione utilizzando i file. parquet.

Per controllare la frequenza delle scritture su una destinazione Amazon S3 durante un'attività di replica dei dati, puoi configurare le impostazioni CdcMaxBatchInterval e CdcMinFileSize. In tal modo le prestazioni possono risultare migliori durante l'analisi dei dati senza ulteriori operazioni di sovraccarico. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#)

Per indicare ad AWS DMS di archiviare tutte le modifiche alle righe nell'ordine di transazione

1. Configura l'impostazione PreserveTransactions S3 nella destinazione su true.
2. Configura l'impostazione CdcPath S3 nella destinazione su un percorso di cartella relativo in cui desideri che AWS DMS archivi i file di transazione in formato.csv.

AWS DMS crea questo percorso nel bucket di destinazione S3 e nella directory di lavoro predefiniti oppure nel bucket e nella cartella del bucket specificati utilizzando le impostazioni `BucketName` e `BucketFolder` S3 nella destinazione.

Indicazione delle operazioni del DB di origine nei dati S3 migrati

Quando AWS DMS migra i record su una destinazione S3, può creare un campo aggiuntivo in ogni record migrato. Il campo aggiuntivo indica l'operazione applicata al record nel database di origine. Il modo in cui AWS DMS crea e imposta questo primo campo dipende dal tipo di attività di migrazione e dalle impostazioni di `includeOpForFullLoad`, `cdcInsertsOnly` e `cdcInsertsAndUpdates`.

Per un pieno carico quando `includeOpForFullLoad` è `true`, AWS DMS crea sempre un ulteriore primo campo in ogni record `.csv`. Il campo contiene la lettera I (INSERT) per confermare che la riga è stata inserita nel database di origine. Per un caricamento CDC quando `cdcInsertsOnly` è `false` (valore predefinito), AWS DMS crea sempre un ulteriore primo campo in ciascun record `.csv` o `.parquet`. Il campo contiene la lettera I (INSERT), U (UPDATE) o D (DELETE) per indicare se la riga è stata inserita, aggiornata o eliminata nel database di origine.

Nella tabella seguente, puoi vedere come le impostazioni degli attributi `includeOpForFullLoad` e `cdcInsertsOnly` interagiscono per influenzare l'impostazione dei record migrati.

Con queste impostazioni dei parametri		DMS imposta i record di destinazione come segue per l'output <code>.csv</code> e <code>.parquet</code>	
<code>includeOpForFullLoad</code>	<code>cdcInsertsOnly</code>	Per il caricamento completo	Per il caricamento CDC
<code>true</code>	<code>true</code>	Aggiunto il valore del primo campo impostato su I	Aggiunto il valore del primo campo impostato su I
<code>false</code>	<code>false</code>	Nessun campo aggiunto	Aggiunto il valore del primo campo impostato su I, U o D
<code>false</code>	<code>true</code>	Nessun campo aggiunto	Nessun campo aggiunto

Con queste impostazioni dei parametri		DMS imposta i record di destinazione come segue per l'output .csv e .parquet	
<code>includeOpForFullLoad</code>	<code>cdcInsertsOnly</code>	Per il caricamento completo	Per il caricamento CDC
<code>true</code>	<code>false</code>	Aggiunto il valore del primo campo impostato su I	Aggiunto il valore del primo campo impostato su I, U o D

Quando `includeOpForFullLoad` e `cdcInsertsOnly` sono impostati sullo stesso valore, i record di destinazione sono impostati in base all'attributo che controlla le impostazioni di registrazione per il tipo di migrazione corrente. Questo attributo è `includeOpForFullLoad` per il caricamento completo e `cdcInsertsOnly` per il caricamento CDC.

Quando `includeOpForFullLoad` e `cdcInsertsOnly` hanno valori diversi, AWS DMS rende coerenti le impostazioni del record di destinazione sia per CDC sia per il caricamento completo. A tale scopo, le impostazioni del record per un caricamento CDC sono conformi alle impostazioni del record per qualsiasi precedente caricamento completo specificato da `includeOpForFullLoad`.

In altre parole, supponiamo che un caricamento completo sia impostato per aggiungere un primo campo per indicare un record inserito. In questo caso, un caricamento CDC successivo viene impostato per aggiungere un primo campo che indica un record inserito, aggiornato o eliminato come appropriato nell'origine. Al contrario, supponiamo che un caricamento completo è impostato per non aggiungere un primo campo per indicare un record inserito. In questo caso, viene impostato un caricamento CDC per non aggiungere un primo campo a ciascun record, indipendentemente dall'operazione di registrazione corrispondente nell'origine.

Analogamente, il modo in cui DMS crea e imposta un primo campo aggiuntivo dipende dalle impostazioni di `includeOpForFullLoad` e `cdcInsertsAndUpdates`. Nella tabella seguente, puoi vedere come le impostazioni degli attributi `includeOpForFullLoad` e `cdcInsertsAndUpdates` interagiscono per influenzare l'impostazione dei record migrati in questo formato.

Con queste impostazioni dei parametri		DMS imposta i record di destinazione come segue per l'output .csv	
includeOpForFullLoad	cdcInsertsAndUpdates	Per il caricamento completo	Per il caricamento CDC
true	true	Aggiunto il valore del primo campo impostato su I	Aggiunto il valore del primo campo impostato su I o U
false	false	Nessun campo aggiunto	Aggiunto il valore del primo campo impostato su I, U o D
false	true	Nessun campo aggiunto	Aggiunto il valore del primo campo impostato su I o U
true	false	Aggiunto il valore del primo campo impostato su I	Aggiunto il valore del primo campo impostato su I, U o D

Tipi di dati di destinazione per Parquet S3

La tabella seguente mostra i tipi di dati di destinazione Parquet supportati quando si utilizza AWS DMS e la mappatura predefinita dei tipi di dati AWS DMS.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipo di dati AWS DMS	Tipo di dati parquet S3
BYTES	BINARY
DATE	DATE32
TIME	TIME32

Tipo di dati AWS DMS	Tipo di dati parquet S3
DATETIME	TIMESTAMP
INT1	INT8
INT2	INT16
INT4	INT32
INT8	INT64
NUMERIC	DECIMAL
REAL4	FLOAT
REAL8	DOUBLE
STRING	STRING
UINT1	UINT8
UINT2	UINT16
UINT4	UINT32
UINT8	UINT64
WSTRING	STRING
BLOB	BINARY
NCLOB	STRING
CLOB	STRING
BOOLEAN	BOOL

Utilizzo di un database Amazon DynamoDB come destinazione per AWS Database Migration Service

È possibile utilizzare AWS DMS per migrare dati in una tabella Amazon DynamoDB. Amazon DynamoDB è un servizio di database NoSQL completamente gestito che fornisce prestazioni rapide e prevedibili con una scalabilità ottimale. AWS DMS supporta l'utilizzo di un database relazionale o MongoDB come origine.

In DynamoDB, le tabelle, le voci e gli attributi sono i componenti principali da utilizzare. Una tabella è una raccolta di elementi e ogni elemento è una raccolta di attributi. DynamoDB utilizza le chiavi primarie, denominate chiavi di partizione, per identificare in modo univoco ciascuna voce in una tabella. Puoi inoltre utilizzare chiavi e indici secondari per fornire maggiore flessibilità nell'esecuzione di query.

È possibile utilizzare la mappatura degli oggetti per migrare i dati da un database di origine a una tabella DynamoDB di destinazione. La mappatura di oggetti consente di determinare dove sono posizionati i dati di origine nella destinazione.

Quando AWS DMS crea tabelle su un endpoint di destinazione DynamoDB, crea un numero di tabelle pari a quello delle tabelle presenti nell'endpoint del database di origine. AWS DMS imposta inoltre diversi valori di parametri DynamoDB. Il costo per la creazione della tabella dipende dalla quantità di dati e dal numero di tabelle da migrare.

Note

L'opzione Modalità SSL della console AWS DMS o dell'API non si applica ad alcuni servizi di flusso di dati e NoSQL, come Kinesis e DynamoDB. Tali servizi sono sicuri per impostazione predefinita, quindi AWS DMS mostra che la modalità SSL non è impostata (SSL Mode=None). Per utilizzare SSL non è necessario eseguire alcuna configurazione aggiuntiva per l'endpoint. Ad esempio, l'utilizzo di DynamoDB come endpoint di destinazione è sicuro per impostazione predefinita. Tutte le chiamate API a DynamoDB utilizzano SSL, quindi non è necessaria un'opzione SSL aggiuntiva nell'endpoint AWS DMS. È possibile inserire dati e recuperarli in modo sicuro tramite gli endpoint SSL utilizzando il protocollo HTTPS, usato da AWS DMS per impostazione predefinita per la connessione a un database DynamoDB.

Per incrementare la velocità del trasferimento, AWS DMS supporta il pieno carico multithread in un'istanza DynamoDB di destinazione. DMS supporta questo multithreading con impostazioni delle attività che includono le seguenti:

- `MaxFullLoadSubTasks`: imposta questa opzione per indicare il numero massimo di tabelle da caricare in parallelo. DMS carica ogni tabella nella corrispondente tabella di destinazione DynamoDB utilizzando un'attività secondaria dedicata. Il valore predefinito è 8. Il valore massimo è 49.
- `ParallelLoadThreads`: utilizza questa opzione per specificare il numero di thread usati da AWS DMS per caricare ogni tabella nella tabella di destinazione DynamoDB. Il valore predefinito è 0 (a thread singolo). Il valore massimo è 200. Puoi chiedere che questo limite massimo venga aumentato.

Note

DMS assegna ogni segmento di una tabella al proprio thread per il caricamento. Pertanto, impostare `ParallelLoadThreads` al numero massimo di segmenti specificati dall'utente per una tabella nella sorgente.

- `ParallelLoadBufferSize`: utilizza questa opzione per specificare il numero massimo di record da archiviare nel buffer utilizzato dai thread di caricamento parallelo per caricare i dati nella destinazione DynamoDB. Il valore predefinito è 50. Il valore massimo è 1.000. Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread.
- Impostazioni di mappatura delle tabelle per le singole tabelle: utilizza le regole `table-settings` per identificare le singole tabelle dell'origine da caricare in parallelo. Inoltre utilizza queste regole per specificare come segmentare le righe di ciascuna tabella multithreaded per il caricamento. Per ulteriori informazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Note

Quando AWS DMS imposta i valori di parametri DynamoDB per un'attività di migrazione, il valore del parametro RCU (Read Capacity Unit, unità di capacità in lettura) predefinito è impostato su 200.

Viene inoltre impostato il valore del parametro WCU (Write Capacity Unit, Unità di capacità in scrittura), ma tale valore dipende da diverse altre impostazioni:

- Il valore predefinito per il parametro WCU è 200.
- Se l'attività `ParallelLoadThreads` è impostata su un valore superiore a 1 (il valore di default è 0), allora il parametro WCU è impostato su 200 volte il valore `ParallelLoadThreads`.
- Il costo di utilizzo di AWS DMS standard si applica alle risorse utilizzate.

Migrazione da un database relazionale a una tabella DynamoDB

AWS DMS supporta la migrazione dei dati a tipi di dati scalari di DynamoDB. Durante la migrazione da un database relazionale, ad esempio Oracle o MySQL, a DynamoDB, potresti voler ristrutturare il modo in cui vengono archiviati i dati.

Attualmente, AWS DMS supporta la ristrutturazione da tabella singola a tabella singola per attributi di tipo scalare di DynamoDB. Se esegui la migrazione dei dati in DynamoDB da una tabella di database relazionale, prelevi i dati da una tabella e li riformatti in attributi del tipo di dati scalare di DynamoDB. Questi attributi possono accettare i dati provenienti da più colonne e puoi mappare direttamente una colonna a un attributo.

AWS DMS supporta i seguenti tipi di dati scalari di DynamoDB:

- Stringa
- Numero
- Booleano

Note

I dati NULL dall'origine vengono ignorati sulla destinazione.

Prerequisiti per l'utilizzo di DynamoDB come destinazione per AWS Database Migration Service

Prima di iniziare a utilizzare un database DynamoDB come destinazione per AWS DMS, è necessario creare un ruolo IAM. Il ruolo IAM deve consentire ad AWS DMS di disporre e concedere l'accesso alle tabelle DynamoDB in cui viene eseguita la migrazione. Nella seguente policy IAM viene mostrato il set minimo di autorizzazioni di accesso.

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

Il ruolo utilizzato per la migrazione a DynamoDB deve disporre delle seguenti autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:PutItem",
        "dynamodb:CreateTable",
        "dynamodb:DescribeTable",
        "dynamodb>DeleteTable",
        "dynamodb>DeleteItem",
        "dynamodb:UpdateItem"
      ],
      "Resource": [
        "arn:aws:dynamodb:us-west-2:account-id:table/name1",
        "arn:aws:dynamodb:us-west-2:account-id:table/OtherName*",
        "arn:aws:dynamodb:us-west-2:account-id:table/awsdms_apply_exceptions",
        "arn:aws:dynamodb:us-west-2:account-id:table/awsdms_full_load_exceptions"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "dynamodb:ListTables"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}  
  ]  
}
```

Limitazioni all'utilizzo di DynamoDB come destinazione per AWS Database Migration Service

Le seguenti limitazioni si applicano quando si utilizza DynamoDB come destinazione:

- DynamoDB limita la precisione del tipo di dati Number a 38 posizioni. Archivia tutti i tipi di dati con una precisione superiore come String. Devi specificare esplicitamente questo valore mediante la caratteristica di mappatura degli oggetti.
- Poiché DynamoDB non dispone di un tipo di dati Date, i dati che utilizzano il tipo di dati Date vengono convertiti in stringhe.
- DynamoDB non consente gli aggiornamenti degli attributi di chiave primaria. Questa restrizione è importante quando si utilizza la replica continua con l'acquisizione dei dati di modifica (CDC), perché può causare la presenza di dati indesiderati nella destinazione. A seconda del tipo di mappatura degli oggetti, un'operazione CDC che aggiorna la chiave primaria può eseguire una delle due seguenti azioni: Può restituire un errore o inserire un nuovo elemento con la chiave primaria aggiornata e dati incompleti.
- AWS DMS supporta solo la replica di tabelle con chiavi primarie non composite. L'eccezione è se si specifica una mappatura degli oggetti per la tabella di destinazione con una chiave di partizione personalizzata o una chiave di ordinamento o con entrambe.
- AWS DMS non supporta dati LOB a meno che non si tratti di un CLOB. Durante la migrazione dei dati, AWS DMS converte i dati CLOB in una stringa DynamoDB.
- Quando si utilizza DynamoDB come destinazione, solo la tabella di controllo Apply Exceptions (`dmslogs.aws_dms_apply_exceptions`) è supportata. Per ulteriori informazioni sulle tabelle di controllo, consultare [Impostazioni delle attività delle tabelle di controllo](#).
- AWS DMS non supporta l'impostazione delle attività `TargetTablePrepMode=TRUNCATE_BEFORE_LOAD` per DynamoDB come destinazione.
- AWS DMS non supporta l'impostazione delle attività `TaskRecoveryTableEnabled` per DynamoDB come destinazione.

Utilizzo della mappatura degli oggetti per la migrazione dei dati a DynamoDB

AWS DMS utilizza le regole di mappatura delle tabelle per mappare i dati dall'origine alla tabella DynamoDB di destinazione. Per mappare i dati a una destinazione DynamoDB, è necessario utilizzare una regola di mappatura delle tabelle denominata `object-mapping`. La mappatura degli oggetti consente di definire i nomi degli attributi e i dati da migrare. Quando utilizzi la mappatura degli oggetti, devi disporre di regole di selezione.

DynamoDB non dispone di una struttura preimpostata oltre a una chiave di partizione e una chiave di ordinamento opzionale. Se disponi di una chiave primaria non composta, AWS DMS la utilizza. Se disponi di una chiave primaria composta o desideri utilizzare una chiave di ordinamento, definisci tali chiavi e gli altri attributi nella tabella DynamoDB di destinazione.

Per creare una regola di mappatura degli oggetti, è necessario specificare il parametro `rule-type` come `object-mapping`. Questa regola specifica il tipo di mappatura degli oggetti da utilizzare.

Di seguito è riportata la struttura per la regola:

```
{ "rules": [
  {
    "rule-type": "object-mapping",
    "rule-id": "<id>",
    "rule-name": "<name>",
    "rule-action": "<valid object-mapping rule action>",
    "object-locator": {
      "schema-name": "<case-sensitive schema name>",
      "table-name": ""
    },
    "target-table-name": "<table_name>"
  }
]
```

AWS DMS attualmente supporta `map-record-to-record` e `map-record-to-document` come i soli valori validi per il parametro `rule-action`. Questi valori specificano le operazioni eseguite per impostazione predefinita da AWS DMS sui record che non vengono esclusi come parte dell'elenco degli attributi `exclude-columns`. Questi valori non influiscono in alcun modo sulle mappature degli attributi.

- Puoi utilizzare `map-record-to-record` per la migrazione da un database relazionale a DynamoDB. Questo parametro utilizza la chiave primaria dal database relazionale come chiave

di partizione in DynamoDB e crea un attributo per ogni colonna nel database di origine. Quando utilizzi `map-record-to-record`, per qualsiasi colonna nella tabella di origine non elencata nell'elenco di attributi `exclude-columns`, AWS DMS crea un attributo corrispondente nell'istanza DynamoDB di destinazione. Questa operazione avviene indipendentemente dal fatto che tale colonna di origine venga utilizzata o meno in una mappatura degli attributi.

- Puoi utilizzare `map-record-to-document` per inserire le colonne origine in una singola mappa piana DynamoDB nella destinazione utilizzando il nome di attributo `"_doc"`. Quando utilizzi `map-record-to-document`, AWS DMS inserisce i dati in un singolo attributo di mappa piana DynamoDB nell'origine. Questo attributo è denominato `"_doc"`. Questo posizionamento si applica a qualsiasi colonna della tabella di origine non elencata nell'elenco di attributi `exclude-columns`.

Uno dei modi per comprendere la differenza tra i parametri `rule-action`, `map-record-to-record` e `map-record-to-document` è di osservare i due parametri in azione. Per questo esempio, supponiamo che tu stia iniziando con una riga di tabella del database relazionale con la struttura e i dati seguenti:

FirstName	LastName	NickName	WorkAddress	WorkPhone	HomeAddress	HomePhone	income
▶ Daniel	Sheridan	Dan	101 Main St Cambridge, MA	800-867-5309	100 Secret St, Unknownville, MA	123-456-7890	12345678

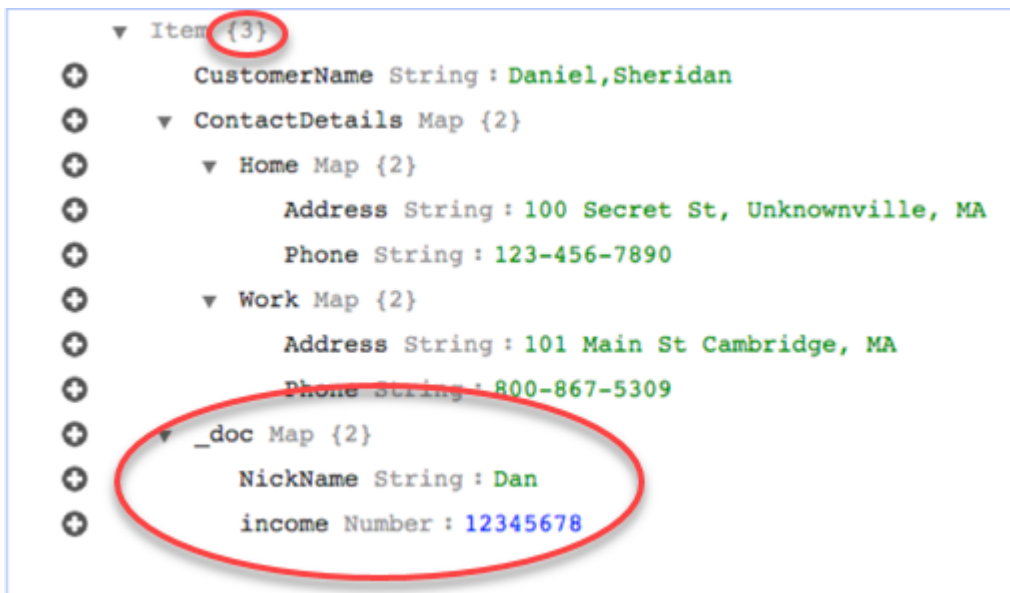
Per eseguire la migrazione di queste informazioni a DynamoDB, crei le regole per mappare i dati in una voce di tabella DynamoDB. Nota le colonne elencate per il parametro `exclude-columns`. Queste colonne non sono mappate direttamente alla destinazione. Al contrario, la mappatura degli attributi è utilizzata combinare i dati in nuove voci, ad esempio nel caso in cui `FirstName` e `LastName` vengano raggruppati per diventare `CustomerName` sulla destinazione DynamoDB. `NickName` e `income` non sono esclusi.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
```

```

"rule-type": "object-mapping",
"rule-id": "2",
"rule-name": "TransformToDDB",
"rule-action": "map-record-to-record",
"object-locator": {
  "schema-name": "test",
  "table-name": "customer"
},
"target-table-name": "customer_t",
"mapping-parameters": {
  "partition-key-name": "CustomerName",
  "exclude-columns": [
    "FirstName",
    "LastName",
    "HomeAddress",
    "HomePhone",
    "WorkAddress",
    "WorkPhone"
  ],
  "attribute-mappings": [
    {
      "target-attribute-name": "CustomerName",
      "attribute-type": "scalar",
      "attribute-sub-type": "string",
      "value": "${FirstName},${LastName}"
    },
    {
      "target-attribute-name": "ContactDetails",
      "attribute-type": "document",
      "attribute-sub-type": "dynamodb-map",
      "value": {
        "M": {
          "Home": {
            "M": {
              "Address": {
                "S": "${HomeAddress}"
              },
              "Phone": {
                "S": "${HomePhone}"
              }
            }
          },
          "Work": {
            "M": {

```

Utilizzo di espressioni di condizioni personalizzate con mappatura degli oggetti

Puoi utilizzare una funzionalità di DynamoDB denominata espressioni condizionali per gestire i dati scritti in una tabella DynamoDB. Per ulteriori informazioni sulle espressioni condizionali in DynamoDB, consulta [Espressioni di condizione](#).

Un membro di espressione condizionale è costituito dai seguenti elementi:

- un'espressione (obbligatoria)
- valori degli attributi dell'espressione (opzionali). Specifica una struttura json DynamoDB del valore dell'attributo
- nomi degli attributi dell'espressione (opzionali)
- opzioni per i casi in cui utilizzare l'espressione condizionale (opzionali). I valori predefiniti sono `apply-during-cdc = false` e `apply-during-full-load = true`

Di seguito è riportata la struttura per la regola:

```

"target-table-name": "customer_t",
  "mapping-parameters": {
    "partition-key-name": "CustomerName",
    "condition-expression": {
      "expression": "<conditional expression>",
      "expression-attribute-values": [
        {

```

```

        "name": "<attribute name>",
        "value": "<attribute value>"
    }
],
"apply-during-cdc": <optional Boolean value>,
"apply-during-full-load": <optional Boolean value>
}

```

L'esempio seguente evidenzia le sezioni utilizzate per l'espressione condizionale.

```

{
  "rules": [
    {
      "rule-type": "object-mapping",
      "rule-id": "1",
      "rule-name": "TransformToDDB",
      "rule-action": "map-record-to-record",
      "object-locator": {
        "schema-name": "test",
        "table-name": "customer",
      },
    },
    "target-table-name": "customer_t",
    "mapping-parameters": {
      "partition-key-name": "CustomerName",
      "condition-expression": {
        "expression": "attribute_not_exists(version) or version <= :record_version",
        "expression-attribute-values": [
          {
            "name": ":record_version",
            "value": {"N": "${version}"}
          }
        ],
      },
      "apply-during-cdc": true,
      "apply-during-full-load": true
    }
  ],
  "attribute-mappings": [
    {
      "target-attribute-name": "CustomerName",
      "attribute-type": "scalar",
      "attribute-sub-type": "string",
      "value": "${FirstName},${LastName}"
    }
  ]
}

```

The diagram illustrates a JSON configuration for a rule. Three callouts point to specific parts of the configuration:

- Object mapping section defines name, rule-action, and object locator information:** Points to the `object-locator` object within the rule definition.
- Condition expression:** Points to the `condition-expression` object within the `mapping-parameters` object.
- Options:** Points to the `apply-during-cdc` and `apply-during-full-load` boolean values within the `mapping-parameters` object.

Utilizzo della mappatura degli attributi con la mappatura degli oggetti

La mappatura degli attributi consente di specificare una stringa di modello mediante i nomi di colonna di origine per ristrutturare i dati sulla destinazione. Non viene eseguita alcuna formattazione oltre a quella che l'utente specifica nel modello.

L'esempio seguente mostra la struttura del database di origine e la struttura desiderata della destinazione DynamoDB. In primo luogo è riportata la struttura dell'origine, in questo caso un

database Oracle, quindi la struttura dei dati in DynamoDB. Al termine dell'esempio, il file JSON viene utilizzato per creare la struttura di destinazione desiderata.

La struttura dei dati Oracle è la seguente:

First	Last	Street	Home/SS	HomeF	WorkAddress	Work	DateOfBirth
Chiave primaria				N/D			
Randy	Sh	5	221B Baker Street	1234567890	31 Spooner Street, Quahog	9876541230	02/29/1988

La struttura dei dati DynamoDB è la seguente:

Customer Name	StoreId	ContactDetails	DateOfBirth
Chiave di partizione	Chiave di ordinamento	N/D	
Randy Sh	5	{ "Name": "Randy", "Home": { "Address": "221B Baker Street", "Phone": 1234567890 }, "Work": { "Address": "31 Spooner Street, Quahog", "Phone": 9876541230 } }	02/29/1988

CustomerName	StoreId	ContactDetails	DateOfBirth
		}	

Il seguente file JSON mostra la mappatura degli oggetti e la mappatura delle colonne utilizzate per ottenere la struttura DynamoDB:

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "TransformToDDB",
      "rule-action": "map-record-to-record",
      "object-locator": {
        "schema-name": "test",
        "table-name": "customer"
      },
      "target-table-name": "customer_t",
      "mapping-parameters": {
        "partition-key-name": "CustomerName",
        "sort-key-name": "StoreId",
        "exclude-columns": [
          "FirstName",
          "LastName",
          "HomeAddress",
          "HomePhone",
          "WorkAddress",
          "WorkPhone"
        ]
      }
    }
  ],
}
```

```

    "attribute-mappings": [
      {
        "target-attribute-name": "CustomerName",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "${FirstName},${LastName}"
      },
      {
        "target-attribute-name": "StoreId",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "${StoreId}"
      },
      {
        "target-attribute-name": "ContactDetails",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "{\"Name\": \"${FirstName}\", \"Home\": {\"Address
\": \"${HomeAddress}\", \"Phone\": \"${HomePhone}\"}, \"Work\": {\"Address\":
\": \"${WorkAddress}\", \"Phone\": \"${WorkPhone}\"}}}"
      }
    ]
  }
]
}

```

Un altro modo per utilizzare la mappatura delle colonne consiste nell'utilizzo del formato DynamoDB come tipo di documento. Il seguente codice di esempio utilizza dynamodb-map come attribute-sub-type per la mappatura degli attributi.

```

{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "test",
        "table-name": "%"
      }
    },
  ],
}

```



```

    "rule-action": "include"
  },
  {
    "rule-type": "object-mapping",
    "rule-id": "2",
    "rule-name": "TransformToDDB",
    "rule-action": "map-record-to-record",
    "object-locator": {
      "schema-name": "test",
      "table-name": "customer"
    },
    "target-table-name": "customer_t",
    "mapping-parameters": {
      "partition-key-name": "CustomerName",
      "sort-key-name": "StoreId",
      "exclude-columns": [
        "FirstName",
        "LastName",
        "HomeAddress",
        "HomePhone",
        "WorkAddress",
        "WorkPhone"
      ],
      "attribute-mappings": [
        {
          "target-attribute-name": "CustomerName",
          "attribute-type": "scalar",
          "attribute-sub-type": "string",
          "value": "${FirstName},${LastName}"
        },
        {
          "target-attribute-name": "StoreId",
          "attribute-type": "scalar",
          "attribute-sub-type": "string",
          "value": "${StoreId}"
        },
        {
          "target-attribute-name": "ContactDetails",
          "attribute-type": "document",
          "attribute-sub-type": "dynamodb-map",
          "value": {
            "M": {
              "Name": {
                "S": "${FirstName}"
              }
            }
          }
        }
      ]
    }
  }
}

```



```

    },
    {
      "N": "${HomeAddress}"
    },
    {
      "N": "${HomePhone}"
    },
    {
      "N": "${WorkAddress}"
    },
    {
      "N": "${WorkPhone}"
    }
  ]
}

```

Esempio 1: utilizzo della mappatura degli attributi con la mappatura degli oggetti

Nell'esempio seguente vengono migrati i dati provenienti da due tabelle di database MySQL, `nfl_data` e `sport_team`, a due tabelle DynamoDB denominate `NFLTeams` e `SportTeams`. Di seguito sono riportati la struttura delle tabelle e il file JSON utilizzato per mappare i dati dalle tabelle di database MySQL alle tabelle DynamoDB.

Di seguito è riportata la struttura della tabella di database MySQL `nfl_data`:

```
mysql> desc nfl_data;
+-----+-----+-----+-----+-----+-----+
| Field          | Type          | Null | Key | Default | Extra |
+-----+-----+-----+-----+-----+-----+
| Position       | varchar(5)    | YES  |     | NULL    |       |
| player_number  | smallint(6)   | YES  |     | NULL    |       |
| Name           | varchar(40)   | YES  |     | NULL    |       |
| status         | varchar(10)   | YES  |     | NULL    |       |
| stat1          | varchar(10)   | YES  |     | NULL    |       |
| stat1_val      | varchar(10)   | YES  |     | NULL    |       |
| stat2          | varchar(10)   | YES  |     | NULL    |       |
| stat2_val      | varchar(10)   | YES  |     | NULL    |       |
| stat3          | varchar(10)   | YES  |     | NULL    |       |
| stat3_val      | varchar(10)   | YES  |     | NULL    |       |
| stat4          | varchar(10)   | YES  |     | NULL    |       |

```

```
| stat4_val      | varchar(10) | YES | | NULL | | |
| team          | varchar(10) | YES | | NULL | | |
+-----+-----+-----+-----+-----+-----+
```

Di seguito è riportata la struttura della tabella di database MySQL sport_team:

```
mysql> desc sport_team;
+-----+-----+-----+-----+-----+-----+
| Field          | Type          | Null | Key | Default | Extra          |
+-----+-----+-----+-----+-----+-----+
| id             | mediumint(9) | NO   | PRI | NULL    | auto_increment |
| name           | varchar(30)   | NO   |     | NULL    |                |
| abbreviated_name | varchar(10)   | YES  |     | NULL    |                |
| home_field_id  | smallint(6)   | YES  | MUL | NULL    |                |
| sport_type_name | varchar(15)   | NO   | MUL | NULL    |                |
| sport_league_short_name | varchar(10) | NO   |     | NULL    |                |
| sport_division_short_name | varchar(10) | YES  |     | NULL    |                |
```

Di seguito sono riportate le regole di mappatura delle tabelle utilizzate per mappare le due tabelle alle due tabelle DynamoDB:

```
{
  "rules":[
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "dms_sample",
        "table-name": "nfl_data"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "selection",
      "rule-id": "2",
      "rule-name": "2",
      "object-locator": {
        "schema-name": "dms_sample",
```

```

    "table-name": "sport_team"
  },
  "rule-action": "include"
},
{
  "rule-type": "object-mapping",
  "rule-id": "3",
  "rule-name": "MapNFLData",
  "rule-action": "map-record-to-record",
  "object-locator": {
    "schema-name": "dms_sample",
    "table-name": "nfl_data"
  },
  "target-table-name": "NFLTeams",
  "mapping-parameters": {
    "partition-key-name": "Team",
    "sort-key-name": "PlayerName",
    "exclude-columns": [
      "player_number", "team", "name"
    ],
    "attribute-mappings": [
      {
        "target-attribute-name": "Team",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "${team}"
      },
      {
        "target-attribute-name": "PlayerName",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "${name}"
      },
      {
        "target-attribute-name": "PlayerInfo",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "{\"Number\": \"${player_number}\", \"Position\": \"${Position}\",
        \"Status\": \"${status}\", \"Stats\": {\"Stat1\": \"${stat1}:${stat1_val}\", \"Stat2\":
        \"${stat2}:${stat2_val}\", \"Stat3\": \"${stat3}:${
        stat3_val}\", \"Stat4\": \"${stat4}:${stat4_val}\"}"}
      }
    ]
  }
}
}

```

```

},
{
  "rule-type":"object-mapping",
  "rule-id":"4",
  "rule-name":"MapSportTeam",
  "rule-action":"map-record-to-record",
  "object-locator":{
    "schema-name":"dms_sample",
    "table-name":"sport_team"
  },
  "target-table-name":"SportTeams",
  "mapping-parameters":{
    "partition-key-name":"TeamName",
    "exclude-columns": [
      "name", "id"
    ],
    "attribute-mappings":[
      {
        "target-attribute-name":"TeamName",
        "attribute-type":"scalar",
        "attribute-sub-type":"string",
        "value":"${name}"
      },
      {
        "target-attribute-name":"TeamInfo",
        "attribute-type":"scalar",
        "attribute-sub-type":"string",
        "value":"{\\"League\\": \\"${sport_league_short_name}\\",\\"Division\\":
\\"${sport_division_short_name}\\"}"
      }
    ]
  }
}
]
}

```

Di seguito è riportato l'output di esempio per la tabella DynamoDB NFLTeams:

```

"PlayerInfo": "{\\"Number\\": \\"6\\",\\"Position\\": \\"P\\",\\"Status\\": \\"ACT\\",\\"Stats\\":
{\\"Stat1\\": \\"PUNTS:73\\",\\"Stat2\\": \\"AVG:46\\",\\"Stat3\\": \\"LNG:67\\",\\"Stat4\\": \\"IN
20:31\\"}"

```

```
"PlayerName": "Allen, Ryan",
"Position": "P",
"stat1": "PUNTS",
"stat1_val": "73",
"stat2": "AVG",
"stat2_val": "46",
"stat3": "LNG",
"stat3_val": "67",
"stat4": "IN 20",
"stat4_val": "31",
"status": "ACT",
"Team": "NE"
}
```

Di seguito è riportato l'output di esempio per la tabella DynamoDB SportsTeams:

```
{
  "abbreviated_name": "IND",
  "home_field_id": 53,
  "sport_division_short_name": "AFC South",
  "sport_league_short_name": "NFL",
  "sport_type_name": "football",
  "TeamInfo": "{\"League\": \"NFL\", \"Division\": \"AFC South\"}",
  "TeamName": "Indianapolis Colts"
}
```

Tipi di dati di destinazione per DynamoDB

L'endpoint DynamoDB per AWS DMS supporta la maggior parte dei tipi di dati DynamoDB. La tabella seguente mostra i tipi di dati di destinazione di Amazon AWS DMS supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati AWS DMS.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Quando AWS DMS esegue la migrazione dei dati da database eterogenei, mappiamo i tipi di dati dal database di origine ai tipi di dati intermedi, denominati tipi di dati AWS DMS. Mappiamo quindi i tipi di dati intermedi ai tipi di dati di destinazione. La seguente tabella mostra ciascun tipo di dati AWS DMS e il tipo di dati a cui viene mappato in DynamoDB:

Tipo di dati AWS DMS	Tipo di dati DynamoDB
Stringa	Stringa
WString	Stringa
Booleano	Booleano
Data	Stringa
DateTime	Stringa
INT1	Numero
INT2	Numero
INT4	Numero
INT8	Numero
Numerico	Numero
Real4	Numero
Real8	Numero
UINT1	Numero
UINT2	Numero
UINT4	Numero
UINT8	Numero
CLOB	Stringa

Utilizzo di Amazon Kinesis Data Streams come destinazione per AWS Database Migration Service

Puoi utilizzarlo AWS DMS per migrare i dati verso un flusso di dati Amazon Kinesis. I flussi di dati Amazon Kinesis fanno parte del servizio Flusso di dati Amazon Kinesis. Puoi utilizzare i flussi di dati Kinesis per raccogliere ed elaborare flussi di grandi dimensioni di record di dati in tempo reale.

Un flusso di dati Kinesis è costituito da partizioni. Gli shard sono sequenze identificate in modo univoco di record di dati in un flusso. Per ulteriori informazioni sulle partizioni in Flusso di dati Amazon Kinesis, consulta [Shard](#) nella Guida per gli sviluppatori di Flusso di dati Amazon Kinesis.

AWS Database Migration Service pubblica i record in un flusso di dati Kinesis utilizzando JSON. Durante la conversione, AWS DMS serializza ogni record dal database di origine in una coppia attributo-valore in formato JSON o in un formato di messaggio JSON_UNFORMATTED. Un formato di messaggio JSON_UNFORMATTED è una stringa JSON a riga singola con nuovo delimitatore di riga. Consente ad Amazon Data Firehose di distribuire dati Kinesis a una destinazione Amazon S3 e quindi di interrogarli utilizzando vari motori di query tra cui Amazon Athena.

È possibile utilizzare la mappatura degli oggetti per migrare i dati da qualsiasi origine dati supportata a un flusso di destinazione. Con la mappatura degli oggetti, determini il modo in cui strutturare i record di dati nel flusso. Puoi inoltre definire una chiave di partizione per ogni tabella che viene utilizzata dai flussi di dati Kinesis per raggruppare i dati nelle partizioni.

Quando AWS DMS crea tabelle su un endpoint di destinazione Kinesis Data Streams, crea tante tabelle quante sono nell'endpoint del database di origine. AWS DMS imposta anche diversi valori dei parametri Kinesis Data Streams. Il costo per la creazione della tabella dipende dalla quantità di dati e dal numero di tabelle da migrare.

Note

L'opzione SSL Mode sulla AWS DMS console o sull'API non si applica ad alcuni servizi di streaming di dati e NoSQL come Kinesis e DynamoDB. Sono sicuri per impostazione predefinita, quindi AWS DMS mostra che l'impostazione della modalità SSL è uguale a none (modalità SSL = Nessuno). Per utilizzare SSL non è necessario eseguire alcuna configurazione aggiuntiva per l'endpoint. Ad esempio, l'utilizzo di Kinesis come endpoint di destinazione è sicuro per impostazione predefinita. Tutte le chiamate API a Kinesis utilizzano SSL, quindi non è necessaria un'opzione SSL aggiuntiva nell'endpoint. AWS DMS È possibile inserire dati e recuperarli in modo sicuro tramite gli endpoint SSL utilizzando il protocollo

HTTPS, usato da AWS DMS per impostazione predefinita per la connessione a un flusso di dati Kinesis.

Impostazioni degli endpoint del flusso di dati Kinesis

Quando utilizzi gli endpoint target di Kinesis Data Streams, puoi ottenere i dettagli delle transazioni e del controllo `KinesisSettings` utilizzando l'opzione nell'API. AWS DMS

Puoi configurare le impostazioni di connessione nei modi seguenti:

- Nella AWS DMS console, utilizzando le impostazioni degli endpoint.
- Nella CLI, utilizzando l'`kinesis-settings` opzione del [CreateEndpoint](#) comando.

Nella CLI utilizza i seguenti parametri di richiesta dell'opzione `kinesis-settings`:

Note

Il supporto per l'impostazione dell'endpoint `IncludeNullAndEmpty` è disponibile in AWS DMS 3.4.1 e versioni successive. Tuttavia, il supporto per le altre impostazioni degli endpoint seguenti per i target Kinesis Data Streams è disponibile in. AWS DMS

- `MessageFormat`: il formato di output per i record creati nell'endpoint. Il formato del messaggio è JSON (predefinito) o `JSON_UNFORMATTED` (una singola riga senza tabulazione).
- `IncludeControlDetails`: mostra informazioni dettagliate sul controllo per la definizione di tabella, la definizione di colonna e le modifiche di tabelle e colonne nell'output dei messaggi Kinesis. Il valore predefinito è `false`.
- `IncludeNullAndEmpty`: include le colonne vuote e NULL nella destinazione. Il valore predefinito è `false`.
- `IncludePartitionValue`: mostra il valore della partizione all'interno dell'output dei messaggi di Kinesis, a meno che il tipo della partizione non sia `schema-table-type`. Il valore predefinito è `false`.
- `IncludeTableAlterOperations`: include tutte le operazioni DDL (Data Definition Language) che modificano i dati di controllo della tabella, ad esempio `rename-table`, `drop-table`, `add-column`, `drop-column` e `rename-column`. Il valore predefinito è `false`.

- **IncludeTransactionDetails**: fornisce informazioni dettagliate sulle transazioni dal database di origine. Tali informazioni includono un timestamp di commit, una posizione nel log e valori per `transaction_id`, `previous_transaction_id` e `transaction_record_id` (l'offset del record all'interno di una transazione). Il valore predefinito è `false`.
- **PartitionIncludeSchemaTable**: aggiunge ai nomi di schemi e tabelle il prefisso con i valori di partizione, quando il tipo di partizione è `primary-key-type`. In questo modo si aumenta la distribuzione dei dati tra gli shard di Kinesis. Ad esempio, si supponga che uno schema SysBench includa migliaia di tabelle e che ogni tabella faccia riferimento solo a un intervallo limitato di valori della chiave primaria. In questo caso, la stessa chiave primaria viene inviata da migliaia di tabelle allo stesso shard, causando un rallentamento. Il valore predefinito è `false`.

L'esempio seguente mostra l'opzione `kinesis-settings` in uso con un comando `create-endpoint` di esempio emesso utilizzando la AWS CLI.

```
aws dms create-endpoint --endpoint-identifier=$target_name --engine-name kinesis --
endpoint-type target
--region us-east-1 --kinesis-settings
  ServiceAccessRoleArn=arn:aws:iam::333333333333:role/dms-kinesis-role,
  StreamArn=arn:aws:kinesis:us-east-1:333333333333:stream/dms-kinesis-target-
  doc,MessageFormat=json-unformatted,
  IncludeControlDetails=true,IncludeTransactionDetails=true,IncludePartitionValue=true,PartitionI
  IncludeTableAlterOperations=true
```

Impostazioni attività a pieno carico multithread

Per contribuire ad aumentare la velocità di trasferimento, AWS DMS supporta un caricamento completo multithread su un'istanza di destinazione Kinesis Data Streams. DMS supporta questo multithreading con impostazioni delle attività che includono le seguenti:

- **MaxFullLoadSubTasks**: imposta questa opzione per indicare il numero massimo di tabelle da caricare in parallelo. DMS consente di caricare ogni tabella nella corrispondente tabella di destinazione Kinesis utilizzando un'attività secondaria dedicata. Il valore predefinito è 8; il valore il massimo è 49.
- **ParallelLoadThreads**— Utilizzate questa opzione per specificare il numero di thread da utilizzare per caricare ogni tabella nella relativa tabella di destinazione Kinesis. AWS DMS Il valore massimo per una destinazione del flusso di dati Kinesis è 32. Puoi chiedere che questo limite massimo venga aumentato.

- `ParallelLoadBufferSize`: utilizza questa opzione per specificare il numero massimo di record da archiviare nel buffer utilizzato dai thread di caricamento parallelo per caricare i dati nella destinazione Kinesis. Il valore predefinito è 50. Il valore massimo è 1.000. Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread.
- `ParallelLoadQueuesPerThread`: utilizza questa opzione per specificare il numero di code a cui accede ogni thread simultaneo per eliminare i record di dati dalle code e generare un carico batch per la destinazione. Il valore di default è 1. Tuttavia, per le destinazioni Kinesis di varie dimensioni del payload, l'intervallo valido è compreso tra 5 e 512 code per thread.

Impostazioni attività di carico CDC multithread

È possibile migliorare le prestazioni dell'acquisizione dei dati di modifica (CDC) per gli endpoint di destinazione in streaming dei dati in tempo reale come Kinesis utilizzando le impostazioni delle attività per modificare il comportamento della chiamata API `PutRecords`. A tale scopo, è possibile specificare il numero di thread simultanei, di code per thread e di record da memorizzare in un buffer utilizzando le impostazioni delle attività `ParallelApply*`. Ad esempio, si supponga di voler eseguire un carico CDC e applicare 128 thread in parallelo. Si desidera inoltre accedere a 64 code per thread, con 50 record memorizzati per buffer.

Per promuovere le prestazioni del CDC, AWS DMS supporta le seguenti impostazioni delle attività:

- `ParallelApplyThreads`— specifica il numero di thread simultanei che vengono AWS DMS utilizzati durante un caricamento CDC per inviare i record di dati a un endpoint di destinazione Kinesis. Il valore predefinito è zero (0) e il valore massimo è 32.
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per eseguire il push dei thread simultanei a un endpoint di destinazione Kinesis durante un carico CDC. Il valore predefinito è 100 e il valore massimo è 1.000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per eliminare i record di dati dalle code e generare un carico batch per un endpoint Kinesis durante CDC. Il valore predefinito è 1 e il valore massimo è 512.

Quando si utilizzano le impostazioni delle attività `ParallelApply*`, l'impostazione di `partition-key-type` predefinita è la `primary-key` della tabella, non `schema-name.table-name`.

Utilizzo di un'immagine precedente per visualizzare i valori originali delle righe CDC per un flusso di dati Kinesis come destinazione

Quando si scrivono aggiornamenti CDC su una destinazione di streaming dati come Kinesis, è possibile visualizzare i valori originali di una riga di database di origine prima di apportare modifiche da un aggiornamento. Per rendere possibile ciò, AWS DMS compila un'immagine precedente degli eventi di aggiornamento sulla base dei dati forniti dal motore di database di origine.

Diversi motori di database di origine forniscono diverse quantità di informazioni per un'immagine precedente:

- Oracle fornisce aggiornamenti alle colonne solo se cambiano.
- PostgreSQL fornisce solo i dati per le colonne che fanno parte della chiave primaria (modificata o meno). Per fornire dati per tutte le colonne (modificate o meno), devi impostare su `REPLICA_IDENTITY` su `FULL` invece di `DEFAULT`. Tieni presente che occorre scegliere attentamente l'impostazione `REPLICA_IDENTITY` per ogni tabella. Se si imposta `REPLICA_IDENTITY` su `FULL`, tutti i valori delle colonne vengono scritti continuamente nel WAL (Write-Ahead Logging). Ciò può causare problemi di prestazioni o di risorse con le tabelle che vengono aggiornate frequentemente.
- MySQL generalmente fornisce dati per tutte le colonne ad eccezione dei tipi di dati BLOB e CLOB (modificati o meno).

Per consentire prima dell'imaging di aggiungere valori originali dal database di origine all'output AWS DMS, utilizzare l'impostazione dell'attività `BeforeImageSettings` o il parametro `add-before-image-columns`. Questo parametro applica una regola di trasformazione della colonna.

`BeforeImageSettings` aggiunge un nuovo attributo JSON a ogni operazione di aggiornamento con valori raccolti dal sistema di database di origine, come illustrato di seguito.

```
"BeforeImageSettings": {
  "EnableBeforeImage": boolean,
  "FieldName": string,
  "ColumnFilter": pk-only (default) / non-lob / all (but only one)
}
```

Note

Si applica solo `BeforeImageSettings` alle AWS DMS attività che contengono un componente CDC, come le attività a pieno carico e le attività CDC (che migrano i dati esistenti e replicano le modifiche in corso) o alle attività solo CDC (che replicano solo le modifiche ai dati). Non applicare `BeforeImageSettings` alle attività a pieno carico.

Per le opzioni `BeforeImageSettings`, si applica quanto segue:

- Impostare l'opzione `EnableBeforeImage` su `true` da abilitare prima dell'imaging. Il valore predefinito è `false`.
- Utilizzare l'opzione `FieldName` per assegnare un nome al nuovo attributo JSON. Quando `EnableBeforeImage` è `true`, `FieldName` è richiesto e non può essere vuoto.
- L'opzione `ColumnFilter` specifica una colonna da aggiungere utilizzando l'imaging precedente. Per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella, utilizzare il valore predefinito, `pk-only`. Per aggiungere qualsiasi colonna con un valore immagine prima, utilizzare `all`. Tieni presente che l'immagine precedente non contiene colonne con tipi di dati LOB, come CLOB o BLOB.

```
"BeforeImageSettings": {  
  "EnableBeforeImage": true,  
  "FieldName": "before-image",  
  "ColumnFilter": "pk-only"  
}
```

Note

Le destinazioni Amazon S3 non supportano `BeforeImageSettings`. Per le destinazioni S3, utilizzare solo la regola di trasformazione `add-before-image-columns` da eseguire prima dell'imaging durante CDC.

Utilizzo di una regola di trasformazione dell'immagine precedente

In alternativa alle impostazioni delle attività, è possibile utilizzare il parametro `add-before-image-columns`, che applica una regola di trasformazione delle colonne. Con questo parametro, è possibile abilitare l'imaging precedente durante CDC su destinazioni di flusso di dati come Kinesis.

Utilizzando `add-before-image-columns` in una regola di trasformazione, è possibile applicare un controllo più dettagliato dei risultati dell'immagine precedente. Le regole di trasformazione consentono di utilizzare un localizzatore di oggetti che consente di controllare le tabelle selezionate per la regola. Inoltre, è possibile concatenare le regole di trasformazione, consentendo l'applicazione di regole diverse a tabelle diverse. È quindi possibile manipolare le colonne prodotte utilizzando altre regole.

Note

Non utilizzare il parametro `add-before-image-columns` insieme all'impostazione dell'attività `BeforeImageSettings` all'interno della stessa attività. Utilizzare invece il parametro o l'impostazione, ma non entrambi, per una singola attività.

Un tipo di regola `transformation` regola con il parametro `add-before-image-columns` per una colonna deve fornire una sezione `before-image-def`. Di seguito viene riportato un esempio.

```
{
  "rule-type": "transformation",
  ...
  "rule-target": "column",
  "rule-action": "add-before-image-columns",
  "before-image-def": {
    "column-filter": one-of (pk-only / non-lob / all),
    "column-prefix": string,
    "column-suffix": string,
  }
}
```

Il valore di `column-prefix` viene anteposto a un nome di colonna e il valore predefinito di `column-prefix` è `BI_`. Il valore di `column-suffix` viene aggiunto al nome della colonna e il valore predefinito è vuoto. Non impostare sia `column-prefix` sia `column-suffix` sull'opzione per svuotare le stringhe.

Scegliere un valore per `column-filter`. Per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella, scegliere `pk-only`. Scegliere `non-lob` per aggiungere solo colonne non di tipo LOB. Oppure scegliere `all` per aggiungere qualsiasi colonna con un valore immagine precedente.

Esempio di una regola di trasformazione dell'immagine precedente

La regola di trasformazione nell'esempio seguente aggiunge una nuova colonna chiamata `BI_emp_no` nella destinazione. Quindi una dichiarazione come `UPDATE employees SET emp_no = 3 WHERE emp_no = 1;` popola il campo `BI_emp_no` con 1. Quando si scrivono aggiornamenti CDC alle destinazioni Amazon S3, la colonna `BI_emp_no` indica quale riga originale è stata aggiornata.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "%",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-target": "column",
      "object-locator": {
        "schema-name": "%",
        "table-name": "employees"
      },
      "rule-action": "add-before-image-columns",
      "before-image-def": {
        "column-prefix": "BI_",
        "column-suffix": "",
        "column-filter": "pk-only"
      }
    }
  ]
}
```



```
}
```

Per informazioni sull'utilizzo dell'operazione della regola `add-before-image-columns`, consulta [Operazioni e regole di trasformazione](#).

Prerequisiti per l'utilizzo di un flusso di dati Kinesis come destinazione per AWS Database Migration Service

Ruolo IAM per l'utilizzo di un flusso di dati Kinesis come destinazione per AWS Database Migration Service

Prima di configurare un flusso di dati Kinesis come destinazione per AWS DMS, assicurati di creare un ruolo IAM. Questo ruolo deve consentire di AWS DMS assumere e concedere l'accesso ai flussi di dati Kinesis in cui viene effettuata la migrazione. Nella seguente policy IAM viene mostrato il set minimo di autorizzazioni di accesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Il ruolo utilizzato per la migrazione a un flusso di dati Kinesis deve disporre delle seguenti autorizzazioni.

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

```
{
  "Effect": "Allow",
  "Action": [
    "kinesis:DescribeStream",
    "kinesis:PutRecord",
    "kinesis:PutRecords"
  ],
  "Resource": "arn:aws:kinesis:region:accountID:stream/streamName"
}
```

Accesso a un flusso di dati Kinesis come destinazione per AWS Database Migration Service

Nella AWS DMS versione 3.4.7 e successive, per connetterti a un endpoint Kinesis, devi eseguire una delle seguenti operazioni:

- Configura DMS per utilizzare gli endpoint VPC. Per informazioni sulla configurazione di DMS per utilizzare gli endpoint VPC, consulta [Configurazione degli endpoint VPC come endpoint di origine e di destinazione AWS DMS](#).
- Configura DMS per utilizzare routing pubblici, ovvero per rendere pubblica l'istanza di replica. Per ulteriori informazioni sulle istanze di replica pubbliche, consulta [Istanze di replica pubbliche e private](#).

Limitazioni nell'utilizzo di Kinesis Data Streams come destinazione per AWS Database Migration Service

Le seguenti limitazioni si applicano quando si utilizza il flusso di dati Kinesis come destinazione:

- AWS DMS pubblica ogni aggiornamento di un singolo record nel database di origine come un unico record di dati in un determinato flusso di dati Kinesis indipendentemente dalle transazioni. Tuttavia, è possibile includere i dettagli della transazione per ogni record di dati utilizzando i parametri pertinenti dell'API `KinesisSettings`.
- La modalità LOB completa non è supportata.
- La dimensione massima del LOB supportata è 1 MB.
- I flussi di dati Kinesis non supportano la deduplicazione. Le applicazioni che utilizzano i dati provenienti da un flusso devono gestire i record duplicati. Per ulteriori informazioni, consulta [Handling duplicate records](#) nella Guida per gli sviluppatori di Flusso di dati Amazon Kinesis.

- AWS DMS supporta i seguenti due moduli per le chiavi di partizione:
 - `SchemaName.TableName`: una combinazione del nome dello schema e quello della tabella.
 - `${AttributeName}`: il valore di uno dei campi nel formato JSON o la chiave primaria della tabella del database di origine.
- Per informazioni sulla crittografia dei dati a riposo all'interno del flusso di dati Kinesis, consulta [Data protection in Kinesis Data Streams](#) nella Guida per gli sviluppatori di AWS Key Management Service .
- `BatchApply` non è supportato per un endpoint Kinesis. L'utilizzo dell'applicazione in batch, ad esempio l'impostazione dell'attività dei metadati di destinazione `BatchApplyEnabled`, per una destinazione Kinesis potrebbe causare la perdita di dati.
- Le destinazioni Kinesis sono supportate solo per un flusso di dati Kinesis nello stesso AWS account e nello stesso dell'istanza di replica. Regione AWS
- Durante la migrazione da una fonte MySQL, i dati non includono `BeforeImage` i tipi di dati CLOB e BLOB. Per ulteriori informazioni, consulta [Utilizzo di un'immagine precedente per visualizzare i valori originali delle righe CDC per un flusso di dati Kinesis come destinazione](#).
- AWS DMS non supporta la migrazione di valori di tipi di `BigInt` dati con più di 16 cifre. Per aggirare questa limitazione puoi utilizzare la seguente regola di trasformazione per convertire la colonna `BigInt` in una stringa. Per ulteriori informazioni sulle regole di trasformazione, consulta [Operazioni e regole di trasformazione](#).

```
{
  "rule-type": "transformation",
  "rule-id": "id",
  "rule-name": "name",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "valid object-mapping rule action",
    "table-name": "",
    "column-name": ""
  },
  "rule-action": "change-data-type",
  "data-type": {
    "type": "string",
    "length": 20
  }
}
```

Utilizzo della mappatura degli oggetti per la migrazione dei dati a un flusso di dati Kinesis

AWS DMS utilizza regole di mappatura delle tabelle per mappare i dati dal flusso di dati Kinesis di origine a quello di destinazione. Per mappare i dati a un flusso di destinazione, è necessario utilizzare una regola di mappatura delle tabelle denominata mappatura degli oggetti. La mappatura degli oggetti consente di definire il modo in cui i record di dati nell'origine vengono mappati ai record di dati pubblicati nel flusso di dati Kinesis.

I flussi di dati Kinesis non dispongono di una struttura preimpostata oltre a una chiave di partizione. In una regola di mapping degli oggetti, i valori possibili di una `partition-key-type` per i record di dati sono `schema-table`, `transaction-id`, `primary-key`, `constant` e `attribute-name`.

Per creare una regola di mappatura degli oggetti, è necessario specificare il parametro `rule-type` come `object-mapping`. Questa regola specifica il tipo di mappatura degli oggetti da utilizzare.

Di seguito è riportata la struttura per la regola.

```
{
  "rules": [
    {
      "rule-type": "object-mapping",
      "rule-id": "id",
      "rule-name": "name",
      "rule-action": "valid object-mapping rule action",
      "object-locator": {
        "schema-name": "case-sensitive schema name",
        "table-name": ""
      }
    }
  ]
}
```

AWS DMS attualmente supporta `map-record-to-record` e `map-record-to-document` l'unico valore valido per il parametro `rule-action`. Queste impostazioni influiscono sui valori che non sono esclusi come parte dell'elenco degli attributi `exclude-columns`. I `map-record-to-document` valori `map-record-to-record` and `specificano` come AWS DMS gestisce questi record per impostazione predefinita. Questi valori non influiscono in alcun modo sulle mappature degli attributi.

Utilizza `map-record-to-record` per la migrazione da un database relazionale a un flusso di dati Kinesis. Questo tipo di regola utilizza il valore `taskResourceId.schemaName.tableName` dal database relazionale come chiave di partizione nel flusso di dati Kinesis e crea un attributo per ogni colonna nel database di origine.

Quando utilizzi `map-record-to-record`, tieni presente quanto segue:

- Questa impostazione ha effetto solo sulle colonne escluse dall'elenco `exclude-columns`.
- Per ogni colonna di questo tipo, AWS DMS crea un attributo corrispondente nell'argomento di destinazione.
- AWS DMS crea questo attributo corrispondente indipendentemente dal fatto che la colonna di origine venga utilizzata in una mappatura degli attributi.

Utilizza `map-record-to-document` per inserire le colonne di origine in un unico documento flat nel flusso di destinazione appropriato utilizzando il nome dell'attributo `"_doc"`. AWS DMS posiziona i dati in un'unica mappa flat sull'origine chiamata `"_doc"`. Questo posizionamento si applica a qualsiasi colonna della tabella di origine non elencata nell'elenco di attributi `exclude-columns`.

Per comprendere il funzionamento di `map-record-to-record`, è opportuno esaminarne il comportamento in azione. Per questo esempio, supponiamo che tu stia iniziando con una riga di tabella del database relazionale con la struttura e i dati seguenti.

FirstName	LastName	StoreId	HomeAddress	HomePhone	WorkAddress	WorkPhone	DateofBirth
Randy	Marsh	5	221B Baker Street	123456789 0	31 Spooner Street, Quahog	987654321 0	02/29/198 8

Per eseguire la migrazione di queste informazioni da uno schema denominato `Test` a un flusso di dati Kinesis, crea le regole per mappare i dati sul flusso di destinazione. La regola seguente illustra la mappatura.

```
{
  "rules": [
```

```
{
  "rule-type": "selection",
  "rule-id": "1",
  "rule-name": "1",
  "rule-action": "include",
  "object-locator": {
    "schema-name": "Test",
    "table-name": "%"
  }
},
{
  "rule-type": "object-mapping",
  "rule-id": "2",
  "rule-name": "DefaultMapToKinesis",
  "rule-action": "map-record-to-record",
  "object-locator": {
    "schema-name": "Test",
    "table-name": "Customers"
  }
}
]
```

Di seguito viene illustrato il formato di record risultante nel flusso di dati Kinesis:

- StreamName: XXX
- PartitionKey: Test.Customers //schmaname.tableName
- Dati: //Il seguente messaggio JSON

```
{
  "FirstName": "Randy",
  "LastName": "Marsh",
  "StoreId": "5",
  "HomeAddress": "221B Baker Street",
  "HomePhone": "1234567890",
  "WorkAddress": "31 Spooner Street, Quahog",
  "WorkPhone": "9876543210",
  "DateOfBirth": "02/29/1988"
}
```

Supponi tuttavia di utilizzare le stesse regole ma modificando il parametro `rule-action` su `map-record-to-document` ed escludendo determinate colonne. La regola seguente illustra la mappatura.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "DefaultMapToKinesis",
      "rule-action": "map-record-to-document",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customers"
      },
      "mapping-parameters": {
        "exclude-columns": [
          "homeaddress",
          "homephone",
          "workaddress",
          "workphone"
        ]
      }
    }
  ]
}
```

In questo caso, le colonne non elencate nel parametro `exclude-columns`, `FirstName`, `LastName`, `StoreId` e `DateOfBirth` sono mappate a `_doc`. Di seguito viene illustrato il formato di record risultante.

```
{
  "data":{
    "_doc":{
      "FirstName": "Randy",
      "LastName": "Marsh",
      "StoreId": "5",
      "DateOfBirth": "02/29/1988"
    }
  }
}
```

Ristrutturazione dei dati con la mappatura degli attributi

Puoi ristrutturare i dati mentre li stai migrando a un flusso di dati Kinesis utilizzando una mappa degli attributi. Ad esempio, potresti voler combinare più campi nell'origine in un unico campo nella destinazione. La seguente mappa degli attributi illustra come ristrutturare i dati.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "TransformToKinesis",
      "rule-action": "map-record-to-record",
      "target-table-name": "CustomerData",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customers"
      },
      "mapping-parameters": {
        "partition-key-type": "attribute-name",
```



```

    "partition-key-name": "CustomerName",
    "exclude-columns": [
      "firstname",
      "lastname",
      "homeaddress",
      "homephone",
      "workaddress",
      "workphone"
    ],
    "attribute-mappings": [
      {
        "target-attribute-name": "CustomerName",
        "attribute-type": "scalar",
        "attribute-sub-type": "string",
        "value": "${lastname}, ${firstname}"
      },
      {
        "target-attribute-name": "ContactDetails",
        "attribute-type": "document",
        "attribute-sub-type": "json",
        "value": {
          "Home": {
            "Address": "${homeaddress}",
            "Phone": "${homephone}"
          },
          "Work": {
            "Address": "${workaddress}",
            "Phone": "${workphone}"
          }
        }
      }
    ]
  }
}

```

Per impostare un valore costante per `partition-key`, specificare un valore `partition-key`. Ad esempio, potresti eseguire questa operazione per forzare l'archiviazione di tutti i dati in un singolo shard. Questo approccio viene illustrato nella mappatura seguente.

```

{
  "rules": [

```

```
{
  "rule-type": "selection",
  "rule-id": "1",
  "rule-name": "1",
  "object-locator": {
    "schema-name": "Test",
    "table-name": "%"
  },
  "rule-action": "include"
},
{
  "rule-type": "object-mapping",
  "rule-id": "1",
  "rule-name": "TransformToKinesis",
  "rule-action": "map-record-to-document",
  "object-locator": {
    "schema-name": "Test",
    "table-name": "Customer"
  },
  "mapping-parameters": {
    "partition-key": {
      "value": "ConstantPartitionKey"
    },
    "exclude-columns": [
      "FirstName",
      "LastName",
      "HomeAddress",
      "HomePhone",
      "WorkAddress",
      "WorkPhone"
    ],
    "attribute-mappings": [
      {
        "attribute-name": "CustomerName",
        "value": "${FirstName},${LastName}"
      },
      {
        "attribute-name": "ContactDetails",
        "value": {
          "Home": {
            "Address": "${HomeAddress}",
            "Phone": "${HomePhone}"
          },
          "Work": {
```

```

        "Address": "${WorkAddress}",
        "Phone": "${WorkPhone}"
    }
},
{
    "attribute-name": "DateOfBirth",
    "value": "${DateOfBirth}"
}
]
}
]
}

```

Note

Il valore `partition-key` per un record di controllo per una tabella specifica è `TaskId.SchemaName.TableName`. Il valore `partition-key` per un record di controllo per un'attività specifica è il `TaskId` del record. La specifica di un valore `partition-key` nella mappatura degli oggetti non influisce sul parametro `partition-key` per un record di controllo.

Formato del messaggio per il flusso di dati Kinesis

L'output JSON è semplicemente un elenco di coppie chiave-valore. Un formato di messaggio `JSON_UNFORMATTED` è una stringa JSON a riga singola con nuovo delimitatore di riga.

AWS DMS fornisce i seguenti campi riservati per semplificare l'utilizzo dei dati provenienti da Kinesis Data Streams:

RecordType

Il tipo di record può essere relativo ai dati o al controllo. I record di dati rappresentano le righe effettive nell'origine. I record di controllo sono per eventi importanti nel flusso, ad esempio un riavvio dell'attività.

Operazione

Per i record di dati, l'operazione può essere `load`, `insert`, `update` o `delete`.

Per i record di controllo, l'operazione può essere `create-table`, `rename-table`, `drop-table`, `change-columns`, `add-column`, `drop-column`, `rename-column` o `column-type-change`.

SchemaName

Lo schema di origine per il record. Questo campo può essere vuoto per un record di controllo.

TableName

La tabella di origine per il record. Questo campo può essere vuoto per un record di controllo.

Timestamp

Il timestamp relativo al momento della creazione del messaggio JSON. Il campo viene formattato con il formato ISO 8601.

Usare Apache Kafka come obiettivo per AWS Database Migration Service

È possibile utilizzarlo AWS DMS per migrare i dati in un cluster Apache Kafka. Apache Kafka è una piattaforma di streaming distribuita. È possibile utilizzare Apache Kafka per l'inserimento e l'elaborazione dei dati di streaming in tempo reale.

AWS offre anche Amazon Managed Streaming for Apache Kafka (Amazon MSK) da utilizzare come destinazione. AWS DMS Amazon MSK è un servizio di streaming Apache Kafka completamente gestito che semplifica l'implementazione e la gestione delle istanze Apache Kafka. Funziona con le versioni open source di Apache Kafka e accedi alle istanze Amazon MSK come AWS DMS destinazioni esattamente come qualsiasi istanza di Apache Kafka. Per ulteriori informazioni, consulta [Che cos'è Amazon MSK?](#) nella Guida per sviluppatori di Streaming gestito da Amazon per Apache Kafka.

Un cluster Kafka archivia i flussi di record in categorie denominate argomenti che sono suddivisi in partizioni. Le partizioni sono sequenze di record di dati (messaggi) identificate in modo univoco in un argomento. Le partizioni possono essere distribuite tra più broker in un cluster per consentire l'elaborazione parallela dei record dell'argomento. Per ulteriori informazioni su argomenti e partizioni e la loro distribuzione in Apache Kafka, consulta [Argomenti e registri](#) e [Distribuzione](#).

Il cluster Kafka può essere un'istanza Amazon MSK, un cluster in esecuzione su un'istanza Amazon EC2 o un cluster on-premise. Un'istanza Amazon MSK o un cluster su un'istanza Amazon EC2 può trovarsi nello stesso VPC o in uno diverso. Se il cluster è on-premise, è possibile utilizzare il server dei nomi on-premise dell'istanza di replica per risolvere il nome host del cluster. Per informazioni sulla configurazione di un server dei nomi per l'istanza di replica, consulta [Utilizzo del server dei nomi in](#)

[locale](#). Per ulteriori informazioni sulla configurazione di una rete, consulta [Configurazione di una rete per un'istanza di replica](#).

Quando utilizzi un cluster Amazon MSK, assicurati che il relativo gruppo di sicurezza consenta l'accesso dall'istanza di replica. Per informazioni sulla modifica del gruppo di sicurezza di un cluster Amazon MSK, consulta [Modifica del gruppo di sicurezza di un cluster Amazon MSK](#).

AWS Database Migration Service pubblica i record relativi a un argomento di Kafka utilizzando JSON. Durante la conversione, AWS DMS serializza ogni record dal database di origine in una coppia attributo-valore in formato JSON.

È possibile usare la mappatura degli oggetti per migrare i dati da qualsiasi origine dati supportata a un cluster Kafka di destinazione. Con la mappatura degli oggetti, determini il modo in cui strutturare i record di dati nell'argomento di destinazione. Puoi inoltre definire una chiave di partizionamento per ogni tabella che viene utilizzata da Kafka per raggruppare i dati nelle sue partizioni.

Attualmente, AWS DMS supporta un singolo argomento per attività. Per una singola attività con più tabelle, tutti i messaggi vengono indirizzati a un unico argomento. Ogni messaggio include una sezione di metadati che identifica lo schema e la tabella di destinazione. AWS DMS le versioni 3.4.6 e successive supportano la replica multitematica utilizzando la mappatura degli oggetti. Per ulteriori informazioni, consulta [Replica di più argomenti con la mappatura degli oggetti](#).

Impostazioni endpoint Apache Kafka

È possibile specificare i dettagli della connessione tramite le impostazioni dell'endpoint nella AWS DMS console o l'`--kafka-settings` opzione nella CLI. I requisiti per ogni impostazione sono i seguenti:

- **Broker:** specifica le posizioni di uno o più broker nel cluster Kafka sotto forma di elenco di voci separate da virgole per ogni *broker-hostname:port*. Un esempio è `"ec2-12-345-678-901.compute-1.amazonaws.com:2345,ec2-10-987-654-321.compute-1.amazonaws.com:2345"`. Questa impostazione può specificare le posizioni di uno o tutti i broker del cluster. Tutti i broker del cluster comunicano per gestire il partizionamento dei record di dati migrati verso l'argomento.
- **Topic (facoltativo):** specifica il nome dell'argomento con una lunghezza massima di 255 lettere e simboli. È possibile utilizzare punto (.), carattere di sottolineatura (_) e segno meno (-). I nomi degli argomenti con un punto (.) o un carattere di sottolineatura (_) possono interferire con le strutture dati interne. Nel nome dell'argomento utilizzare uno dei due simboli ma non entrambi. Se non specificate il nome di un argomento, AWS DMS lo usa `"kafka-default-topic"` come argomento di migrazione.

Note

Se desiderate AWS DMS creare un argomento di migrazione specificato dall'utente o l'argomento predefinito, impostatelo `auto.create.topics.enable = true` come parte della configurazione del cluster Kafka. Per ulteriori informazioni, consultare [Limitazioni nell'utilizzo di Apache Kafka come destinazione per AWS Database Migration Service](#)

- **MessageFormat**: il formato di output per i record creati nell'endpoint. Il formato del messaggio è JSON (predefinito) o JSON_UNFORMATTED (una singola riga senza tabulazione).
- **MessageMaxBytes**: la dimensione massima in byte per i record creati nell'endpoint. Il valore di default è 1.000.000.

Note

È possibile utilizzare solo AWS CLI/SDK per passare **MessageMaxBytes** a un valore non predefinito. Ad esempio utilizza il seguente comando per modificare l'endpoint Kafka esistente e cambiare **MessageMaxBytes**.

```
aws dms modify-endpoint --endpoint-arn your-endpoint
--kafka-settings Broker="broker1-server:broker1-port,broker2-server:broker2-
port,...",
Topic=topic-name,MessageMaxBytes=integer-of-max-message-size-in-bytes
```

- **IncludeTransactionDetails**: fornisce informazioni dettagliate sulle transazioni dal database di origine. Tali informazioni includono un timestamp di commit, una posizione nel log e valori per `transaction_id`, `previous_transaction_id` e `transaction_record_id` (l'offset del record all'interno di una transazione). Il valore predefinito è `false`.
- **IncludePartitionValue**: mostra il valore della partizione nell'output dei messaggi di Kafka, a meno che il tipo della partizione non sia `schema-table-type`. Il valore predefinito è `false`.
- **PartitionIncludeSchemaTable**: aggiunge ai nomi di schemi e tabelle il prefisso con i valori di partizione, quando il tipo di partizione è `primary-key-type`. In questo modo si aumenta la distribuzione dei dati tra le partizioni di Kafka. Ad esempio, si supponga che uno schema `SysBench` includa migliaia di tabelle e che ogni tabella faccia riferimento solo a un intervallo limitato di valori della chiave primaria. In questo caso, la stessa chiave primaria viene inviata da migliaia di tabelle alla stessa partizione, causando un rallentamento. Il valore predefinito è `false`.

- `IncludeTableAlterOperations`: include tutte le operazioni DDL (Data Definition Language) che modificano i dati di controllo della tabella, ad esempio `rename-table`, `drop-table`, `add-column`, `drop-column` e `rename-column`. Il valore predefinito è `false`.
- `IncludeControlDetails`: mostra le informazioni dettagliate del controllo per la definizione di tabelle, la definizione di colonne e le modifiche di tabelle e colonne nell'output dei messaggi Kafka. Il valore predefinito è `false`.
- `IncludeNullAndEmpty`: include le colonne vuote e NULL nella destinazione. Il valore predefinito è `false`.
- `SecurityProtocol`: imposta una connessione sicura a un endpoint di destinazione Kafka utilizzando Transport Layer Security (TLS). Le opzioni includono `ssl-authentication`, `ssl-encryption` e `sasl-ssl`. L'utilizzo di `sasl-ssl` richiede `SaslUsername` e `SaslPassword`.
- `SslEndpointIdentificationAlgorithm`— Imposta la verifica del nome host per il certificato. Questa impostazione è supportata nella AWS DMS versione 3.5.1 e successive. Le opzioni sono le seguenti:
 - `NONE`: Disattiva la verifica del nome host del broker nella connessione del client.
 - `HTTPS`: Abilita la verifica del nome host del broker nella connessione del client.

È possibile utilizzare le impostazioni per aumentare la velocità del trasferimento. Per farlo, AWS DMS supporta il pieno carico multithread in un cluster Apache Kafka di destinazione. AWS DMS supporta il multithreading con le impostazioni delle attività seguenti:

- `MaxFullLoadSubTasks`— Utilizzate questa opzione per indicare il numero massimo di tabelle di origine da caricare in parallelo. AWS DMS carica ogni tabella nella corrispondente tabella di destinazione di Kafka utilizzando una sottoattività dedicata. Il valore predefinito è 8; il valore il massimo è 49.
- `ParallelLoadThreads`— Utilizzate questa opzione per specificare il numero di thread da utilizzare per caricare ogni tabella nella relativa tabella di destinazione Kafka. AWS DMS Il valore massimo per una destinazione Apache Kafka è 32. Puoi chiedere che questo limite massimo venga aumentato.
- `ParallelLoadBufferSize`: utilizza questa opzione per specificare il numero massimo di record da archiviare nel buffer usato dai thread di caricamento parallelo per caricare i dati nella destinazione Kafka. Il valore predefinito è 50. Il valore massimo è 1.000. Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread.

- `ParallelLoadQueuesPerThread`: utilizza questa opzione per specificare il numero di code a cui accede ogni thread simultaneo per eliminare i record di dati dalle code e generare un carico batch per la destinazione. Il valore di default è 1. Il numero massimo è 512.

È possibile migliorare le prestazioni dell'acquisizione dei dati di modifica (CDC) per gli endpoint Kafka ottimizzando le impostazioni delle attività per thread paralleli e operazioni in blocco. A tale scopo, è possibile specificare il numero di thread simultanei, di code per thread e di record da memorizzare in un buffer utilizzando le impostazioni delle attività `ParallelApply*`. Ad esempio, si supponga di voler eseguire un carico CDC e applicare 128 thread in parallelo. Si desidera inoltre accedere a 64 code per thread, con 50 record memorizzati per buffer.

Per promuovere le prestazioni del CDC, AWS DMS supporta le seguenti impostazioni delle attività:

- `ParallelApplyThreads`— specifica il numero di thread simultanei che vengono AWS DMS utilizzati durante un caricamento CDC per inviare i record di dati a un endpoint di destinazione Kafka. Il valore predefinito è zero (0) e il valore massimo è 32.
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per eseguire il push dei thread simultanei a un endpoint di destinazione Kafka durante un carico CDC. Il valore predefinito è 100 e il valore massimo è 1.000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per eliminare i record di dati dalle code e generare un carico batch per un endpoint Kafka durante la CDC. Il valore di default è 1. Il numero massimo è 512.

Quando si utilizzano le impostazioni delle attività `ParallelApply*`, l'impostazione di `partition-key-type` predefinita è la `primary-key` della tabella, non `schema-name.table-name`.

Connessione a Kafka utilizzando Transport Layer Security (TLS)

Il cluster Kafka accetta solo connessioni protette con Transport Layer Security (TLS). Con DMS, è possibile utilizzare una qualsiasi delle seguenti tre opzioni di protocollo di sicurezza per proteggere la connessione degli endpoint Kafka.

Crittografia SSL (**server-encryption**)

I client convalidano l'identità del server tramite il certificato del server. Quindi viene stabilita una connessione crittografata tra server e client.

Autenticazione SSL (**mutual-authentication**)

Server e client convalidano l'identità reciprocamente tramite i propri certificati. Quindi viene stabilita una connessione crittografata tra server e client.

SASL-SSL (**mutual-authentication**)

Il metodo Simple Authentication and Security Layer (SASL) sostituisce il certificato del client con un nome utente e una password per convalidare l'identità del client. In particolare, si forniscono un nome utente e una password registrati dal server in modo che il server possa convalidare l'identità del client. Quindi viene stabilita una connessione crittografata tra server e client.

Important

Apache Kafka e Amazon MSK accettano certificati risolti. Questa è una limitazione nota di Kafka e Amazon MSK da risolvere. Per ulteriori informazioni, consulta [Apache Kafka issues, KAFKA-3700](#).

Se utilizzi Amazon MSK, prendi in considerazione le liste di controllo degli accessi (ACL) come soluzione alternativa a questa limitazione nota. Per ulteriori informazioni sull'utilizzo delle ACL, consulta la sezione [ACL Apache Kafka](#) nella Guida per gli sviluppatori di Streaming gestito da Amazon per Apache Kafka.

Se utilizzi un cluster Kafka autogestito, consulta il [commento datato 21 ottobre 2018](#) per informazioni sulla configurazione del cluster.

Utilizzo della crittografia SSL con Amazon MSK o un cluster Kafka autogestito

È possibile utilizzare la crittografia SSL per proteggere la connessione di un endpoint ad Amazon MSK o a un cluster Kafka autogestito. Quando usi il metodo di autenticazione con crittografia SSL, i client convalidano l'identità di un server tramite il certificato del server. Quindi viene stabilita una connessione crittografata tra server e client.

Per utilizzare la crittografia SSL per connettersi ad Amazon MSK

- Configura l'impostazione dell'endpoint del protocollo di sicurezza (`SecurityProtocol`) utilizzando l'opzione `ssl-encryption` quando crei l'endpoint Kafka di destinazione.

L'esempio JSON che segue imposta il protocollo di sicurezza come crittografia SSL.

```
"KafkaSettings": {  
  "SecurityProtocol": "ssl-encryption",  
}
```

Per utilizzare la crittografia SSL per un cluster Kafka autogestito

1. Se utilizzi un'autorità di certificazione (CA, Certification Authority) privata nel cluster Kafka on-premise, carica il certificato CA privato e ottieni un nome della risorsa Amazon (ARN).
2. Configura l'impostazione dell'endpoint del protocollo di sicurezza (`SecurityProtocol`) utilizzando l'opzione `ssl-encryption` quando crei l'endpoint Kafka di destinazione. L'esempio JSON che segue imposta il protocollo di sicurezza come `ssl-encryption`.

```
"KafkaSettings": {  
  "SecurityProtocol": "ssl-encryption",  
}
```

3. Se utilizzi una CA privata, imposta `SslCaCertificateArn` nell'ARN che hai ottenuto nella prima fase precedente.

Utilizzo dell'autenticazione SSL

È possibile utilizzare l'autenticazione SSL per proteggere la connessione di un endpoint ad Amazon MSK o a un cluster Kafka autogestito.

Per abilitare l'autenticazione e la crittografia del client utilizzando l'autenticazione SSL per la connessione ad Amazon MSK, procedi come segue:

- Prepara una chiave privata e un certificato pubblico per Kafka.
- Carica i certificati nella gestione certificati DMS.
- Crea un endpoint di destinazione Kafka con i corrispondenti ARN di certificati specificati nelle impostazioni degli endpoint Kafka.

Per preparare una chiave privata e un certificato pubblico per Amazon MSK

1. Crea un'istanza EC2 e configura un client per utilizzare l'autenticazione come descritto nelle fasi da 1 a 9 della sezione [Client Authentication](#) della Guida per sviluppatori di Streaming gestito da Amazon per Apache Kafka.

Dopo aver completato queste fasi, avrai un Certificate-ARN (l'ARN del certificato pubblico salvato in ACM) e una chiave privata contenuta in un file `kafka.client.keystore.jks`.

2. Recupera il certificato pubblico e copia il certificato nel file `signed-certificate-from-acm.pem` utilizzando il comando seguente:

```
aws acm-pca get-certificate --certificate-authority-arn Private_CA_ARN --
certificate-arn Certificate_ARN
```

Il comando restituisce informazioni simili a quelle mostrate nell'esempio seguente:

```
{"Certificate": "123", "CertificateChain": "456"}
```

Quindi copia l'equivalente di "123" nel file `signed-certificate-from-acm.pem`.

3. Recupera la chiave privata importando la chiave `msk-rsa` da `kafka.client.keystore.jks` to `keystore.p12`, come mostrato nel seguente esempio.

```
keytool -importkeystore \
-srckeystore kafka.client.keystore.jks \
-destkeystore keystore.p12 \
-deststoretype PKCS12 \
-srcalias msk-rsa-client \
-deststorepass test1234 \
-destkeypass test1234
```

4. Utilizza il comando seguente per esportare `keystore.p12` nel formato `.pem`.

```
openssl pkcs12 -in keystore.p12 -out encrypted-private-client-key.pem -nocerts
```

Viene visualizzato il messaggio `Enter PEM pass phrase` che richiede la chiave applicata per crittografare il certificato.

5. Rimuovi gli attributi contenitore e gli attributi chiave dal file `.pem` per assicurarti che la prima riga inizi con la stringa seguente.

```
---BEGIN ENCRYPTED PRIVATE KEY---
```

Per caricare un certificato pubblico e una chiave privata nella gestione certificati DMS e testare la connessione ad Amazon MSK

1. Carica nella gestione certificati DMS utilizzando il comando seguente.

```
aws dms import-certificate --certificate-identifier signed-cert --certificate-pem
file://path to signed cert
aws dms import-certificate --certificate-identifier private-key --certificate-pem
file://path to private key
```

2. Crea un endpoint di destinazione Amazon MSK e verifica la connessione per assicurarti che l'autenticazione TLS funzioni.

```
aws dms create-endpoint --endpoint-identifier $endpoint-identifier --engine-name
kafka --endpoint-type target --kafka-settings
'{"Broker": "b-0.kafka260.aaaaa1.a99.kafka.us-east-1.amazonaws.com:0000",
"SecurityProtocol": "ssl-authentication",
"SslClientCertificateArn": "arn:aws:dms:us-east-1:012346789012:cert:",
"SslClientKeyArn": "arn:aws:dms:us-
east-1:0123456789012:cert:", "SslClientKeyPassword": "test1234"}'
aws dms test-connection -replication-instance-arn=$rep_inst_arn --endpoint-arn=
$kafka_tar_arn_msk
```

Important

È possibile utilizzare l'autenticazione SSL per proteggere una connessione a un cluster Kafka autogestito. In alcuni casi, si potrebbe utilizzare un'autorità di certificazione (CA) privata nel cluster Kafka on-premise. In tal caso, carica la catena di CA, il certificato pubblico e la chiave privata nella gestione certificati DMS. Quindi, utilizza il corrispondente nome della risorsa Amazon (ARN) nelle impostazioni degli endpoint quando crei l'endpoint di destinazione Kafka on-premise.

Per preparare una chiave privata e un certificato firmato per un cluster Kafka autogestito

1. Genera una coppia di chiavi come nel seguente esempio.

```
keytool -genkey -keystore kafka.server.keystore.jks -validity 300 -storepass your-keystore-password
-keypass your-key-passphrase -dname "CN=your-cn-name"
-alias alias-of-key-pair -storetype pkcs12 -keyalg RSA
```

2. Genera una richiesta di firma del certificato (CSR, Certificate Sign Request).

```
keytool -keystore kafka.server.keystore.jks -certreq -file server-cert-sign-request-rsa -alias on-premise-rsa -storepass your-key-store-password
-keypass your-key-password
```

3. Usa la CA nel truststore del cluster per firmare la CSR. Se non disponi di una CA, puoi creare una CA privata.

```
openssl req -new -x509 -keyout ca-key -out ca-cert -days validate-days
```

4. Importa `ca-cert` nel truststore e nel keystore del server. Se non si dispone di un truststore, utilizza il comando seguente per crearlo e importare `ca-cert` .

```
keytool -keystore kafka.server.truststore.jks -alias CARoot -import -file ca-cert
keytool -keystore kafka.server.keystore.jks -alias CARoot -import -file ca-cert
```

5. Firma il certificato.

```
openssl x509 -req -CA ca-cert -CAkey ca-key -in server-cert-sign-request-rsa -out signed-server-certificate.pem
-days validate-days -CAcreateserial -passin pass:ca-password
```

6. Importa il certificato firmato nel keystore.

```
keytool -keystore kafka.server.keystore.jks -import -file signed-certificate.pem -
alias on-premise-rsa -storepass your-keystore-password
-keypass your-key-password
```

7. Utilizza il seguente comando per importare la chiave `on-premise-rsa` da `kafka.server.keystore.jks` a `keystore.p12`.

```
keytool -importkeystore \
-srckeystore kafka.server.keystore.jks \
-destkeystore keystore.p12 \
-deststoretype PKCS12 \
-srcalias on-premise-rsa \
-deststorepass your-truststore-password \
-destkeypass your-key-password
```

8. Utilizza il comando seguente per esportare `keystore.p12` nel formato `.pem`.

```
openssl pkcs12 -in keystore.p12 -out encrypted-private-server-key.pem -nocerts
```

9. Carica `encrypted-private-server-key.pem` e `signed-certificate.pem` e `ca-cert` nella gestione certificati DMS.
10. Crea un endpoint utilizzando gli ARN restituiti.

```
aws dms create-endpoint --endpoint-identifier $endpoint-identifier --engine-name
kafka --endpoint-type target --kafka-settings
'{"Broker": "b-0.kafka260.aaaaa1.a99.kafka.us-east-1.amazonaws.com:9092",
"SecurityProtocol": "ssl-authentication",
"SslClientCertificateArn": "your-client-cert-arn", "SslClientKeyArn": "your-client-
key-arn", "SslClientKeyPassword": "your-client-key-password",
"SslCaCertificateArn": "your-ca-certificate-arn"}'
```

```
aws dms test-connection -replication-instance-arn=$rep_inst_arn --endpoint-arn=
$kafka_tar_arn_msk
```

Utilizzo dell'autenticazione SASL-SSL per connettersi ad Amazon MSK

Il metodo Simple Authentication and Security Layer (SASL) utilizza un nome utente e una password per convalidare l'identità di un client e stabilisce una connessione crittografata tra server e client.

Per utilizzare SASL, devi prima creare un nome utente e una password sicuri quando configuri il cluster Amazon MSK. Per una descrizione di come configurare un nome utente e una password sicuri per un cluster Amazon MSK, consulta [Configurazione dell'autenticazione SASL/SCRAM per un cluster Amazon MSK](#) nella Guida per sviluppatori di Streaming gestito da Amazon per Apache Kafka.

Quindi, quando crei l'endpoint di destinazione Kafka, imposta l'impostazione dell'endpoint del protocollo di sicurezza (`SecurityProtocol`) utilizzando l'opzione `sasl-ssl`. Imposti anche le opzioni `SaslUsername` e `SaslPassword`. Assicurati che siano coerenti con il nome utente e la password sicuri creati durante la configurazione del cluster Amazon MSK, come mostrato nel seguente esempio JSON.

```
"KafkaSettings": {  
  "SecurityProtocol": "sasl-ssl",  
  "SaslUsername": "Amazon MSK cluster secure user name",  
  "SaslPassword": "Amazon MSK cluster secure password"  
}
```

Note

- Attualmente, supporta solo SASL-SSL pubblico supportato da CA AWS DMS . DMS non supporta SASL-SSL per l'uso con Kafka autogestito supportato da una CA privata.
- Per l'autenticazione SASL-SSL, AWS DMS supporta il meccanismo SCRAM-SHA-512 per impostazione predefinita. AWS DMS le versioni 3.5.0 e successive supportano anche il meccanismo Plain. Per supportare il meccanismo Plain, imposta il parametro `SaslMechanism` del tipo di dati API `KafkaSettings` su PLAIN.

Utilizzo di un'immagine precedente per visualizzare i valori originali delle righe CDC per Apache Kafka come destinazione

Quando si scrivono aggiornamenti CDC su una destinazione di streaming dati come Kafka, è possibile visualizzare i valori originali di una riga di database di origine prima di apportare modifiche

da un aggiornamento. Per rendere possibile ciò, AWS DMS compila un'immagine precedente degli eventi di aggiornamento sulla base dei dati forniti dal motore del database di origine.

Diversi motori di database di origine forniscono diverse quantità di informazioni per un'immagine precedente:

- Oracle fornisce aggiornamenti alle colonne solo se cambiano.
- PostgreSQL fornisce solo i dati per le colonne che fanno parte della chiave primaria (modificata o meno). Se è in uso la replica logica e REPLICATION IDENTITY FULL è impostato per la tabella di origine, è possibile ottenere informazioni complete prima e dopo sulla riga scritta e disponibile nei WAL.
- MySQL generalmente fornisce dati per tutte le colonne (modificate o meno).

Per consentire prima dell'imaging di aggiungere valori originali dal database di origine all'output AWS DMS, utilizzare l'impostazione dell'attività `BeforeImageSettings` o il parametro `add-before-image-columns`. Questo parametro applica una regola di trasformazione della colonna.

`BeforeImageSettings` aggiunge un nuovo attributo JSON a ogni operazione di aggiornamento con valori raccolti dal sistema di database di origine, come illustrato di seguito.

```
"BeforeImageSettings": {
  "EnableBeforeImage": boolean,
  "FieldName": string,
  "ColumnFilter": pk-only (default) / non-lob / all (but only one)
}
```

Note

Applicare `BeforeImageSettings` alle attività CDC a pieno carico e alle attività CDC (che eseguono la migrazione dei dati esistenti e replicano le modifiche in corso) o solo alle attività CDC (che replicano solo le modifiche dei dati). Non applicare `BeforeImageSettings` alle attività a pieno carico.

Per le opzioni `BeforeImageSettings`, si applica quanto segue:

- Impostare l'opzione `EnableBeforeImage` su `true` da abilitare prima dell'imaging. Il valore predefinito è `false`.
- Utilizzare l'opzione `FieldName` per assegnare un nome al nuovo attributo JSON. Quando `EnableBeforeImage` è `true`, `FieldName` è richiesto e non può essere vuoto.
- L'opzione `ColumnFilter` specifica una colonna da aggiungere utilizzando l'imaging precedente. Per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella, utilizzare il valore predefinito, `pk-only`. Per aggiungere solo colonne non di tipo LOB, utilizzare `non-lob`. Per aggiungere qualsiasi colonna con un valore immagine prima, utilizzare `all`.

```
"BeforeImageSettings": {  
  "EnableBeforeImage": true,  
  "FieldName": "before-image",  
  "ColumnFilter": "pk-only"  
}
```

Utilizzo di una regola di trasformazione dell'immagine precedente

In alternativa alle impostazioni delle attività, è possibile utilizzare il parametro `add-before-image-columns`, che applica una regola di trasformazione delle colonne. Con questo parametro, è possibile abilitare l'imaging precedente durante il CDC su destinazioni di streaming dati come Kafka.

Utilizzando `add-before-image-columns` in una regola di trasformazione, è possibile applicare un controllo più dettagliato dei risultati dell'immagine precedente. Le regole di trasformazione consentono di utilizzare un localizzatore di oggetti che consente di controllare le tabelle selezionate per la regola. Inoltre, è possibile concatenare le regole di trasformazione, consentendo l'applicazione di regole diverse a tabelle diverse. È quindi possibile manipolare le colonne prodotte utilizzando altre regole.

Note

Non utilizzare il parametro `add-before-image-columns` insieme all'impostazione dell'attività `BeforeImageSettings` all'interno della stessa attività. Utilizzare invece il parametro o l'impostazione, ma non entrambi, per una singola attività.

Un tipo di regola `transformation` regola con il parametro `add-before-image-columns` per una colonna deve fornire una sezione `before-image-def`. Di seguito viene riportato un esempio.

```
{
  "rule-type": "transformation",
  ...
  "rule-target": "column",
  "rule-action": "add-before-image-columns",
  "before-image-def": {
    "column-filter": one-of (pk-only / non-lob / all),
    "column-prefix": string,
    "column-suffix": string,
  }
}
```

Il valore di `column-prefix` viene anteposto a un nome di colonna e il valore predefinito di `column-prefix` è `BI_`. Il valore di `column-suffix` viene aggiunto al nome della colonna e il valore predefinito è vuoto. Non impostare sia `column-prefix` sia `column-suffix` sull'opzione per svuotare le stringhe.

Scegliere un valore per `column-filter`. Per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella, scegliere `pk-only`. Scegliere `non-lob` per aggiungere solo colonne non di tipo LOB. Oppure scegliere `all` per aggiungere qualsiasi colonna con un valore immagine precedente.

Esempio di una regola di trasformazione dell'immagine precedente

La regola di trasformazione nell'esempio seguente aggiunge una nuova colonna chiamata `BI_emp_no` nella destinazione. Quindi una dichiarazione come `UPDATE employees SET emp_no = 3 WHERE emp_no = 1`; popola il campo `BI_emp_no` con 1. Quando si scrivono aggiornamenti CDC alle destinazioni Amazon S3, la colonna `BI_emp_no` indica quale riga originale è stata aggiornata.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "%",
        "table-name": "%"
      },
      "rule-action": "include"
    }
  ]
}
```

```
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-target": "column",
      "object-locator": {
        "schema-name": "%",
        "table-name": "employees"
      },
      "rule-action": "add-before-image-columns",
      "before-image-def": {
        "column-prefix": "BI_",
        "column-suffix": "",
        "column-filter": "pk-only"
      }
    }
  ]
}
```

Per informazioni sull'utilizzo dell'operazione della regola `add-before-image-columns`, consulta [Operazioni e regole di trasformazione](#).

Limitazioni nell'utilizzo di Apache Kafka come destinazione per AWS Database Migration Service

Utilizzando Apache Kafka come destinazione valgono le seguenti limitazioni:

- AWS DMS Gli endpoint target Kafka non supportano il controllo degli accessi IAM per Amazon Managed Streaming for Apache Kafka (Amazon MSK).
- La modalità LOB completa non è supportata.
- Specificate un file di configurazione Kafka per il vostro cluster con proprietà che consentano di creare automaticamente nuovi argomenti. AWS DMS Include l'impostazione `auto.create.topics.enable = true`. Se si utilizza Amazon MSK, è possibile specificare la configurazione predefinita alla creazione del cluster Kafka, quindi modificare l'impostazione `auto.create.topics.enable` su `true`. Per ulteriori informazioni sulle impostazioni di configurazione predefinite, consulta [La configurazione predefinita di Amazon MSK](#) nella Guida per gli sviluppatori di Streaming gestito da Amazon per Apache Kafka. Se devi modificare un cluster Kafka esistente creato utilizzando Amazon MSK, esegui il AWS CLI comando `aws kafka create-configuration` per aggiornare la configurazione di Kafka, come nell'esempio seguente:

```
14:38:41 $ aws kafka create-configuration --name "kafka-configuration" --kafka-versions "2.2.1" --server-properties file://~/kafka_configuration
{
  "LatestRevision": {
    "Revision": 1,
    "CreationTime": "2019-09-06T14:39:37.708Z"
  },
  "CreationTime": "2019-09-06T14:39:37.708Z",
  "Name": "kafka-configuration",
  "Arn": "arn:aws:kafka:us-east-1:111122223333:configuration/kafka-configuration/7e008070-6a08-445f-9fe5-36ccf630ecfd-3"
}
```

Qui, `~/kafka_configuration` è il file di configurazione creato con le impostazioni delle proprietà richieste.

Se utilizzi la tua istanza Kafka installata su Amazon EC2, modifica la configurazione del cluster Kafka con l'impostazione per AWS DMS consentire `auto.create.topics.enable = true` la creazione automatica di nuovi argomenti, utilizzando le opzioni fornite con l'istanza.

- AWS DMS pubblica ogni aggiornamento di un singolo record nel database di origine come un unico record di dati (messaggio) in un determinato argomento Kafka indipendentemente dalle transazioni.
- AWS DMS supporta i seguenti due moduli per le chiavi di partizione:
 - `SchemaName.TableName`: una combinazione del nome dello schema e quello della tabella.
 - `${AttributeName}`: il valore di uno dei campi nel formato JSON o la chiave primaria della tabella del database di origine.
- `BatchApply` non è supportato per un endpoint Kafka. L'utilizzo dell'applicazione in batch, ad esempio l'impostazione dell'attività dei metadati di destinazione `BatchApplyEnabled`, per una destinazione Kafka potrebbe causare la perdita di dati.
- AWS DMS non supporta la migrazione di valori di tipo di `BigInt` dati con più di 16 cifre. Per aggirare questa limitazione puoi utilizzare la seguente regola di trasformazione per convertire la colonna `BigInt` in una stringa. Per ulteriori informazioni sulle regole di trasformazione, consulta [Operazioni e regole di trasformazione](#).

```
{
  "rule-type": "transformation",
  "rule-id": "id",
  "rule-name": "name",
```

```
"rule-target": "column",
"object-locator": {
  "schema-name": "valid object-mapping rule action",
  "table-name": "",
  "column-name": ""
},
"rule-action": "change-data-type",
"data-type": {
  "type": "string",
  "length": 20
}
}
```

Utilizzo della mappatura degli oggetti per la migrazione dei dati in un argomento Kafka

AWS DMS utilizza regole di mappatura delle tabelle per mappare i dati dall'argomento Kafka di origine a quello di destinazione. Per mappare i dati a un argomento di destinazione, è necessario utilizzare una regola di mappatura delle tabelle denominata mappatura degli oggetti. La mappatura degli oggetti consente di definire il modo in cui i record di dati nell'origine vengono mappati ai record di dati pubblicati nell'argomento Kafka.

Gli argomenti Kafka non dispongono di una struttura preimpostata oltre a una chiave di partizione.

Note

Non è necessario utilizzare la mappatura degli oggetti. È possibile utilizzare la normale mappatura delle tabelle per varie trasformazioni. Tuttavia, il tipo di chiave della partizione segue questi comportamenti predefiniti:

- La chiave primaria viene utilizzata come chiave di partizione per il pieno carico.
- Se non vengono utilizzate impostazioni delle attività di applicazione parallela, `schema.table` viene utilizzato come chiave di partizione per CDC.
- Se vengono utilizzate le impostazioni delle attività di applicazione parallela, la chiave primaria viene utilizzata come chiave di partizione per CDC.

Per creare una regola di mappatura degli oggetti, è necessario impostare il parametro `rule-type` su `object-mapping`. Questa regola specifica il tipo di mappatura degli oggetti da utilizzare.

Di seguito è riportata la struttura per la regola.

```
{
  "rules": [
    {
      "rule-type": "object-mapping",
      "rule-id": "id",
      "rule-name": "name",
      "rule-action": "valid object-mapping rule action",
      "object-locator": {
        "schema-name": "case-sensitive schema name",
        "table-name": ""
      }
    }
  ]
}
```

AWS DMS attualmente supporta `map-record-to-record` e `map-record-to-document` è l'unico valore valido per il parametro `rule-action`. Queste impostazioni influiscono sui valori che non sono esclusi come parte dell'elenco degli attributi `exclude-columns`. I `map-record-to-document` valori `map-record-to-record` and specificano come AWS DMS gestisce questi record per impostazione predefinita. Questi valori non influiscono in alcun modo sulle mappature degli attributi.

Nel caso di migrazione da un database relazionale a un argomento Kafka utilizza `map-record-to-record`. Questo tipo di regola utilizza il valore `taskResourceId.schemaName.tableName` dal database relazionale come chiave di partizione nell'argomento Kafka e crea un attributo per ogni colonna nel database di origine.

Quando utilizzi `map-record-to-record`, tieni presente quanto segue:

- Questa impostazione ha effetto solo sulle colonne escluse dall'elenco `exclude-columns`.
- Per ogni colonna di questo tipo, AWS DMS crea un attributo corrispondente nell'argomento di destinazione.
- AWS DMS crea questo attributo corrispondente indipendentemente dal fatto che la colonna di origine venga utilizzata in una mappatura degli attributi.

Per comprendere il funzionamento di `map-record-to-record`, è opportuno esaminarne il comportamento in azione. Per questo esempio, supponiamo che tu stia iniziando con una riga di tabella del database relazionale con la struttura e i dati seguenti.

FirstName	LastName	StoreId	HomeAddress	HomePhone	WorkAddress	WorkPhone	DateofBirth
Randy	Marsh	5	221B Baker Street	123456789 0	31 Spooner Street, Quahog	987654321 0	02/29/198 8

Per eseguire la migrazione di queste informazioni da uno schema denominato `Test` verso un argomento `Kafka`, crea le regole per mappare i dati sull'argomento di destinazione. La regola seguente illustra la mappatura.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "DefaultMapToKafka",
      "rule-action": "map-record-to-record",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customers"
      }
    }
  ]
}
```

Dato un argomento Kafka e una chiave di partizione (in questo caso, `taskResourceId.schemaName.tableName`), il seguente esempio illustra il formato di record risultante per l'argomento di destinazione Kafka utilizzando i dati di esempio:

```
{
  "FirstName": "Randy",
  "LastName": "Marsh",
  "StoreId": "5",
  "HomeAddress": "221B Baker Street",
  "HomePhone": "1234567890",
  "WorkAddress": "31 Spooner Street, Quahog",
  "WorkPhone": "9876543210",
  "DateOfBirth": "02/29/1988"
}
```

Argomenti

- [Ristrutturazione dei dati con la mappatura degli attributi](#)
- [Replica di più argomenti con la mappatura degli oggetti](#)
- [Formato dei messaggi per Apache Kafka](#)

Ristrutturazione dei dati con la mappatura degli attributi

Utilizzando una mappa degli attributi puoi modificare la struttura dei dati mentre li stai migrando verso un argomento Kafka. Ad esempio, potresti voler combinare più campi nell'origine in un unico campo nella destinazione. La seguente mappa degli attributi illustra come ristrutturare i dati.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    }
  ],
  {
```



```
"rule-type": "object-mapping",
"rule-id": "2",
"rule-name": "TransformToKafka",
"rule-action": "map-record-to-record",
"target-table-name": "CustomerData",
"object-locator": {
  "schema-name": "Test",
  "table-name": "Customers"
},
"mapping-parameters": {
  "partition-key-type": "attribute-name",
  "partition-key-name": "CustomerName",
  "exclude-columns": [
    "firstname",
    "lastname",
    "homeaddress",
    "homephone",
    "workaddress",
    "workphone"
  ],
  "attribute-mappings": [
    {
      "target-attribute-name": "CustomerName",
      "attribute-type": "scalar",
      "attribute-sub-type": "string",
      "value": "${lastname}, ${firstname}"
    },
    {
      "target-attribute-name": "ContactDetails",
      "attribute-type": "document",
      "attribute-sub-type": "json",
      "value": {
        "Home": {
          "Address": "${homeaddress}",
          "Phone": "${homephone}"
        },
        "Work": {
          "Address": "${workaddress}",
          "Phone": "${workphone}"
        }
      }
    }
  ]
}
```

```

    }
  ]
}

```

Per impostare un valore costante per `partition-key`, specificare un valore `partition-key`. Ad esempio, potresti eseguire questa operazione per forzare la memorizzazione di tutti i dati in una singola partizione. Questo approccio viene illustrato nella mappatura seguente.

```

{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "1",
      "rule-name": "TransformToKafka",
      "rule-action": "map-record-to-document",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customer"
      },
      "mapping-parameters": {
        "partition-key": {
          "value": "ConstantPartitionKey"
        },
        "exclude-columns": [
          "FirstName",
          "LastName",
          "HomeAddress",
          "HomePhone",
          "WorkAddress",
          "WorkPhone"
        ],
        "attribute-mappings": [
          {

```


- quello specificato da `kafka-default-topic` se il campo Argomento dell'endpoint di destinazione non è compilato e l'impostazione Kafka `auto.create.topics.enable` è impostata su `true`.

Con le versioni AWS DMS del motore 3.4.6 e successive, è possibile utilizzare l'`kafka-target-topic` attributo per mappare ogni tabella di origine migrata su un argomento separato. Ad esempio, le regole di mappatura degli oggetti riportate di seguito migrano le tabelle di origine `Customer` e `Address` agli argomenti Kafka `customer_topic` e `address_topic` rispettivamente. Allo stesso tempo, AWS DMS migra tutte le altre tabelle di origine, inclusa la `Bills` tabella nello `Test` schema, all'argomento specificato nell'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "MapToKafka1",
      "rule-action": "map-record-to-record",
      "kafka-target-topic": "customer_topic",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customer"
      },
      "partition-key": {"value": "ConstantPartitionKey" }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "3",
      "rule-name": "MapToKafka2",
      "rule-action": "map-record-to-record",
      "kafka-target-topic": "address_topic",
```

```
    "object-locator": {
      "schema-name": "Test",
      "table-name": "Address"
    },
    "partition-key": {"value": "HomeAddress" }
  },
  {
    "rule-type": "object-mapping",
    "rule-id": "4",
    "rule-name": "DefaultMapToKafka",
    "rule-action": "map-record-to-record",
    "object-locator": {
      "schema-name": "Test",
      "table-name": "Bills"
    }
  }
]
```

Utilizzando la replica di più argomenti Kafka, è possibile raggruppare e migrare le tabelle di origine su argomenti Kafka separati utilizzando un'unica attività di replica.

Formato dei messaggi per Apache Kafka

L'output JSON è semplicemente un elenco di coppie chiave-valore.

RecordType

Il tipo di record può essere relativo ai dati o al controllo. I record di dati rappresentano le righe effettive nell'origine. I record di controllo sono per eventi importanti nel flusso, ad esempio un riavvio dell'attività.

Operazione

Per i record di dati, l'operazione può essere load, insert, update o delete.

Per i record di controllo, l'operazione può essere create-table, rename-table, drop-table, change-columns, add-column, drop-column, rename-column o column-type-change.

SchemaName

Lo schema di origine per il record. Questo campo può essere vuoto per un record di controllo.

TableName

La tabella di origine per il record. Questo campo può essere vuoto per un record di controllo.

Timestamp

Il timestamp relativo al momento della creazione del messaggio JSON. Il campo viene formattato con il formato ISO 8601.

Il seguente esempio di messaggio JSON illustra un tipo di dati con tutti i metadati aggiuntivi.

```
{
  "data":{
    "id":100000161,
    "fname":"val61s",
    "lname":"val61s",
    "REGION":"val61s"
  },
  "metadata":{
    "timestamp":"2019-10-31T22:53:59.721201Z",
    "record-type":"data",
    "operation":"insert",
    "partition-key-type":"primary-key",
    "partition-key-value":"sbtest.sbtest_x.100000161",
    "schema-name":"sbtest",
    "table-name":"sbtest_x",
    "transaction-id":9324410911751,
    "transaction-record-id":1,
    "prev-transaction-id":9324410910341,
    "prev-transaction-record-id":10,
    "commit-timestamp":"2019-10-31T22:53:55.000000Z",
    "stream-position":"mysql-bin-
changelog.002171:36912271:0:36912333:9324410911751:mysql-bin-changelog.002171:36912209"
  }
}
```

Il seguente esempio di messaggio JSON illustra un tipo di controllo.

```
{
  "control":{
    "table-def":{
      "columns":{
```

```
    "id":{
      "type":"WSTRING",
      "length":512,
      "nullable":false
    },
    "fname":{
      "type":"WSTRING",
      "length":255,
      "nullable":true
    },
    "lname":{
      "type":"WSTRING",
      "length":255,
      "nullable":true
    },
    "REGION":{
      "type":"WSTRING",
      "length":1000,
      "nullable":true
    }
  },
  "primary-key":[
    "id"
  ],
  "collation-name":"latin1_swedish_ci"
}
},
"metadata":{
  "timestamp":"2019-11-21T19:14:22.223792Z",
  "record-type":"control",
  "operation":"create-table",
  "partition-key-type":"task-id",
  "schema-name":"sbtest",
  "table-name":"sbtest_t1"
}
}
```

Utilizzo di un cluster del servizio OpenSearch di Amazon come destinazione per AWS Database Migration Service

È possibile utilizzare AWS DMS per migrare i dati nel servizio OpenSearch di Amazon (servizio OpenSearch). OpenSearch è un servizio gestito che consente di implementare, utilizzare e dimensionare i cluster del servizio OpenSearch.

Nel servizio OpenSearch è possibile utilizzare indici e documenti. Un indice è una raccolta di documenti e un documento è un oggetto JSON contenente valori scalari, matrici e altri oggetti. OpenSearch fornisce un linguaggio di query basato su JSON, in modo da poter eseguire le query sui dati di un indice e recuperare i documenti corrispondenti.

Quando AWS DMS crea gli indici per un endpoint di destinazione del servizio OpenSearch, viene creato un indice per ogni tabella dall'endpoint di origine. Il costo per la creazione di un indice del servizio OpenSearch dipende da diversi fattori. Tali fattori sono il numero di indici creati, la quantità totale di dati in questi indici e la piccola quantità di metadati che OpenSearch archivia per ogni documento.

Configura il cluster del servizio OpenSearch con risorse di calcolo e storage appropriate per l'ambito della migrazione. È consigliabile considerare i seguenti fattori, a seconda dell'attività di replica che desideri utilizzare:

- Per un caricamento di dati completo, considera la quantità totale di dati da migrare, nonché la velocità del trasferimento.
- Per la replica di modifiche in corso, considera la frequenza degli aggiornamenti e i requisiti di latenza end-to-end.

Inoltre, configura le impostazioni dell'indice sul cluster OpenSearch, prestando molta attenzione al conteggio dei documenti.

Impostazioni attività a pieno carico multithread

Per contribuire ad aumentare la velocità di trasferimento, AWS DMS supporta il pieno carico multithread su un cluster di destinazione del servizio OpenSearch. AWS DMS supporta questo multithreading con le seguenti impostazioni delle attività:

- `MaxFullLoadSubTasks`: imposta questa opzione per indicare il numero massimo di tabelle da caricare in parallelo. DMS consente di caricare ogni tabella nell'indice di destinazione del servizio

OpenSearch corrispondente utilizzando una attività secondaria dedicata. Il valore predefinito è 8; il valore il massimo è 49.

- `ParallelLoadThreads`: imposta questa opzione per specificare il numero di thread che AWS DMS utilizza per caricare ogni tabella in un indice di destinazione del servizio OpenSearch. Il valore massimo per una destinazione del servizio OpenSearch è 32. Puoi chiedere che questo limite massimo venga aumentato.

Note

Se non si modifica il valore predefinito di `ParallelLoadThreads` (0), AWS DMS trasferisce un singolo record alla volta. Questo approccio pone un carico non richiesto nel cluster del servizio OpenSearch. Assicurati di impostare questa opzione per 1 o più.

- `ParallelLoadBufferSize`: imposta questa opzione per specificare il numero massimo di record da archiviare nel buffer utilizzato dai thread di caricamento parallelo per caricare i dati nella destinazione del servizio OpenSearch. Il valore predefinito è 50. Il valore massimo è 1.000. Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread.

Per ulteriori informazioni su come DMS consente di caricare un cluster del servizio OpenSearch utilizzando il multithreading, consulta il post del blog AWS [Scale Amazon OpenSearch Service for AWS Database Migration Service migrations](#).

Impostazioni attività di carico CDC multithread

È possibile migliorare le prestazioni dell'acquisizione dei dati di modifica (CDC) per un cluster di destinazione del servizio OpenSearch utilizzando le impostazioni delle attività per modificare il comportamento della chiamata API `PutRecords`. A tale scopo, è possibile specificare il numero di thread simultanei, di code per thread e di record da memorizzare in un buffer utilizzando le impostazioni delle attività `ParallelApply*`. Ad esempio, si supponga di voler eseguire un carico CDC e applicare 32 thread in parallelo. Si desidera inoltre accedere a 64 code per thread, con 50 record memorizzati per buffer.

Note

Il supporto per l'uso delle impostazioni delle attività `ParallelApply*` durante la CDC negli endpoint di destinazione del servizio OpenSearch di Amazon è disponibile in AWS DMS 3.4.0 e versioni successive.

Per promuovere le prestazioni del CDC, AWS DMS supporta le seguenti impostazioni di attività:

- `ParallelApplyThreads`: specifica il numero di thread simultanei utilizzati da AWS DMS durante un carico CDC per eseguire il push di record di dati a un endpoint di destinazione del servizio OpenSearch. Il valore predefinito è zero (0) e il valore massimo è 32.
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per il push di thread simultanei a un endpoint di destinazione del servizio OpenSearch durante un carico CDC. Il valore predefinito è 100 e il valore massimo è 1.000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per eliminare i record di dati dalle code e generare un carico batch per un endpoint del servizio OpenSearch durante CDC.

Quando si utilizzano le impostazioni delle attività `ParallelApply*`, l'impostazione di `partition-key-type` predefinita è la `primary-key` della tabella, non `schema-name.table-name`.

Migrazione da una tabella di database relazionale a un indice del servizio OpenSearch

AWS DMS supporta la migrazione dei dati a tipi di dati scalari del servizio OpenSearch. Durante la migrazione da un database relazionale, ad esempio Oracle o MySQL, al servizio OpenSearch, potresti voler ristrutturare il modo in cui vengono archiviati i dati.

AWS DMS supporta i seguenti tipi di dati scalari del servizio OpenSearch:

- Boolean
- Data
- Float
- Int
- Stringa

AWS DMS converte i dati di tipo Date nel tipo String. Puoi specificare la mappatura personalizzata per interpretare queste date.

AWS DMS non supporta la migrazione dei tipi di dati LOB.

Prerequisiti per l'utilizzo del servizio OpenSearch di Amazon come destinazione per AWS Database Migration Service

Prima di iniziare a utilizzare un database del servizio OpenSearch come destinazione per AWS DMS, è necessario creare un ruolo AWS Identity and Access Management (IAM). Questo ruolo deve consentire a AWS DMS di accedere agli indici del servizio OpenSearch sull'endpoint di destinazione. Nella seguente policy IAM viene mostrato il set minimo di autorizzazioni di accesso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Il ruolo utilizzato per la migrazione al servizio OpenSearch deve disporre delle seguenti autorizzazioni.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:ESHttpDelete",
        "es:ESHttpGet",

```

```

        "es:ESHttpHead",
        "es:ESHttpPost",
        "es:ESHttpPut"
    ],
    "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
}
]
}

```

Nell'esempio precedente, sostituisci *region* con l'identificatore della regione AWS, *account-id* con l'ID dell'account AWS e *domain-name* con il nome del dominio del servizio OpenSearch di Amazon. Un esempio è `arn:aws:es:us-west-2:123456789012:domain/my-es-domain`

Impostazioni dell'endpoint quando si utilizza il servizio OpenSearch come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione del servizio OpenSearch in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--elasticsearch-settings '{"EndpointSetting": "value", ...}'`.

Nella tabella seguente vengono elencate le impostazioni degli endpoint che è possibile utilizzare con il servizio OpenSearch come destinazione.

Nome attributo	Valori validi	Valore predefinito e descrizione
FullLoadErrorPercentage	Un numero intero positivo maggiore di 0 ma non superiore a 100.	10 - Per un'attività di caricamento completo, questo attributo determina la soglia di errori consentita prima che l'attività abbia esito negativo. Ad esempio, supponiamo che vi siano 1.500 righe sull'endpoint di origine e che questo parametro sia impostato su 10. Quindi, l'attività ha esito negativo se AWS DMS rileva più di 150 errori (10 percento del conteggio di righe) quando si esegue l'operazione di scrittura sull'endpoint di destinazione.

Nome attributo	Valori validi	Valore predefinito e descrizione
ErrorRetryDuration	Un numero intero positivo maggiore di 0.	300 - Se si verifica un errore sull'endpoint di destinazione, AWS DMS tenta di nuovo per questo numero di secondi. In caso contrario, l'attività ha esito negativo.

Limitazioni all'utilizzo del servizio OpenSearch di Amazon come destinazione per AWS Database Migration Service

Quando si utilizza il servizio OpenSearch di Amazon come destinazione si applicano le seguenti limitazioni:

- Il servizio OpenSearch utilizza la mappatura dinamica (stima automatica) per determinare i tipi di dati da utilizzare per i dati migrati.
- Il servizio OpenSearch archivia ogni documento con un ID univoco. Di seguito è riportato un ID di esempio.

```
"_id": "D359F8B537F1888BC71FE20B3D79EAE6674BE7ACA9B645B0279C7015F6FF19FD"
```

Ogni ID documento è lungo 64 byte, quindi è possibile prevedere questo valore come requisito di storage. Ad esempio, se esegui la migrazione di 100.000 righe da un'origine AWS DMS, l'indice del servizio OpenSearch risultante richiede uno spazio di storage per ulteriori 6.400.000 byte.

- Con il servizio OpenSearch non puoi effettuare aggiornamenti agli attributi di chiave primaria. Questa restrizione è importante quando si utilizza la replica continua con l'acquisizione dei dati di modifica (CDC), perché può causare la presenza di dati indesiderati nella destinazione. In modalità CDC, le chiavi primarie sono mappate ai valori SHA256, che sono lunghi 32 byte. Questi vengono convertiti in stringhe a 64 byte leggibili e sono utilizzati come ID documento del servizio OpenSearch.
- Se AWS DMS rileva voci che non possono essere migrate, scrive e invia i messaggi di errore a File di log Amazon CloudWatch. Questo comportamento differisce da quello di altri endpoint di destinazione AWS DMS, che scrivono gli errori in una tabella di eccezioni.
- AWS DMS non supporta la connessione a un cluster Amazon ES con controllo granulare degli accessi abilitato con utente master e password.
- AWS DMS non supporta il servizio OpenSearch serverless.

- Il servizio OpenSearch non supporta la scrittura di dati in indici preesistenti.

Tipi di dati di destinazione per il servizio OpenSearch di Amazon

Quando AWS DMS esegue la migrazione dei dati da database eterogenei, il servizio mappa i tipi di dati dal database di origine ai tipi di dati intermedi, denominati tipi di dati AWS DMS. Il servizio mappa quindi i tipi di dati intermedi ai tipi di dati di destinazione. La seguente tabella mostra ciascun tipo di dati AWS DMS e il tipo di dati a cui viene mappato nel servizio OpenSearch.

Tipo di dati AWS DMS	Tipo di dati del servizio OpenSearch
Boolean	booleano
Data	stringa
Orario	date
Timestamp	date
INT4	integer
Real4	float
UINT4	integer

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service

Per informazioni sulle versioni di Amazon DocumentDB (compatibile con MongoDB) supportate da AWS DMS, consulta [Obiettivi per AWS DMS](#). Puoi utilizzare AWS DMS per eseguire la migrazione dei dati a Amazon DocumentDB (compatibile con MongoDB) da uno qualsiasi dei motori dei dati di origine supportati da AWS DMS. Il motore può essere in un servizio gestito da AWS, ad esempio Amazon RDS, Aurora o Amazon S3. In alternativa, il motore può essere un database autogestito, ad esempio MongoDB in esecuzione su Amazon EC2 o on-premise.

Puoi utilizzare AWS DMS per replicare i dati di origine in database, raccolte o documenti di Amazon DocumentDB.

Note

Se l'endpoint di origine è MongoDB o Amazon DocumentDB, esegui la migrazione in modalità documento.

MongoDB archivia i dati in formato JSON binario (BSON). AWS DMS supporta tutti i tipi di dati BSON previsti da Amazon DocumentDB. Per l'elenco di questi tipi di dati, consulta [Supported MongoDB APIs, operations, and data types](#) nella Guida per gli sviluppatori di Amazon DocumentDB.

Se l'endpoint di origine è un database relazionale, AWS DMS mappa gli oggetti di database ad Amazon DocumentDB come segue:

- Un database relazionale, o schema di database, viene mappato a un database Amazon DocumentDB.
- Le tabelle all'interno di un database relazionale vengono mappate a raccolte in Amazon DocumentDB.
- I record in una tabella relazionale vengono mappati a documenti in Amazon DocumentDB. Ogni documento viene costruito da dati nel record di origine.

Se l'endpoint di origine è Amazon S3, allora gli oggetti Amazon DocumentDB risultanti corrispondono a regole di mappatura AWS DMS per Amazon S3. Considera, ad esempio, l'URI seguente:

```
s3://mybucket/hr/employee
```

In questo caso, AWS DMS mappa gli oggetti in mybucket ad Amazon DocumentDB come segue:

- La parte URI di alto livello (hr) viene mappata a un database Amazon DocumentDB.
- La parte URI successiva (employee) viene mappata a una raccolta Amazon DocumentDB.
- Ogni oggetto in employee viene mappato a un documento in Amazon DocumentDB.

Per ulteriori informazioni sulle regole di mappatura per Amazon S3, consulta [Utilizzo di Amazon S3 come sorgente per AWS DMS](#).

Impostazioni degli endpoint Amazon DocumentDB

In AWS DMS 3.5.0 e versioni successive, puoi migliorare le prestazioni dell'acquisizione dei dati di modifica (CDC) per gli endpoint Amazon DocumentDB ottimizzando le impostazioni delle attività per thread paralleli e operazioni in blocco. A tale scopo, è possibile specificare il numero di thread simultanei, di code per thread e di record da memorizzare in un buffer utilizzando le impostazioni delle attività `ParallelApply*`. Ad esempio, si supponga di voler eseguire un carico CDC e applicare 128 thread in parallelo. Si desidera inoltre accedere a 64 code per thread, con 50 record memorizzati per buffer.

Per promuovere le prestazioni del CDC, AWS DMS supporta le seguenti impostazioni di attività:

- `ParallelApplyThreads`: specifica il numero di thread simultanei utilizzati da AWS DMS durante un carico CDC per eseguire il push dei record di dati a un endpoint di destinazione Amazon DocumentDB. Il valore predefinito è zero (0) e il valore massimo è 32.
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per eseguire il push dei thread simultanei a un endpoint di destinazione Amazon DocumentDB durante un carico CDC. Il valore predefinito è 100 e il valore massimo è 1.000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per eliminare i record di dati dalle code e generare un carico batch per un endpoint Amazon DocumentDB durante CDC. Il valore di default è 1. Il numero massimo è 512.

Per ulteriori dettagli sull'utilizzo di Amazon DocumentDB come destinazione per AWS DMS, consulta le seguenti sezioni:

Argomenti

- [Mappatura dei dati da un'origine a una destinazione Amazon DocumentDB](#)
- [Connessione ai cluster elastici Amazon DocumentDB come destinazione](#)
- [Replica continua con Amazon DocumentDB come destinazione](#)
- [Limitazioni all'utilizzo di Amazon DocumentDB come destinazione](#)
- [Utilizzo delle impostazioni degli endpoint con Amazon DocumentDB come destinazione](#)
- [Tipi di dati di destinazione per Amazon DocumentDB](#)

Note

Per una guida dettagliata del processo di migrazione, consulta [Migrazione da MongoDB ad Amazon DocumentDB](#) nella Guida dettagliata per la migrazione di AWS Database Migration Service.

Mappatura dei dati da un'origine a una destinazione Amazon DocumentDB

AWS DMS legge i record da un endpoint di origine e costruisce documenti JSON basati sui dati letti. Per ogni documento JSON, AWS DMS deve determinare un campo `_id` che agisca come un identificatore unico. Quindi scrive il documento JSON in una raccolta Amazon DocumentDB, utilizzando il campo `_id` come chiave primaria.

Dati di origine che sono una singola colonna

Se i dati di origine sono costituiti da una singola colonna, i dati devono essere di un tipo stringa. A seconda del motore di origine, il tipo di dati effettivo potrebbe essere VARCHAR, NVARCHAR, TEXT, LOB, CLOB o simile. AWS DMS presuppone che i dati siano un documento JSON valido e replica i dati in Amazon DocumentDB senza modificarli.

Se il documento JSON risultante contiene un campo denominato `_id`, tale campo viene utilizzato come `_id` univoco in Amazon DocumentDB.

Se il documento JSON non contiene un campo `_id`, Amazon DocumentDB genera automaticamente un valore `_id`.

Dati di origine che sono colonne multiple

Se i dati di origine sono costituiti da più colonne, allora AWS DMS crea un documento JSON da tutte queste colonne. Per determinare il campo `_id` per il documento, AWS DMS procede come segue:

- Se una delle colonne è denominata `_id`, allora i dati in tale colonna vengono utilizzati come `destinazione_id`.
- Se non esiste una colonna `_id`, ma i dati di origine dispongono di una chiave primaria o un indice univoco, allora AWS DMS utilizza tale chiave o valore di indice come valore `_id`. I dati della chiave primaria o dell'indice univoco vengono visualizzati come campi espliciti nel documento JSON.
- Se non esiste una colonna `_id` né una chiave primaria o indice univoco, Amazon DocumentDB genera automaticamente un valore `_id`.

Assegnazione forzata di un tipo di dati all'endpoint di destinazione

AWS DMS può modificare le strutture di dati quando scrive in un endpoint di destinazione Amazon DocumentDB. Puoi richiedere tali modifiche rinominando colonne e tabelle a livello di endpoint di origine, oppure fornendo le regole di trasformazione che vengono applicate durante l'esecuzione di un'attività.

Utilizzo di un documento JSON nidificato (prefisso json_)

Per forzare un tipo di dati, puoi anteporre al nome della colonna di origine `json_` (ovvero `json_columnName`) manualmente o utilizzando una trasformazione. In questo caso, la colonna viene creata come un documento JSON nidificato all'interno del documento di destinazione, anziché come un campo stringa.

Ad esempio, supponiamo di voler migrare il seguente documento da un endpoint di origine MongoDB.

```
{
  "_id": "1",
  "FirstName": "John",
  "LastName": "Doe",
  "ContactDetails": {"Home": {"Address": "Boston", "Phone": "1111111"}, "Work":
  { "Address": "Boston", "Phone": "2222222222"}}
}
```

Se non forzi uno qualsiasi dei tipi di dati di origine, il documento `ContactDetails` incorporato viene migrato come stringa.

```
{
  "_id": "1",
  "FirstName": "John",
  "LastName": "Doe",
  "ContactDetails": "{\"Home\": {\"Address\": \"Boston\", \"Phone\": \"1111111\"},
  \"Work\": { \"Address\": \"Boston\", \"Phone\": \"2222222222\"}}"
```

Tuttavia, puoi aggiungere una regola di trasformazione per forzare `ContactDetails` a un oggetto JSON. Ad esempio, supponiamo che il nome della colonna di origine originale sia `ContactDetails`. Per forzare il tipo di dati come JSON nidificato, la colonna sull'endpoint di origine deve essere rinominata `json_ContactDetails` aggiungendo il prefisso `*json_*` all'origine manualmente o tramite regole di trasformazione. Ad esempio, puoi utilizzare la seguente regola di trasformazione:

```
{
  "rules": [
    {
      "rule-type": "transformation",
      "rule-id": "1",
      "rule-name": "1",
      "rule-target": "column",
      "object-locator": {
        "schema-name": "%",
        "table-name": "%",
        "column-name": "ContactDetails"
      },
      "rule-action": "rename",
      "value": "json_ContactDetails",
      "old-value": null
    }
  ]
}
```

AWS DMS replica il campo ContactDetails come JSON nidificato, come segue.

```
{
  "_id": "1",
  "FirstName": "John",
  "LastName": "Doe",
  "ContactDetails": {
    "Home": {
      "Address": "Boston",
      "Phone": "1111111111"
    },
    "Work": {
      "Address": "Boston",
      "Phone": "2222222222"
    }
  }
}
```

Utilizzo di un array JSON (prefisso array_)

Per forzare un tipo di dati, puoi anteporre al nome della colonna `array_` (ovvero `array_columnName`) manualmente o utilizzando una trasformazione. In questo caso, AWS DMS considera la colonna come un array JSON e lo crea come tale nel documento di destinazione.

Supponiamo di voler migrare il seguente documento da un endpoint di origine MongoDB.

```
{
  "_id" : "1",
  "FirstName": "John",
  "LastName": "Doe",

  "ContactAddresses": ["Boston", "New York"],

  "ContactPhoneNumbers": ["1111111111", "2222222222"]
}
```

Se non forzi uno qualsiasi dei tipi di dati di origine, il documento `ContactDetails` incorporato viene migrato come stringa.

```
{
  "_id": "1",
  "FirstName": "John",
  "LastName": "Doe",

  "ContactAddresses": "[\"Boston\", \"New York\"]",

  "ContactPhoneNumbers": "[\"1111111111\", \"2222222222\"]"
}
```

Tuttavia, puoi aggiungere regole di trasformazione per forzare `ContactAddress` e `ContactPhoneNumbers` ad array JSON, come mostrato nella seguente tabella.

Nome colonna di origine originale	Colonna di origine rinominata
<code>ContactAddress</code>	<code>array_ContactAddress</code>
<code>ContactPhoneNumbers</code>	<code>array_ContactPhoneNumbers</code>

AWS DMS replica ContactAddress e ContactPhoneNumbers come segue.

```
{
  "_id": "1",
  "FirstName": "John",
  "LastName": "Doe",
  "ContactAddresses": [
    "Boston",
    "New York"
  ],
  "ContactPhoneNumbers": [
    "1111111111",
    "2222222222"
  ]
}
```

Connessione ad Amazon DocumentDB tramite TLS

Per impostazione predefinita, un nuovo cluster Amazon DocumentDB creato accetta solo connessioni protette con Transport Layer Security (TLS). Quando TLS è abilitato, ogni connessione ad Amazon DocumentDB richiede una chiave pubblica.

È possibile recuperare la chiave pubblica di Amazon DocumentDB scaricando il file `rds-combined-ca-bundle.pem` da un bucket Amazon S3 ospitato su AWS. Per ulteriori informazioni sul download di questo file, consulta [Crittografia delle connessioni con TLS](#) nella Guida per gli sviluppatori di Amazon DocumentDB

Dopo aver scaricato il file `.pem`, è possibile importare la chiave pubblica che contiene in AWS DMS come descritto di seguito.

AWS Management Console

Per importare il file della chiave pubblica (`.pem`)

1. Aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms>.
2. Nel riquadro di navigazione, scegliere Certificates (Certificati).
3. Scegliere Import certificate (Importa certificato) ed effettuare le seguenti operazioni:
 - Per Certificate identifier (Identificatore certificato), immettere un nome univoco per il certificato, ad esempio `docdb-cert`.

- Per Import file (Importa file), passare al percorso in cui è stato salvato il file .pem.

Dopo aver selezionato le impostazioni desiderate, selezionare Add new CA certificate (Aggiungi un nuovo certificato CA).

AWS CLI

Utilizza il comando `aws dms import-certificate` come visualizzato nell'esempio seguente.

```
aws dms import-certificate \  
  --certificate-identifier docdb-cert \  
  --certificate-pem file:///./rds-combined-ca-bundle.pem
```

Quando crei l'endpoint di destinazione AWS DMS, fornisci l'identificatore certificato (ad esempio, `docdb-cert`). Inoltre, imposta il parametro Modalità SSL su `verify-full`.

Connessione ai cluster elastici Amazon DocumentDB come destinazione

In AWS DMS 3.4.7 e versioni successive, puoi creare un endpoint di destinazione Amazon DocumentDB come cluster elastico. Se crei l'endpoint di destinazione come cluster elastico, è necessario allegare un nuovo certificato SSL all'endpoint del cluster elastico Amazon DocumentDB in quanto il certificato SSL esistente non funzionerà.

Per collegare un nuovo certificato SSL all'endpoint del cluster elastico Amazon DocumentDB

1. In un browser, apri <https://www.amazontrust.com/repository/SFSRootCAG2.pem> e salva il contenuto in un file .pem con un nome file univoco, ad esempio `SFSRootCAG2.pem`. Questo è il file di certificato che dovrai importare nelle fasi successive.
2. Crea l'endpoint del cluster elastico e imposta le seguenti opzioni:
 - a. In Configurazione dell'endpoint scegli Aggiungi un nuovo certificato CA.
 - b. Per Identificativo del certificato immetti **SFSRootCAG2.pem**.
 - c. Per Importa file del certificato seleziona Scegli file e passa al file `SFSRootCAG2.pem` scaricato in precedenza.
 - d. Seleziona e apri il file `SFSRootCAG2.pem` scaricato.
 - e. Selezionare Import certificate (Importa certificato).
 - f. Dal menu a discesa Scegli un certificato seleziona `SFSRootCAG2.pem`.

Il nuovo certificato SSL del file SFSRootCAG2 . pem scaricato è ora collegato all'endpoint del cluster elastico Amazon DocumentDB.

Replica continua con Amazon DocumentDB come destinazione

Se la replica continua (acquisizione dei dati di modifica o CDC) è abilitata per Amazon DocumentDB come destinazione, AWS DMS 3.5.0 e versioni successive forniscono un miglioramento delle prestazioni venti volte superiore rispetto alle versioni precedenti. Nelle versioni precedenti AWS DMS gestiva fino a 250 record al secondo, AWS DMS ora gestisce circa 5000 record al secondo. AWS DMS assicura inoltre che i documenti in Amazon DocumentDB rimangano sincronizzati con l'origine. Quando un record di origine viene creato o aggiornato, AWS DMS deve innanzitutto determinare quale record Amazon DocumentDB è interessato procedendo come segue:

- Se il record di origine dispone di una colonna denominata `_id`, il valore di tale colonna determina l'elemento `_id` corrispondente nella raccolta Amazon DocumentDB.
- Se non esiste una colonna `_id`, ma i dati di origine dispongono di una chiave primaria o un indice univoco, AWS DMS utilizza il valore della chiave o dell'indice come `_id` per la raccolta Amazon DocumentDB.
- Se il record di origine non dispone di una colonna `_id`, una chiave primaria o un indice univoco, AWS DMS associa tutte le colonne di origine ai campi corrispondenti nella raccolta Amazon DocumentDB.

Quando viene creato un nuovo record di origine, AWS DMS scrive un documento corrispondente in Amazon DocumentDB. Se un record di origine esistente viene aggiornato, AWS DMS aggiorna i campi corrispondenti nel documento di destinazione Amazon DocumentDB. Gli eventuali campi esistenti nel documento di destinazione ma non nel record di origine non vengono modificati.

Quando viene eliminato un nuovo record di origine, AWS DMS elimina il documento corrispondente da Amazon DocumentDB.

Modifiche strutturali (DDL) all'origine

Con la replica continua, le eventuali modifiche alle strutture di dati di origine (ad esempio tabelle, colonne e così via) vengono propagate alle relative controparti in Amazon DocumentDB. Nei database relazionali, tali modifiche vengono avviate utilizzando istruzioni DDL (Data Definition Language). Puoi vedere come AWS DMS propaga queste modifiche in Amazon DocumentDB nella tabella seguente.

DDL all'origine	Effetto sulla destinazione Amazon DocumentDB
CREATE TABLE	Crea una raccolta vuota.
Istruzione che rinomina una tabella (RENAME TABLE, ALTER TABLE . . . RENAME e simili)	Rinomina la raccolta.
TRUNCATE TABLE	Rimuove tutti i documenti dalla raccolta, ma solo se <code>HandleSourceTableTruncated</code> è <code>true</code> . Per ulteriori informazioni, consulta Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche .
DROP TABLE	Elimina la raccolta, ma solo se <code>HandleSourceTableDropped</code> è <code>true</code> . Per ulteriori informazioni, consulta Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche .
Istruzione che aggiunge una colonna a una tabella (ALTER TABLE . . . ADD e simili)	L'istruzione DDL viene ignorata e viene emesso un avviso. Quando viene eseguita la prima istruzione INSERT presso l'origine, il nuovo campo viene aggiunto al documento di destinazione.
ALTER TABLE . . . RENAME COLUMN	L'istruzione DDL viene ignorata e viene emesso un avviso. Quando viene eseguita la prima istruzione INSERT presso l'origine, il campo con il nuovo nome viene aggiunto al documento di destinazione.
ALTER TABLE . . . DROP COLUMN	L'istruzione DDL viene ignorata e viene emesso un avviso.
Istruzione che modifica il tipo di dati della colonna (ALTER COLUMN . . . MODIFY e simili)	L'istruzione DDL viene ignorata e viene emesso un avviso. Quando la prima istruzione INSERT viene eseguita presso l'origine con il nuovo

DDL all'origine	Effetto sulla destinazione Amazon DocumentDB
	tipo di dati, il documento di destinazione viene creato con un campo di tale nuovo tipo di dati.

Limitazioni all'utilizzo di Amazon DocumentDB come destinazione

Le seguenti limitazioni si applicano quando si utilizza Amazon DocumentDB come destinazione per AWS DMS:

- In Amazon DocumentDB i nomi di raccolte non possono contenere il simbolo di dollaro (\$). Inoltre, i nomi di database non possono contenere caratteri Unicode.
- AWS DMS non supporta l'unione di più tabelle di origine in una singola raccolta Amazon DocumentDB.
- Quando AWS DMS elabora le modifiche da una tabella di origine che non dispone di una chiave primaria, le eventuali colonne LOB in tale tabella vengono ignorate.
- Se l'opzione Change table (Modifica tabella) è abilitata e AWS DMS incontra una colonna di origine denominata "_id", allora tale colonna viene visualizzata come "__id" (due trattini bassi) nella tabella di modifica.
- Se scegli Oracle come un endpoint di origine, allora l'abilitazione del log supplementare deve essere abilitata nell'origine Oracle. In caso contrario, se presso l'origine sono presenti colonne che non sono state modificate, allora i dati vengono caricati in Amazon DocumentDB come valori nulli.
- L'impostazione dell'attività di replica `TargetTablePrepMode: TRUNCATE_BEFORE_LOAD` non è supportata per l'uso con un endpoint di destinazione DocumentDB.

Utilizzo delle impostazioni degli endpoint con Amazon DocumentDB come destinazione

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione Amazon DocumentDB in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--doc-db-settings '{"EndpointSetting": "value", ...}'`.

La tabella seguente mostra le impostazioni degli endpoint che puoi utilizzare con Amazon DocumentDB come destinazione.

Nome attributo	Valori validi	Valore predefinito e descrizione
<code>replicateShardCollections</code>	booleano <code>true</code> <code>false</code>	<p>Quando questa impostazione dell'endpoint è <code>true</code> ha gli effetti e le limitazioni indicati di seguito:</p> <ul style="list-style-type: none"> • AWS DMS è autorizzato a replicare i dati su raccolte di partizioni di destinazione. Questa impostazione è applicabile solo se l'endpoint DocumentDB di destinazione è un cluster elastico. • È necessario impostare <code>TargetTablePrepMode</code> su <code>DO_NOTHING</code> . • AWS DMS imposta automaticamente <code>useUpdateLookup</code> su <code>false</code> durante la migrazione.

Tipi di dati di destinazione per Amazon DocumentDB

Nella tabella seguente sono elencati i tipi di dati di destinazione Amazon DocumentDB supportati quando utilizzi AWS DMS e la mappatura predefinita dai tipi di dati AWS DMS. Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipi di dati AWS DMS	Tipi di dati Amazon DocumentDB
<code>BOOLEAN</code>	Boolean
<code>BYTES</code>	Dati binari
<code>DATE</code>	Data
<code>TIME</code>	Stringa (UTF8)
<code>DATETIME</code>	Data
<code>INT1</code>	Intero a 32 bit

Tipi di dati AWS DMS	Tipi di dati Amazon DocumentDB
INT2	Intero a 32 bit
INT4	Intero a 32 bit
INT8	Intero a 64 bit
NUMERIC	Stringa (UTF8)
REAL4	Doppio
REAL8	Doppio
STRING	Se i dati vengono riconosciuti come JSON, AWS DMS esegue la migrazione in Amazon DocumentDB come documento. In caso contrario, i dati vengono mappati alla Stringa (UTF8).
UINT1	Intero a 32 bit
UINT2	Intero a 32 bit
UINT4	Intero a 64 bit
UINT8	Stringa (UTF8)
WSTRING	Se i dati vengono riconosciuti come JSON, AWS DMS esegue la migrazione in Amazon DocumentDB come documento. In caso contrario, i dati vengono mappati alla Stringa (UTF8).
BLOB	Binario
CLOB	Se i dati vengono riconosciuti come JSON, AWS DMS esegue la migrazione in Amazon DocumentDB come documento. In caso contrario, i dati vengono mappati alla Stringa (UTF8).
NCLOB	Se i dati vengono riconosciuti come JSON, AWS DMS esegue la migrazione in Amazon DocumentDB come documento. In caso contrario, i dati vengono mappati alla Stringa (UTF8).

Utilizzo di Amazon Neptune come destinazione per AWS Database Migration Service

Amazon Neptune è un servizio di database a grafo gestito rapido e affidabile che rende più semplice la creazione e l'esecuzione di applicazioni che funzionano con set di dati altamente connessi. Il cuore di Neptune è un motore di database a grafo ad alte prestazioni appositamente progettato. Questo motore è ottimizzato per archiviare miliardi di relazioni ed eseguire query sul database a grafo con una latenza di millisecondi. Neptune supporta i più comuni linguaggi di query sul database a grafo Apache TinkerPop Gremlin e SPARQL di W3C. Per ulteriori informazioni su Amazon Neptune, consulta [What is Amazon Neptune?](#) nella Guida per l'utente di Amazon Neptune.

Senza un database a grafo come Neptune, è probabile che dati altamente connessi vengano modellati in un database relazionale. Poiché i dati dispongono di connessioni potenzialmente dinamiche, le applicazioni che utilizzano tali origini dati devono modellare query di dati connessi in SQL. Questo approccio richiede la scrittura di un livello aggiuntivo per convertire le query a grafo in SQL. Inoltre, i database relazionali sono dotati di uno schema rigido. Qualsiasi modifica nello schema per modellare il cambio di connessioni richiede tempi di inattività e una ulteriore manutenzione della conversione della query per supportare il nuovo schema. Le prestazioni delle query sono un altro grande limite da considerare durante la progettazione delle applicazioni.

I database a grafo possono semplificare notevolmente tali situazioni. Libero da uno schema, un livello avanzato di query a grafo (Gremlin o SPARQL) e indici ottimizzati per le query a grafo aumentano la flessibilità e le prestazioni. Il database a grafo Amazon Neptune dispone anche di funzionalità aziendali come la crittografia a riposo, un livello di autorizzazione sicuro, backup predefiniti, supporto Multi-AZ, supporto delle repliche di lettura e altre ancora.

Con AWS DMS, è possibile eseguire la migrazione di dati relazionali, che modellano un grafo altamente connesso, a un endpoint di destinazione di Neptune da un endpoint di origine di DMS per qualsiasi database SQL supportato.

Per ulteriori dettagli, consulta quanto segue:

Argomenti

- [Panoramica sulla migrazione a Amazon Neptune come destinazione](#)
- [Specifiche delle impostazioni degli endpoint per Amazon Neptune come destinazione](#)
- [Creazione di un ruolo di servizio IAM per l'accesso ad Amazon Neptune come destinazione](#)
- [Specifiche delle regole di mappatura del grafo utilizzando Gremlin e R2RML per Amazon Neptune come destinazione](#)

- [Tipi di dati per la migrazione di Gremlin e R2RML ad Amazon Neptune come destinazione](#)
- [Limitazioni all'utilizzo di Amazon Neptune come destinazione](#)

Panoramica sulla migrazione a Amazon Neptune come destinazione

Prima di avviare la migrazione a una destinazione Neptune, crea le seguenti risorse nell'account AWS:

- Un cluster Neptune per l'endpoint di destinazione.
- Un database relazionale SQL supportato da AWS DMS per l'endpoint di origine.
- Un bucket Amazon S3 per l'endpoint di destinazione. Crea questo bucket S3 nella stessa regione AWS del cluster Neptune. AWS DMS utilizza questo bucket S3 per lo storage dei file intermedio con i dati di destinazione caricati in blocco nel database Neptune. Per ulteriori informazioni sulla creazione di un bucket S3, consulta [Creazione di un bucket](#) nella Guida per l'utente di Amazon Simple Storage Service.
- Un endpoint del cloud privato virtuale (VPC) per S3 nello stesso VPC del cluster Neptune.
- Un ruolo AWS Identity and Access Management (IAM) che includa una policy IAM. Questa policy deve specificare al bucket S3 le autorizzazioni `GetObject`, `PutObject`, `DeleteObject` e `ListObject` per l'endpoint di destinazione. Questo ruolo viene assunto da AWS DMS e Neptune, con accesso IAM sia al bucket S3 di destinazione che al database Neptune. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM per l'accesso ad Amazon Neptune come destinazione](#).

Una volta in possesso di queste risorse, la configurazione e l'avvio di una migrazione a una destinazione Neptune è simile a qualsiasi migrazione di pieno carico tramite la console o l'API DMS. Tuttavia, una migrazione a una destinazione Neptune richiede alcuni passaggi specifici.

Per eseguire la migrazione di un database relazionale AWS DMS a Neptune

1. Creare un'istanza di replica nel modo descritto in [Creazione di un'istanza di replica](#).
2. Creare e testare un database relazionale SQL supportato da AWS DMS per l'endpoint di origine.
3. Crea e testa l'endpoint di destinazione per il database Neptune.

Per connettere l'endpoint di destinazione al database Neptune, specifica il nome del server per l'endpoint del cluster Neptune o per l'endpoint dell'istanza di scrittura Neptune. Inoltre, specifica

la cartella del bucket S3 in modo che AWS DMS vi archivi i file intermedi per il caricamento in blocco nel database Neptune.

Durante la migrazione, AWS DMS archivia tutti i dati di destinazione migrati in questa cartella del bucket S3 fino a una dimensione massima del file specificata. Quando questo storage di file raggiunge la dimensione massima, AWS DMS carica in blocco i dati S3 archiviati nel database di destinazione. Cancella la cartella per consentire lo storage di eventuali altri dati di destinazione per un successivo caricamento nel database di destinazione. Per ulteriori informazioni su come specificare queste impostazioni, consulta [Specifica delle impostazioni degli endpoint per Amazon Neptune come destinazione](#).

4. Crea un'attività di replica di pieno carico con le risorse create nelle fasi da 1 a 3 ed effettua le seguenti operazioni:
 - a. Utilizzare come sempre la mappatura delle tabelle dell'attività per identificare schemi, tabelle e viste di origine specifici di cui eseguire la migrazione dal database relazionale utilizzando le regole di selezione e trasformazione appropriate. Per ulteriori informazioni, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#).
 - b. Specifica le mappature di destinazione scegliendo una delle seguenti opzioni per indicare le regole di mappatura dalle tabelle e dalle viste di origine al database a grafo di destinazione Neptune:
 - Gremlin JSON: per informazioni sull'utilizzo di Gremlin JSON per caricare un database Neptune, consulta [Gremlin load data format](#) nella Guida per l'utente di Amazon Neptune.
 - SPARQL RDB to Resource Description Framework Mapping Language (R2RML): per informazioni sull'utilizzo di SPARQL R2RML, consulta la specifica W3C [R2RML: RDB to RDF mapping language](#).
 - c. Completa una delle seguenti operazioni:
 - Tramite la console AWS DMS, specificare le opzioni di mappatura a grafo utilizzando Regole di mappatura a grafo nella pagina Crea attività di migrazione del database .
 - Tramite l'API AWS DMS, specificare queste opzioni utilizzando il parametro di richiesta TaskData della chiamata API CreateReplicationTask.

Per ulteriori informazioni ed esempi sull'utilizzo di Gremlin JSON e SPARQL R2RML per specificare le regole di mappatura a grafo, consulta [Specifica delle regole di mappatura del grafo utilizzando Gremlin e R2RML per Amazon Neptune come destinazione](#).

5. Avviare la replica per l'attività di migrazione.

Specifica delle impostazioni degli endpoint per Amazon Neptune come destinazione

Per creare o modificare un endpoint di destinazione, è possibile utilizzare la console o le operazioni API `CreateEndpoint` o `ModifyEndpoint`.

Per una destinazione Neptune nella console AWS DMS immetti le Impostazioni specifiche dell'endpoint nella pagina della console `Crea endpoint` o `Modifica endpoint`. Per `CreateEndpoint` e `ModifyEndpoint`, specificare i parametri di richiesta per l'opzione `NeptuneSettings`. Nell'esempio seguente viene illustrato come eseguire questa operazione utilizzando la CLI.

```
dms create-endpoint --endpoint-identifier my-neptune-target-endpoint
--endpoint-type target --engine-name neptune
--server-name my-neptune-db.cluster-cspckvklbvgf.us-east-1.neptune.amazonaws.com
--port 8192
--neptune-settings
  '{"ServiceAccessRoleArn":"arn:aws:iam::123456789012:role/myNeptuneRole",
  "S3BucketName":"my-bucket",
  "S3BucketFolder":"my-bucket-folder",
  "ErrorRetryDuration":57,
  "MaxFileSize":100,
  "MaxRetryCount": 10,
  "IAMAuthEnabled":false}'
```

Qui, l'opzione `--server-name` della CLI indica il nome del server per l'endpoint di scrittura del cluster Neptune. In alternativa, è possibile specificare il nome del server per un endpoint dell'istanza di scrittura Neptune.

Seguono i parametri di richiesta dell'opzione `--neptune-settings`:

- `ServiceAccessRoleArn` (obbligatorio): il nome della risorsa Amazon (ARN) del ruolo di servizio creato per l'endpoint di destinazione Neptune. Per ulteriori informazioni, consulta [Creazione di un ruolo di servizio IAM per l'accesso ad Amazon Neptune come destinazione](#).
- `S3BucketName` (obbligatorio): il nome del bucket Amazon S3 in cui DMS può archiviare temporaneamente i dati a grafo migrati in file.csv prima di caricarli in blocco nel database di destinazione Neptune. DMS mappa i dati di origine SQL ai dati a grafo prima di archivarli in questi file .csv.

- `S3BucketFolder` (obbligatorio): il percorso di una cartella in cui si desidera che DMS archivi i dati a grafo migrati nel bucket S3 specificato da `S3BucketName`.
- `ErrorRetryDuration` (facoltativo): il numero di millisecondi che DMS deve attendere per riprovare a caricare in blocco dati a grafo migrati nel database di destinazione Neptune prima di generare un errore. Il valore di default è 250.
- `MaxFileSize` (facoltativo): la dimensione massima in KB di dati a grafo migrati archiviati in un file con estensione `.csv` prima che DMS carichi in blocco i dati nel database di destinazione Neptune. Il valore predefinito è 1.048.576 KB (1 GB). In caso di esito positivo del caricamento, DMS cancella il bucket, pronto per memorizzare il successivo batch di dati a grafo migrati.
- `MaxRetryCount` (facoltativo): il numero di tentativi eseguiti da DMS per caricare in blocco i dati a grafo migrati nel database di destinazione Neptune prima di generare un errore. Il predefinito è 5.
- `IAMAuthEnabled` (facoltativo): per abilitare l'autorizzazione IAM per l'endpoint, imposta questo parametro su `true` e collega il documento della policy IAM appropriato al ruolo di servizio specificato da `ServiceAccessRoleArn`. Il valore predefinito è `false`.

Creazione di un ruolo di servizio IAM per l'accesso ad Amazon Neptune come destinazione

Per accedere a Neptune come destinazione, creare un ruolo del servizio utilizzando IAM. A seconda della configurazione dell'endpoint Neptune, collega a questo ruolo alcuni o tutti i documenti di trust e della policy IAM descritti di seguito. Quando si crea l'endpoint Neptune, occorre fornire l'ARN del ruolo di servizio. In questo modo si permette ad AWS DMS e Amazon Neptune di assumere le autorizzazioni per accedere a Neptune e al relativo bucket Amazon S3 associato.

Se imposti il parametro `IAMAuthEnabled` in `NeptuneSettings` su `true` nella configurazione dell'endpoint Neptune, collega al ruolo di servizio una policy IAM come la seguente. Se si imposta `IAMAuthEnabled` su `false`, è possibile ignorare questa policy.

```
// Policy to access Neptune

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "neptune-db:*",
```



```

        "Resource": "arn:aws:neptune-db:us-east-1:123456789012:cluster-
        CLG7H7FHK54AZGHEH6MNS55JKM/*"
    }
]
}

```

La policy IAM precedente consente l'accesso completo al cluster di destinazione Neptune specificato da Resource.

Collegare una policy IAM come la seguente al ruolo del servizio. Questa policy consente a DMS di archiviare temporaneamente i dati a grafo migrati nel bucket S3 creato per il caricamento in blocco nel database di destinazione Neptune.

```

//Policy to access S3 bucket

{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "ListObjectsInBucket0",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3::my-bucket"
    ]
  },
  {
    "Sid": "AllObjectActions",
    "Effect": "Allow",
    "Action": ["s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject"
    ],
    "Resource": [
      "arn:aws:s3::my-bucket/"
    ]
  },
  {
    "Sid": "ListObjectsInBucket1",
    "Effect": "Allow",
    "Action": "s3:ListBucket",
    "Resource": [
      "arn:aws:s3::my-bucket",

```

```
"arn:aws:s3:::my-bucket/"
]
}
]
}
```

La policy IAM precedente consente all'account di eseguire query sui contenuti del bucket S3 (arn:aws:s3:::my-bucket) creato per la destinazione Neptune. Permette inoltre all'account di operare in modo completo sui contenuti di tutti i file e le cartelle del bucket (arn:aws:s3:::my-bucket/).

Modifica la relazione di trust e collega il ruolo IAM seguente al ruolo di servizio per consentire ad AWS DMS e al servizio di database Amazon Neptune di assumere il ruolo.

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

Per informazioni su come specificare questo ruolo di servizio per l'endpoint di destinazione Neptune, consulta [Specifiche delle impostazioni degli endpoint per Amazon Neptune come destinazione](#).

Specifica delle regole di mappatura del grafo utilizzando Gremlin e R2RML per Amazon Neptune come destinazione

Le regole di mappatura del grafo create specificano il modo in cui i dati estratti da un'origine di database relazionale SQL vengono caricati in una destinazione del cluster di database Neptune. Il formato di queste regole di mappatura varia a seconda se le regole valgono per il caricamento dei dati del grafo delle proprietà tramite Apache TinkerPop Gremlin o per il caricamento dei dati RDF (Resource Description Framework) tramite R2RML. Di seguito è possibile trovare informazioni su questi formati e su dove approfondirle.

È possibile specificare queste regole di mappatura quando si crea l'attività di migrazione utilizzando la console o l'API DMS.

Tramite la console, specificare queste regole di mappatura utilizzando le Regole di mappatura a grafo nella pagina Crea attività di migrazione del database . In Regole di mappatura a grafo è possibile immettere e modificare le regole di mappatura direttamente utilizzando l'editor fornito. In alternativa, è possibile cercare un file che contenga le regole di mappatura nel formato di mappatura a grafo appropriato.

Tramite l'API, specificare queste opzioni utilizzando il parametro di richiesta `TaskData` della chiamata API `CreateReplicationTask`. Impostare `TaskData` sul percorso di un file contenente le regole di mappatura nel formato di mappatura a grafo appropriato.

Regole di mappatura a grafo per la generazione di dati del grafo di proprietà mediante Gremlin

Utilizzando Gremlin per generare i dati del grafo di proprietà, specificare un oggetto JSON con una regola di mappatura per ogni entità a grafo da generare dai dati di origine. Il formato di questo JSON è definito specificamente per il caricamento in blocco su Amazon Neptune. Il modello seguente mostra l'aspetto di ogni regola in questo oggetto.

```
{
  "rules": [
    {
      "rule_id": "(an identifier for this rule)",
      "rule_name": "(a name for this rule)",
      "table_name": "(the name of the table or view being loaded)",
      "vertex_definitions": [
        {
          "vertex_id_template": "{col1}",
          "vertex_label": "(the vertex to create)",

```

```

        "vertex_definition_id": "(an identifier for this vertex)",
        "vertex_properties": [
            {
                "property_name": "(name of the property)",
                "property_value_template": "{col2} or text",
                "property_value_type": "(data type of the property)"
            }
        ]
    }
],
{
    "rule_id": "(an identifier for this rule)",
    "rule_name": "(a name for this rule)",
    "table_name": "(the name of the table or view being loaded)",
    "edge_definitions": [
        {
            "from_vertex": {
                "vertex_id_template": "{col1}",
                "vertex_definition_id": "(an identifier for the vertex
referenced above)"
            },
            "to_vertex": {
                "vertex_id_template": "{col3}",
                "vertex_definition_id": "(an identifier for the vertex
referenced above)"
            },
            "edge_id_template": {
                "label": "(the edge label to add)",
                "template": "{col1}_{col3}"
            },
            "edge_properties": [
                {
                    "property_name": "(the property to add)",
                    "property_value_template": "{col4} or text",
                    "property_value_type": "(data type like String, int,
double)"
                }
            ]
        }
    ]
}
]
}
}

```

La presenza di un'etichetta del vertice implica che il vertice viene creato qui. La sua assenza implica che il vertice viene creato da un'origine diversa e che questa definizione aggiunge solo le proprietà del vertice. Specificare tutte le definizioni di vertici e di edge necessarie per specificare le mappature per l'intera origine del database relazionale.

Segue una regola di esempio per una tabella employee.

```
{
  "rules": [
    {
      "rule_id": "1",
      "rule_name": "vertex_mapping_rule_from_nodes",
      "table_name": "nodes",
      "vertex_definitions": [
        {
          "vertex_id_template": "{emp_id}",
          "vertex_label": "employee",
          "vertex_definition_id": "1",
          "vertex_properties": [
            {
              "property_name": "name",
              "property_value_template": "{emp_name}",
              "property_value_type": "String"
            }
          ]
        }
      ]
    },
    {
      "rule_id": "2",
      "rule_name": "edge_mapping_rule_from_emp",
      "table_name": "nodes",
      "edge_definitions": [
        {
          "from_vertex": {
            "vertex_id_template": "{emp_id}",
            "vertex_definition_id": "1"
          },
          "to_vertex": {
            "vertex_id_template": "{mgr_id}",

```



```

<#TriplesMap1>
  rr:logicalTable [ rr:tableName "nodes" ];
  rr:subjectMap [
    rr:template "http://data.example.com/employee/{id}";
    rr:class ex:Employee;
  ];
  rr:predicateObjectMap [
    rr:predicate ex:name;
    rr:objectMap [ rr:column "label" ];
  ]

```

Nell'esempio precedente, la mappatura definisce i nodi del grafo mappati da una tabella di dipendenti.

Segue un altro semplice esempio per una tabella Student.

```

@prefix rr: <http://www.w3.org/ns/r2rml#>.
@prefix ex: <http://example.com/#>.
@prefix foaf: <http://xmlns.com/foaf/0.1/>.
@prefix xsd: <http://www.w3.org/2001/XMLSchema#>.

<#TriplesMap2>
  rr:logicalTable [ rr:tableName "Student" ];
  rr:subjectMap [ rr:template "http://example.com/{ID}{Name}";
                 rr:class foaf:Person ];
  rr:predicateObjectMap [
    rr:predicate ex:id ;
    rr:objectMap [ rr:column "ID";
                  rr:datatype xsd:integer ]
  ];
  rr:predicateObjectMap [
    rr:predicate foaf:name ;
    rr:objectMap [ rr:column "Name" ]
  ].

```

Nell'esempio precedente, la mappatura definisce i nodi del grafo che mappano le relazioni tra amici e amici nelle persone in una tabella Student.

Per ulteriori informazioni sulla creazione di regole di mappatura a grafo utilizzando SPARQL R2RML, consulta la specifica W3C [R2RML: RDB to RDF Mapping Language](#).

Tipi di dati per la migrazione di Gremlin e R2RML ad Amazon Neptune come destinazione

AWS DMS esegue la mappatura dei tipi di dati dall'endpoint di origine SQL alla destinazione Neptune in due modi. Il modo che scegli dipende dal formato di mappatura del grafo utilizzato per caricare il database Neptune:

- Apache TinkerPop Gremlin, tramite una rappresentazione JSON dei dati di migrazione.
- SPARQL di W3C, tramite una rappresentazione R2RML dei dati di migrazione.

Per ulteriori informazioni su questi due formati di mappatura del grafo, consulta [Specifiche delle regole di mappatura del grafo utilizzando Gremlin e R2RML per Amazon Neptune come destinazione](#).

Di seguito è possibile trovare le descrizioni delle mappature dei tipi di dati per ogni formato.

Mappatura dei tipi di dati da un'origine SQL a una destinazione Gremlin

Nella tabella seguente vengono illustrate le mappature dei tipi di dati da un'origine SQL a una destinazione in formato Gremlin.

AWS DMS mappa qualsiasi tipo di dati di origine SQL non elencato a una `String` Gremlin.

Tipi di dati di origine SQL	Tipi di dati di destinazione Gremlin
NUMERIC (e varianti)	Double
DECIMAL	
TINYINT	Byte
SMALLINT	Short
INT, INTEGER	Int
BIGINT	Long
FLOAT	Float
DOUBLE PRECISION	

Tipi di dati di origine SQL	Tipi di dati di destinazione Gremlin
REAL	Double
BIT	Boolean
BOOLEAN	
DATE	Date
TIME	
TIMESTAMP	
CHARACTER (e varianti)	String

Per ulteriori informazioni sui tipi di dati Gremlin per il caricamento di Neptune, consulta [Gremlin data types](#) nella Guida per l'utente di Amazon Neptune.

Mappatura dei tipi di dati da un'origine SQL a una destinazione R2RML (RDF)

Nella tabella seguente vengono illustrate le mappature dei tipi di dati da un'origine SQL a una destinazione in formato R2RML.

Tutti i tipi di dati RDF elencati fanno distinzione tra maiuscole e minuscole, ad eccezione dei letterali RDF. AWS DMS mappa qualsiasi tipo di dati di origine SQL non elencato a un letterale RDF.

Un letterale RDF è un valore di una serie di forme lessicali letterali e di tipi di dati. Per ulteriori informazioni, consulta [RDF Literals](#) nella specifica W3C Resource Description Framework (RDF): Concepts and Abstract Syntax.

Tipi di dati di origine SQL	Tipi di dati di destinazione R2RML (RDF)
BINARY (e varianti)	xsd:hexBinary
NUMERIC (e varianti)	xsd:decimal
DECIMAL	
TINYINT	xsd:integer

Tipi di dati di origine SQL	Tipi di dati di destinazione R2RML (RDF)
SMALLINT	
INT, INTEGER	
BIGINT	
FLOAT	xsd:double
DOUBLE PRECISION	
REAL	
BIT	xsd:boolean
BOOLEAN	
DATE	xsd:date
TIME	xsd:time
TIMESTAMP	xsd:dateTime
CHARACTER (e varianti)	RDF letterale

Per ulteriori informazioni sui tipi di dati RDF per il caricamento su Neptune e le relative mappature ai tipi di dati di origine SQL, consulta [Datatype conversions](#) nella specifica W3C R2RML: RDB to RDF Mapping Language.

Limitazioni all'utilizzo di Amazon Neptune come destinazione

Le seguenti limitazioni si applicano quando si utilizza Neptune come destinazione:

- AWS DMS attualmente supporta le attività di pieno carico solo per la migrazione a una destinazione Neptune. La migrazione di acquisizione dei dati di modifica (CDC) a una destinazione Neptune non è supportata.
- Assicurati di eliminare manualmente tutti i dati nel database Neptune di destinazione prima di avviare l'attività di migrazione, come negli esempi seguenti.

Per eliminare tutti i dati (vertici ed edge) all'interno del grafo, esegui il comando Gremlin seguente.

```
gremlin> g.V().drop().iterate()
```

Per eliminare i vertici con etichetta 'customer', esegui il comando Gremlin seguente.

```
gremlin> g.V().hasLabel('customer').drop()
```

Note

L'eliminazione di un set di dati di grandi dimensioni può richiedere del tempo. È consigliabile ripetere `drop()` con un limite, ad esempio `limit(1000)`.

Per eliminare gli edge con etichetta 'rated', esegui il comando Gremlin seguente.

```
gremlin> g.E().hasLabel('rated').drop()
```

Note

L'eliminazione di un set di dati di grandi dimensioni può richiedere del tempo. È consigliabile ripetere `drop()` con un limite, ad esempio `limit(1000)`.

- L'operazione API DMS `DescribeTableStatistics` può restituire risultati imprecisi su una determinata tabella a causa della natura della struttura dei dati a grafo di Neptune.

Durante la migrazione, AWS DMS esegue la scansione di ogni tabella di origine e utilizza la mappatura a grafo per convertire i dati di origine in un grafo Neptune. I dati convertiti vengono innanzitutto archiviati nella cartella del bucket S3 specificata per l'endpoint di destinazione. Se l'origine viene sottoposta a scansione e questi dati intermedi S3 vengono generati correttamente, `DescribeTableStatistics` presuppone che i dati siano stati caricati correttamente nel database di destinazione Neptune. Ma ciò non è sempre vero. Per verificare che i dati siano stati caricati correttamente per una determinata tabella, confrontare i valori `count()` restituiti a entrambe le estremità della migrazione per tale tabella.

Nell'esempio seguente, AWS DMS ha caricato una tabella `customer` dal database di origine, a cui viene assegnata l'etichetta 'customer' nel database a grafo Neptune di destinazione. È possibile

verificare che questa etichetta sia scritta nel database di destinazione. A tale scopo, confronta il numero di righe `customer` disponibili nel database di origine con il numero di righe con etichetta 'customer' caricate nel database di destinazione Neptune al termine dell'attività.

Per ottenere il numero di righe cliente disponibili dal database di origine tramite SQL, eseguire le operazioni seguenti.

```
select count(*) from customer;
```

Per ottenere il numero di righe con etichetta 'customer' caricate nel grafo del database di destinazione tramite Gremlin, eseguire le operazioni seguenti.

```
gremlin> g.V().hasLabel('customer').count()
```

- Attualmente, se il caricamento di una singola tabella non riesce, l'intera attività ha esito negativo. A differenza di una destinazione di database relazionale, i dati in Neptune sono altamente connessi, il che rende impossibile in molti casi il ripristino di un'attività. Se non è possibile ripristinare un'attività a causa di questo tipo di errore nel caricamento dei dati, creare una nuova attività per caricare la tabella che non è stato possibile caricare. Prima di eseguire questa nuova attività, elimina manualmente dalla destinazione Neptune la tabella parzialmente caricata.

Note

È possibile ripristinare un'attività che non riesce a eseguire la migrazione a una destinazione Neptune se l'errore è recuperabile (ad esempio un errore di transito di rete).

- AWS DMS supporta la maggior parte degli standard per R2RML. Tuttavia, AWS DMS non supporta alcuni standard R2RML, incluse espressioni inverse, join e viste. Una soluzione alternativa per una vista R2RML consiste nel creare una vista SQL personalizzata corrispondente nel database di origine. Nell'attività di migrazione, utilizzare la mappatura delle tabelle per scegliere la vista come input. Quindi, mappare la vista a una tabella che viene quindi utilizzata da R2RML per generare dati a grafo.
- Quando si esegue la migrazione dei dati di origine con tipi di dati SQL non supportati, i dati di destinazione risultanti possono difettare di precisione. Per ulteriori informazioni, consulta [Tipi di dati per la migrazione di Gremlin e R2RML ad Amazon Neptune come destinazione](#).
- AWS DMS non supporta la migrazione dei dati LOB in una destinazione Neptune.

Utilizzo di Redis come destinazione per AWS Database Migration Service

Redis è uno store di strutture di dati in memoria open source utilizzato come database, cache e broker di messaggi. La gestione dei dati in memoria può eseguire operazioni di lettura o scrittura che richiedono meno di un millisecondo e centinaia di milioni di operazioni ogni secondo. Essendo un datastore in memoria, Redis supporta le applicazioni più esigenti che richiedono tempi di risposta inferiori al millisecondo.

Utilizzando AWS DMS, puoi migrare i dati da qualsiasi database di origine supportato a un data store Redis di destinazione con tempi di inattività minimi. Per ulteriori informazioni su Redis, consulta la [documentazione di Redis](#).

Oltre a Redis on-premise, AWS Database Migration Service supporta:

- [Amazon ElastiCache per Redis](#) come datastore di destinazione. ElastiCache per Redis funziona con i client Redis e utilizza il formato di dati Redis aperto per archiviare i dati.
- [Amazon MemoryDB per Redis](#) come datastore di destinazione. MemoryDB è compatibile con Redis e consente di creare applicazioni utilizzando tutte le strutture di dati, le API e i comandi Redis attualmente disponibili.

Per ulteriori dettagli sull'utilizzo di Redis come destinazione per AWS DMS, consulta le seguenti sezioni:

Argomenti

- [Prerequisiti per l'utilizzo di un cluster Redis come destinazione per AWS DMS](#)
- [Limitazioni all'utilizzo di Redis come destinazione per AWS Database Migration Service](#)
- [Migrazione dei dati da un database relazionale o non relazionale a una destinazione Redis](#)
- [Specifiche delle impostazioni degli endpoint per Redis come destinazione](#)

Prerequisiti per l'utilizzo di un cluster Redis come destinazione per AWS DMS

DMS supporta una destinazione Redis on-premise in una configurazione autonoma o come cluster Redis in cui i dati vengono automaticamente partizionati su più nodi. Il partizionamento è il processo di separazione dei dati in blocchi più piccoli, denominati partizioni, distribuiti su più server o nodi. In effetti, si tratta di una partizione di dati che contiene un sottoinsieme del set di dati totale e serve una parte del carico di lavoro complessivo.

Poiché Redis è un datastore NoSQL di coppie chiave-valore, la convenzione di denominazione delle chiavi Redis da utilizzare quando l'origine è un database relazionale è `schema-name.table-name.primary-key`. In Redis, la chiave e il valore non devono contenere il carattere speciale `%`. In caso contrario, DMS ignora il record.

Note

Se utilizzi ElastiCache per Redis come destinazione, DMS supporta solo le configurazioni abilitate per la modalità cluster. Per ulteriori informazioni sull'utilizzo di ElastiCache per Redis 6.x o versioni successive per creare un datastore di destinazione abilitato per la modalità cluster, consulta [Nozioni di base](#) nella Guida per l'utente di Amazon ElastiCache per Redis.

Prima di iniziare una migrazione del database, avvia il cluster Redis con i seguenti criteri.

- Il cluster ha una o più partizioni.
- Se utilizzi una destinazione ElastiCache per Redis, assicurati che il cluster non usi il controllo degli accessi in base al ruolo IAM. Puoi usare Redis Auth per autenticare gli utenti.
- Abilita Multi-AZ (zone di disponibilità).
- Assicurati che il cluster abbia memoria disponibile sufficiente per contenere i dati da migrare dal database.
- Assicurati che il cluster Redis di destinazione sia privo di tutti i dati prima di avviare l'attività di migrazione iniziale.

È necessario determinare i requisiti di sicurezza per la migrazione dei dati prima di creare la configurazione del cluster. DMS supporta la migrazione in gruppi di replica di destinazione indipendentemente dalla configurazione della crittografia. Tuttavia, è possibile abilitare o disabilitare la crittografia solo quando si crea la configurazione del cluster.

Limitazioni all'utilizzo di Redis come destinazione per AWS Database Migration Service

Le seguenti limitazioni si applicano quando si utilizza Redis come destinazione:

- Poiché Redis è un datastore no-sql di coppie chiave-valore, la convenzione di denominazione delle chiavi Redis da utilizzare quando l'origine è un database relazionale è `schema-name.table-name.primary-key`.

- In Redis, la coppia chiave-valore non può contenere il carattere speciale %. In caso contrario, DMS ignora il record.
- DMS non migra le righe che contengono caratteri speciali.
- DMS non migra i campi che contengono caratteri speciali nel nome del campo.
- La modalità LOB completa non è supportata.
- L'autorità di certificazione (CA) privata non è supportata quando si utilizza ElastiCache per Redis come destinazione.

Migrazione dei dati da un database relazionale o non relazionale a una destinazione Redis

Puoi migrare i dati da qualsiasi datastore SQL o NoSQL di origine direttamente su una destinazione Redis. La configurazione e l'avvio di una migrazione su una destinazione Redis è simile a qualsiasi migrazione di pieno carico e acquisizione dei dati di modifica utilizzando la console o l'API DMS. Per eseguire una migrazione del database su una destinazione Redis, procedi come segue.

- Crea un'istanza di replica che esegua tutti i processi per la migrazione. Per ulteriori informazioni, consulta [Creazione di un'istanza di replica](#).
- Specifica un endpoint di origine. Per ulteriori informazioni, consulta [Creazione di endpoint di origine e destinazione](#).
- Individua il nome DNS e il numero della porta del cluster.
- Scarica un bundle di certificati che puoi usare per verificare le connessioni SSL.
- Specifica un endpoint di destinazione, come descritto di seguito.
- Crea un'attività o una serie di attività per definire le tabelle e i processi di replica da utilizzare. Per ulteriori informazioni, consulta [Creazione di un'attività](#).
- Esegui la migrazione dei dati dal database di origine al cluster di destinazione.

È possibile avviare una migrazione del database in due modi:

1. Puoi scegliere la console AWS DMS ed eseguire ogni passaggio.
2. Puoi utilizzare la AWS Command Line Interface (AWS CLI). Per ulteriori informazioni sull'uso della CLI con AWS DMS, consulta [AWS CLI per AWS DMS](#).

Per individuare il nome DNS e il numero della porta del cluster

- Utilizza il comando AWS CLI seguente per fornire a `replication-group-id` il nome del gruppo di replica.

```
aws elasticache describe-replication-groups --replication-group-id myreplgroup
```

Qui, l'output mostra il nome DNS nell'attributo `Address` e il numero di porta nell'attributo `Port` del nodo primario del cluster.

```
...
"ReadEndpoint": {
  "Port": 6379,
  "Address": "myreplgroup-
111.1abc1d.1111.uuu1.cache.example.com"
}
...
```

Se utilizzi MemoryDB per Redis come destinazione, usa il comando AWS CLI seguente per fornire un indirizzo di endpoint al cluster Redis.

```
aws memorydb describe-clusters --clusterid clusterid
```

Download di un bundle di certificati da usare per verificare le connessioni SSL

- Nella riga di comando, immetti il comando `wget` seguente. `Wget` è uno strumento di utilità a riga di comando GNU gratuito utilizzato per scaricare i file da Internet.

```
wget https://s3.aws-api-domain/rds-downloads/rds-combined-ca-bundle.pem
```

`aws-api-domain` completa il dominio Amazon S3 nella regione AWS necessaria per accedere al bucket S3 specificato e al file `rds-combined-ca-bundle.pem` che fornisce.

Per creare un endpoint di destinazione tramite la console AWS DMS

Questo endpoint è per la destinazione Redis già in esecuzione.

- Nel riquadro di navigazione della console IAM, scegli Endpoint quindi seleziona Crea endpoint. Nella tabella seguente vengono illustrate le impostazioni.

Per questa opzione	Eeguire questa operazione
Endpoint type (Tipo di endpoint)	Scegli il tipo di endpoint Destinazione.
Endpoint identifier (Identificatore endpoint)	Inserisci il nome dell'endpoint. Includi il tipo di endpoint nel nome, ad esempio my-redis-target .
Motore di destinazione	Scegli Redis come tipo di motore di database a cui desideri connettere questo endpoint.
Nome cluster	Inserisci il nome DNS del cluster Redis.
Porta	Inserisci il numero di porta del cluster Redis.
Protocollo di sicurezza SSL	<p>Scegli Testo normale o Crittografia SSL.</p> <p>Testo normale: questa opzione non fornisce la crittografia Transport Layer Security (TLS) per il traffico tra l'endpoint e il database.</p> <p>Crittografia SSL: se scegli questa opzione, inserisci l'ARN del certificato dell'Autorità di certificazione (CA) SSL per verificare il certificato del server e stabilire una connessione crittografata.</p> <p>Per Redis on-premise, DMS supporta l'Autorità di certificazione (CA) pubblica e privata. Per ElastiCache per Redis, DMS supporta solo la CA pubblica.</p>
Tipo di autenticazione	Scegli il tipo di autenticazione da eseguire durante la connessione a Redis. Le opzioni sono Nessuno, Ruolo di autenticazione e Token di autenticazione.

Per questa opzione	Eseguire questa operazione
	<p>Se scegli il ruolo di autenticazione, fornisci un nome utente di autenticazione e una password di autenticazione.</p> <p>Se scegli il token di autenticazione, fornisci solo la password di autenticazione.</p>
Replication instance (Istanza di replica)	[Facoltativo] Solo se intendi testare la connessione, scegli il nome dell'istanza di replica che hai inserito in precedenza nella pagina Crea istanza di replica.

Una volta specificate tutte le informazioni per l'endpoint, AWS DMS crea l'endpoint di destinazione Redis da utilizzare durante la migrazione del database.

Per informazioni sulla creazione di un'attività di migrazione e sull'avvio della migrazione del database, consulta [Creazione di un'attività](#).

Specifiche delle impostazioni degli endpoint per Redis come destinazione

Per creare o modificare un endpoint di destinazione, è possibile utilizzare la console o le operazioni API `CreateEndpoint` o `ModifyEndpoint`.

Per una destinazione Redis, immetti nella console AWS DMS le Impostazioni specifiche dell'endpoint nella pagina Crea endpoint o Modifica endpoint della console.

Quando si utilizzano le operazioni API `CreateEndpoint` e `ModifyEndpoint`, specifica i parametri della richiesta per l'opzione `RedisSettings`. Nell'esempio seguente viene illustrato come eseguire questa operazione utilizzando la AWS CLI.

```
aws dms create-endpoint --endpoint-identifier my-redis-target
--endpoint-type target --engine-name redis --redis-settings
'{"ServerName": "sample-test-sample.zz012zz.cluster.eee1.cache.bbbxxx.com", "Port": 6379, "AuthType": "auth-token",
  "SslSecurityProtocol": "ssl-encryption", "AuthPassword": "notanactualpassword"}'
{
  "Endpoint": {
```

```

    "EndpointIdentifier": "my-redis-target",
    "EndpointType": "TARGET",
    "EngineName": "redis",
    "EngineDisplayName": "Redis",
    "TransferFiles": false,
    "ReceiveTransferredFiles": false,
    "Status": "active",
    "KmsKeyId": "arn:aws:kms:us-east-1:999999999999:key/x-b188188x",
    "EndpointArn": "arn:aws:dms:us-
east-1:555555555555:endpoint:ABCDEFGHIJKLMONOPQRSTUVWXYZ",
    "SslMode": "none",
    "RedisSettings": {
      "ServerName": "sample-test-sample.zz012zz.cluster.eee1.cache.bbbxxx.com",
      "Port": 6379,
      "SslSecurityProtocol": "ssl-encryption",
      "AuthType": "auth-token"
    }
  }
}

```

Di seguito sono riportati i parametri `--redis-settings`:

- `ServerName` (obbligatorio): di tipo `string`, specifica il cluster Redis in cui verranno migrati i dati e che si trova nello stesso VPC.
- `Port` (obbligatorio): di tipo `number`, il valore della porta utilizzato per accedere all'endpoint.
- `SslSecurityProtocol` (facoltativo): i valori validi sono `plaintext` e `ssl-encryption`. Il valore predefinito è `ssl-encryption`.

L'opzione `plaintext` non fornisce la crittografia Transport Layer Security (TLS) per il traffico tra endpoint e database.

Utilizza `ssl-encryption` per creare una connessione crittografata. `ssl-encryption` non richiede l'ARN dell'Autorità di certificazione (CA) SSL per verificare il certificato di un server, ma è possibile indentificarne facoltativamente uno utilizzando l'impostazione `SslCaCertificateArn`. Se non viene fornito l'ARN dell'Autorità di certificazione, DMS utilizza la CA root di Amazon.

Quando si utilizza una destinazione Redis on-premise, è possibile usare `SslCaCertificateArn` per importare un'Autorità di certificazione (CA) pubblica o privata in DMS e fornire l'ARN per l'autenticazione del server. La CA privata non è supportata quando si utilizza ElastiCache per Redis come destinazione.

- **AuthType** (obbligatorio): indica il tipo di autenticazione da eseguire per la connessione a Redis. I valori validi includono `none`, `auth-token` e `auth-role`.

L'opzione `auth-token` richiede che venga fornita "*AuthPassword*", mentre l'opzione `auth-role` richiede che vengano specificati "*AuthUserName*" e "*AuthPassword*".

Uso di Babelfish come destinazione per AWS Database Migration Service

È possibile migrare i dati da un database di origine Microsoft SQL Server a una destinazione Babelfish utilizzando AWS Database Migration Service.

Babelfish per Aurora PostgreSQL estende l'Edizione compatibile con PostgreSQL database Amazon Aurora con la possibilità di accettare connessioni al database dai client Microsoft SQL Server. In questo modo, le applicazioni create originariamente per SQL Server possono funzionare direttamente con Aurora PostgreSQL con poche modifiche al codice rispetto a una migrazione tradizionale e senza modificare i driver del database.

Per informazioni sulle versioni di Babelfish supportate da AWS DMS come destinazione, consulta [Obiettivi per AWS DMS](#). Le versioni precedenti di Babelfish su Aurora PostgreSQL richiedono un aggiornamento prima di utilizzare l'endpoint Babelfish.

Note

L'endpoint di destinazione Aurora PostgreSQL è il modo preferito per migrare i dati su Babelfish. Per ulteriori informazioni, consulta [Utilizzo di Babelfish per Aurora PostgreSQL come destinazione](#).

Per informazioni sull'utilizzo di Babelfish come endpoint di database, consulta [Babelfish per Aurora PostgreSQL](#) nella Guida per l'utente di Amazon Aurora User Guide

Prerequisiti per l'utilizzo di Babelfish come destinazione per AWS DMS

È necessario creare le tabelle prima di migrare i dati per assicurarsi che AWS DMS utilizzi i tipi di dati e i metadati delle tabelle corretti. Se non crei le tabelle sulla destinazione prima di eseguire la migrazione, è possibile che le tabelle vengano create da AWS DMS con tipi di dati e autorizzazioni errati. Ad esempio, AWS DMS crea una colonna timestamp come `binary(8)` e non fornisce la funzionalità `timestamp/rowversion` prevista.

Per preparare e creare le tabelle prima della migrazione

1. Esegui le istruzioni DDL di creazione della tabella che includono vincoli univoci, chiavi primarie o limiti predefiniti.

Non includere vincoli di chiave esterna o istruzioni DDL per oggetti come viste, stored procedure, funzioni o trigger. È possibile applicarli dopo la migrazione del database di origine.

2. Identifica eventuali colonne di identità, colonne calcolate o colonne contenenti tipi di dati rowversion o timestamp per le tabelle. Quindi, crea le regole di trasformazione necessarie per gestire i problemi noti durante l'esecuzione dell'attività di migrazione. Per ulteriori informazioni, consulta [Operazioni e regole di trasformazione](#).
3. Identifica le colonne con tipi di dati che Babelfish non supporta. Quindi, modifica le colonne interessate nella tabella di destinazione per utilizzare i tipi di dati supportati o crea una regola di trasformazione che le rimuova durante l'attività di migrazione. Per ulteriori informazioni, consulta [Operazioni e regole di trasformazione](#).

La tabella seguente elenca i tipi di dati di origine non supportati da Babelfish e il corrispondente tipo di dati di destinazione consigliato per l'uso.

Tipo di dati origine	Tipo di dati Babelfish consigliato
HEIRARCHYID	NVARCHAR(250)
GEOMETRY	VARCHAR(MAX)
GEOGRAPHY	VARCHAR(MAX)

Per impostare il livello delle unità di capacità di Aurora (ACU) per il database di origine Aurora PostgreSQL serverless V2

È possibile migliorare le prestazioni dell'attività di migrazione AWS DMS prima di eseguirla impostando il valore minimo delle ACU.

- Dalla finestra Impostazioni della capacità Severless v2, imposta Numero minimo di ACU su **2** o un livello ragionevole per il cluster di database Aurora.

Per ulteriori informazioni sulle unità di capacità di Aurora, consulta [Scelta dell'intervallo di capacità di Aurora serverless v2 per un cluster Aurora](#) nella Guida per l'utente di Amazon Aurora.

Dopo aver eseguito l'attività di migrazione AWS DMS, è possibile reimpostare il valore minimo delle ACU a un livello ragionevole per il database di origine Aurora PostgreSQL serverless V2.

Requisiti di sicurezza quando si utilizza Babelfish come destinazione per AWS Database Migration Service

Di seguito sono descritti i requisiti di sicurezza per l'utilizzo di AWS DMS con una destinazione Babelfish:

- Il nome utente dell'amministratore (l'utente Admin) utilizzato per creare il database.
- Accesso PSQL e utente con le autorizzazioni SELECT, INSERT, UPDATE, DELETE e REFERENCES sufficienti.

Autorizzazioni dell'utente per l'utilizzo di Babelfish come destinazione per AWS DMS

Important

Per motivi di sicurezza, l'account utente utilizzato per la migrazione dei dati deve corrispondere a un utente registrato in qualsiasi database Babelfish utilizzato come destinazione.

L'endpoint di destinazione Babelfish richiede le autorizzazioni utente minime per eseguire una migrazione AWS DMS.

Per creare un accesso e un utente Transact-SQL (T-SQL) con privilegi limitati

1. Crea un accesso e una password da utilizzare per la connessione al server.

```
CREATE LOGIN dms_user WITH PASSWORD = 'password';  
GO
```

2. Crea il database virtuale per il cluster Babelfish.

```
CREATE DATABASE my_database;  
GO
```

3. Crea l'utente T-SQL per il database di destinazione.

```
USE my_database
GO
CREATE USER dms_user FOR LOGIN dms_user;
GO
```

4. Per ogni tabella del database Babelfish, CONCEDI le autorizzazioni alle tabelle.

```
GRANT SELECT, DELETE, INSERT, REFERENCES, UPDATE ON [dbo].[Categories] TO dms_user;
```

Limitazioni relative all'utilizzo di Babelfish come destinazione per AWS Database Migration Service

Quando si utilizza un database Babelfish come destinazione per AWS DMS, si applicano le seguenti limitazioni:

- È supportata solo la modalità di preparazione delle tabelle "Nessuna operazione".
- Il tipo di dati ROWVERSION richiede una regola di mappatura delle tabelle che rimuove il nome della colonna dalla tabella durante l'attività di migrazione.
- Il tipo di dati sql_variant non è supportato.
- La modalità LOB completa è supportata. L'utilizzo di SQL Server come endpoint di origine richiede l'impostazione ForceFullLob=True dell'attributo di connessione dell'endpoint di SQL Server per consentire la migrazione dei LOB all'endpoint di destinazione.
- Le impostazioni delle attività di replica presentano le seguenti limitazioni:

```
{
  "FullLoadSettings": {
    "TargetTablePrepMode": "DO_NOTHING",
    "CreatePkAfterFullLoad": false,
  }.
}
```

- I tipi di dati TIME(7), DATETIME2(7) e DATETIMEOFFSET(7) in Babelfish limitano a 6 cifre il valore di precisione della parte dei secondi. Prendi in considerazione l'utilizzo di un valore di precisione di 6 cifre per la tabella di destinazione quando utilizzi questi tipi di dati. Per Babelfish

2.2.0 e versioni successive, quando si utilizza TIME(7) e DATETIME2(7), la settima cifra di precisione è sempre zero.

- In modalità DO_NOTHING, DMS verifica se la tabella è già presente. Se la tabella non esiste nello schema di destinazione, DMS crea la tabella in base alla definizione della tabella di origine e mappa i tipi di dati definiti dall'utente al relativo tipo di dati di base.
- L'attività di migrazione AWS DMS a una destinazione Babelfish non supporta le tabelle con colonne che utilizzano tipi di dati ROWVERSION o TIMESTAMP. È possibile utilizzare una regola di mappatura delle tabelle che rimuove il nome della colonna dalla tabella durante il processo di trasferimento. Nell'esempio di regola di trasformazione seguente, viene trasformata la tabella denominata Actor nell'origine per rimuovere tutte le colonne che iniziano con i caratteri col nella tabella Actor della destinazione.

```
{
  "rules": [{
    "rule-type": "selection",is
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "rule-action": "include"
  }, {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",
    "rule-action": "remove-column",
    "rule-target": "column",
    "object-locator": {
      "schema-name": "test",
      "table-name": "Actor",
      "column-name": "col%"
    }
  }
]}
```

- Per le tabelle con colonne identiche o calcolate, in cui le tabelle di destinazione utilizzano nomi con maiuscole e minuscole come Categorie, è necessario creare un'azione della regola di trasformazione che converta i nomi delle tabelle in lettere minuscole per l'attività DMS. L'esempio

seguente mostra come creare l'azione della regola di trasformazione Converti in minuscole usando la console AWS DMS. Per ulteriori informazioni, consulta [Operazioni e regole di trasformazione](#).

▼ Transformation rules

You can use transformation rules to change or transform schema, table or column names of some or all of the selected objects. [Info](#)

Add transformation rule

▼ where schema name is like 'dbo' and table name is like '%', convert-lowercase 📄 ✕

Rule target

Table ▼

Source name

Enter a schema ▼

Source name
Use the % character as a wildcard

dbo

Table name
Use the % character as a wildcard

%

Action

Make lowercase ▼

- Prima di Babelfish 2.2.0, DMS limitava a venti (20) il numero di colonne che era possibile replicare su un endpoint di destinazione Babelfish. Con Babelfish 2.2.0 il limite è aumentato a 100 colonne. Con Babelfish 2.4.0 e versioni successive il numero di colonne che è possibile replicare aumenta nuovamente. È possibile eseguire il seguente esempio di codice sul database SQL Server per determinare quali tabelle sono troppo lunghe.

```
USE myDB;
GO
DECLARE @Babelfish_version_string_limit INT = 8000; -- Use 380 for Babelfish versions
before 2.2.0
WITH bfendpoint
AS (
SELECT
  [TABLE_SCHEMA]
  , [TABLE_NAME]
```

```

    , COUNT( [COLUMN_NAME] ) AS NumberColumns
    , ( SUM( LEN( [COLUMN_NAME] ) + 3 )
+ SUM( LEN( FORMAT(ORDINAL_POSITION, 'N0') ) + 3 )
    + LEN( TABLE_SCHEMA ) + 3
+ 12 -- INSERT INTO string
+ 12) AS InsertIntoCommandLength -- values string
    , CASE WHEN ( SUM( LEN( [COLUMN_NAME] ) + 3 )
+ SUM( LEN( FORMAT(ORDINAL_POSITION, 'N0') ) + 3 )
    + LEN( TABLE_SCHEMA ) + 3
+ 12 -- INSERT INTO string
+ 12) -- values string
    >= @Babelfish_version_string_limit
    THEN 1
    ELSE 0
    END AS IsTooLong
FROM [INFORMATION_SCHEMA].[COLUMNS]
GROUP BY [TABLE_SCHEMA], [TABLE_NAME]
)
SELECT *
FROM bfeedpoint
WHERE IsTooLong = 1
ORDER BY TABLE_SCHEMA, InsertIntoCommandLength DESC, TABLE_NAME
;

```

Tipi di dati di destinazione per Babelfish

La tabella seguente mostra i tipi di dati di destinazione di Babelfish supportati quando si utilizza AWS DMS e la mappatura predefinita dai tipi di dati AWS DMS.

Per ulteriori informazioni sui tipi di dati AWS DMS, consulta [Tipi di dati per AWS Database Migration Service](#).

Tipo di dati AWS DMS	Tipo di dati di Babelfish
BOOLEAN	TINYINT
BYTES	VARBINARY (lunghezza)
DATE	DATE
TIME	TIME

Tipo di dati AWS DMS	Tipo di dati di Babelfish
INT1	SMALLINT
INT2	SMALLINT
INT4	INT
INT8	BIGINT
NUMERIC	NUMERIC(p,s)
REAL4	REAL
REAL8	FLOAT
STRING	<p>Se la colonna è di ora o data, effettuare le seguenti operazioni:</p> <ul style="list-style-type: none"> • Per SQL Server 2008 e versioni successive, utilizza DATETIME2. • Per le versioni precedenti, se il dimensionamento è pari o inferiore a 3, utilizzare DATETIME. In tutti gli altri casi, utilizzare VARCHAR (37). <p>Se la colonna non è di ora o data, utilizzare VARCHAR (lunghezza).</p>
UINT1	TINYINT
UINT2	SMALLINT
UINT4	INT
UINT8	BIGINT
WSTRING	NVARCHAR(length)

Tipo di dati AWS DMS	Tipo di dati di Babelfish
BLOB	<p>VARBINARY(max)</p> <p>Per utilizzare questo tipo di dati con DMS, è necessario abilitare l'utilizzo di BLOB per un'attività specifica. DMS supporta i tipi di dati BLOB solo nelle tabelle che includono una chiave primaria.</p>
CLOB	<p>VARCHAR(max)</p> <p>Per utilizzare questo tipo di dati con DMS, è necessario abilitare l'utilizzo di CLOB per un'attività specifica.</p>
NCLOB	<p>NVARCHAR(max)</p> <p>Per utilizzare questo tipo di dati con DMS, è necessario abilitare l'utilizzo di NCLOB per un'attività specifica. Durante la CDC, DMS supporta i tipi di dati NCLOB solo nelle tabelle che includono una chiave primaria.</p>

Utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service

Puoi utilizzare AWS Database Migration Service per migrare i dati dal tuo database di origine a un endpoint di destinazione Amazon Timestream, con il supporto per le migrazioni di dati di tipo Pieno carico e CDC.

Amazon Timestream è un servizio di database di serie temporali veloce, dimensionabile e serverless creato per l'importazione di grandi volumi di dati. I dati di serie temporali sono una sequenza di punti dati raccolti in un intervallo di tempo che vengono utilizzati per misurare gli eventi che cambiano nel tempo. Viene utilizzato per raccogliere, archiviare e analizzare metriche da applicazioni IoT, DevOps applicazioni e applicazioni di analisi. Una volta che i dati sono disponibili in Timestream, puoi visualizzarne e identificarne le tendenze e i modelli pressoché in tempo reale. Per informazioni

su Amazon Timestream, consulta [What is Amazon Timestream?](#) nella Guida per gli sviluppatori di Amazon Timestream.

Argomenti

- [Prerequisiti per l'utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service](#)
- [Impostazioni attività a pieno carico multithread](#)
- [Impostazioni attività di carico CDC multithread](#)
- [Impostazioni degli endpoint quando si utilizza Timestream come destinazione per AWS DMS](#)
- [Creazione e modifica di un endpoint di destinazione Amazon Timestream](#)
- [Utilizzo della mappatura degli oggetti per la migrazione dei dati in un argomento Timestream](#)
- [Limitazioni relative all'utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service](#)

Prerequisiti per l'utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service

Prima di configurare Amazon Timestream come destinazione per AWS DMS, è necessario creare un ruolo IAM. Questo ruolo deve consentire ad AWS DMS l'accesso ai dati migrati in Amazon Timestream. Il set minimo di autorizzazioni di accesso per il ruolo utilizzato per la migrazione a Timestream è illustrato nella seguente policy IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribeEndpoints",
      "Effect": "Allow",
      "Action": [
        "timestream:DescribeEndpoints"
      ],
      "Resource": "*"
    },
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
```

```

        "timestream:ListTables",
        "timestream:DescribeDatabase"
    ],
    "Resource": "arn:aws:timestream:region:account_id:database/DATABASE_NAME"
  },
  {
    "Sid": "VisualEditor1",
    "Effect": "Allow",
    "Action": [
      "timestream>DeleteTable",
      "timestream:WriteRecords",
      "timestream:UpdateTable",
      "timestream:CreateTable"
    ],
    "Resource": "arn:aws:timestream:region:account_id:database/DATABASE_NAME/
table/TABLE_NAME"
  }
]
}

```

Se intendi migrare tutte le tabelle, usa * per *TABLE_NAME* nell'esempio precedente.

Tieni presenti le seguenti indicazioni sull'utilizzo di Timestream come destinazione:

- Se intendi importare dati storici con timestamp creati da più di un anno, ti consigliamo di usare AWS DMS per scrivere i dati su Amazon S3 nel formato con valori separati da virgole (csv). Quindi, utilizza il caricamento in batch di Timestream per importare i dati in Timestream. Per ulteriori informazioni, consulta [Using batch load in Timestream](#) nella [Guida per gli sviluppatori di Amazon Timestream](#).
- Per le migrazioni di dati di tipo pieno carico eseguite da meno di un anno, ti consigliamo di impostare un periodo di conservazione dell'archivio di memoria della tabella Timestream maggiore o uguale al timestamp più vecchio. Quindi, una volta completata la migrazione, modifica il periodo di conservazione dell'archivio di memoria della tabella impostando il valore desiderato. Ad esempio, per migrare i dati con un timestamp creato da più 2 mesi, procedi come segue:
 - Imposta il periodo di conservazione dell'archivio di memoria della tabella di destinazione Timestream su 2 mesi.
 - Inizia la migrazione dei dati utilizzando AWS DMS.
 - Una volta completata la migrazione dei dati, modifica il periodo di conservazione della tabella di destinazione Timestream impostando il valore desiderato.

Ti consigliamo di stimare il costo dell'archivio di memoria prima della migrazione utilizzando le informazioni presenti nelle pagine seguenti:

- [Prezzi di Amazon Timestream](#)
- [AWS pricing calculator](#)
- Per le migrazioni dei dati di tipo CDC, ti consigliamo di impostare il periodo di conservazione dell'archivio di memoria della tabella di destinazione in modo che i dati importati rientrino nei limiti stabiliti. Per ulteriori informazioni, consulta [Writes Best Practices](#) nella [Guida per gli sviluppatori di Amazon Timestream](#).

Impostazioni attività a pieno carico multithread

Per contribuire ad aumentare la velocità di trasferimento dei dati, AWS DMS supporta l'attività di migrazione multithread di pieno carico a un endpoint di destinazione Timestream con le seguenti impostazioni:

- `MaxFullLoadSubTasks`: imposta questa opzione per indicare il numero massimo di tabelle da caricare in parallelo. DMS carica ogni tabella nella tabella di destinazione Amazon Timestream corrispondente utilizzando una sottoattività dedicata. Il valore predefinito è 8; il valore il massimo è 49.
- `ParallelLoadThreads`: utilizza questa opzione per specificare il numero di thread usati da AWS DMS per caricare ogni tabella nella tabella di destinazione Amazon Timestream. Il valore massimo per una destinazione Timestream è 32. Puoi chiedere che questo limite massimo venga aumentato.
- `ParallelLoadBufferSize`: utilizza questa opzione per specificare il numero massimo di record da archiviare nel buffer usato dai thread di caricamento parallelo per caricare i dati nella destinazione Amazon Timestream. Il valore predefinito è 50. Il valore massimo è 1.000. Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread.
- `ParallelLoadQueuesPerThread`: utilizza questa opzione per specificare il numero di code a cui accede ogni thread simultaneo per eliminare i record di dati dalle code e generare un carico batch per la destinazione. Il valore di default è 1. Tuttavia, per le destinazioni Amazon Timestream con varie dimensioni del payload, l'intervallo valido è compreso tra 5 e 512 code per thread.

Impostazioni attività di carico CDC multithread

Per promuovere le prestazioni del CDC, AWS DMS supporta le seguenti impostazioni di attività:

- `ParallelApplyThreads`: specifica il numero di thread simultanei utilizzati da AWS DMS durante un carico CDC per eseguire il push dei record di dati a un endpoint di destinazione Timestream. Il valore predefinito è 0 e il valore massimo è 32.
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per eseguire il push dei thread simultanei a un endpoint di destinazione Timestream durante un carico CDC. Il valore predefinito è 100 e il valore massimo è 1.000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per eliminare i record di dati dalle code e generare un carico in batch per un endpoint Timestream durante la CDC. Il valore predefinito è 1 e il valore massimo è 512.

Impostazioni degli endpoint quando si utilizza Timestream come destinazione per AWS DMS

È possibile utilizzare le impostazioni di endpoint per configurare il database di destinazione Timestream in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--timestream-settings '{"EndpointSetting": "value", ...}'`.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Timestream come destinazione.

Nome	Descrizione
<code>MemoryDuration</code>	<p>Imposta questo attributo per specificare il limite di conservazione dei dati migrati nell'archivio di memoria di Timestream. Il tempo è misurato in unità di ore. L'archivio di memoria di Timestream è ottimizzato per l'elevata velocità di trasmissione effettiva di importazione e l'accesso rapido.</p> <p>Valore predefinito: 24 (ore)</p>

Nome	Descrizione
	<p>Valori validi: da 1 a 8.736 (da 1 ora a 12 mesi misurati in ore)</p> <p>Esempio: <code>--timestream-settings '{"MemoryDuration": 20}'</code></p>
DatabaseName	<p>Imposta questo attributo per specificare il nome del database di destinazione Timestream.</p> <p>Tipo: stringa</p> <p>Esempio: <code>--timestream-settings '{"DatabaseName": "db_name"}</code></p>
TableName	<p>Imposta questo attributo per specificare il nome della tabella di destinazione Timestream.</p> <p>Tipo: stringa</p> <p>Esempio: <code>--timestream-settings '{"TableName": "table_name"}</code></p>
MagneticDuration	<p>Imposta questo attributo per specificare in giorni la durata dell'archivio magnetico applicata alle tabelle Timestream. Questo è il limite di conservazione per i dati importati. Timestream elimina qualsiasi timestamp che supera il limite di conservazione. Per ulteriori informazioni, consulta Storage nella Guida per gli sviluppatori di Amazon Timestream.</p> <p>Esempio: <code>--timestream-settings '{"MagneticDuration": "3"}</code></p>

Nome	Descrizione
CdcInsertsAndUpdates	<p>Imposta questo attributo su <code>true</code> per specificare che AWS DMS applica solo gli inserimenti e gli aggiornamenti, ma non le eliminazioni. Timestream non consente l'eliminazione di record, quindi se questo valore è <code>false</code>, AWS DMS annulla il record corrispondente nel database Timestream anziché eliminarlo. Per ulteriori informazioni, consulta la sezione seguente: Limitazioni.</p> <p>Valore predefinito: <code>false</code></p> <p>Esempio: <code>--timestream-settings '{"CdcInsertsAndUpdates": "true"}'</code></p>
EnableMagneticStoreWrites	<p>Imposta questo attributo su <code>true</code> per abilitare le scritture dell'archivio magnetico. Quando questo valore è <code>false</code>, AWS DMS non scrive i record con un timestamp precedente al periodo di conservazione nell'archivio di memoria della tabella di destinazione perché Timestream non consente le scritture dell'archivio magnetico per impostazione predefinita. Per ulteriori informazioni, consulta Writes Best Practices nella Guida per gli sviluppatori di Amazon Timestream.</p> <p>Valore predefinito: <code>false</code></p> <p>Esempio: <code>--timestream-settings '{"EnableMagneticStoreWrites": "true"}'</code></p>

Creazione e modifica di un endpoint di destinazione Amazon Timestream

Dopo aver creato un ruolo IAM e stabilito il set minimo di autorizzazioni di accesso, puoi creare un endpoint di destinazione Amazon Timestream utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#) con la sintassi JSON `--timestream-settings '{"EndpointSetting": "value", ...}'`.

Negli esempi seguenti viene illustrato come creare o modificare un endpoint di destinazione Timestream mediante la AWS CLI.

Comando per creare l'endpoint di destinazione Timestream

```
aws dms create-endpoint --endpoint-identifier timestream-target-demo
--endpoint-type target --engine-name timestream
--service-access-role-arn arn:aws:iam::123456789012:role/my-role
--timestream-settings
{
  "MemoryDuration": 20,
  "DatabaseName":"db_name",
  "MagneticDuration": 3,
  "CdcInsertsAndUpdates": true,
  "EnableMagneticStoreWrites": true,
}
```

Comando per modificare l'endpoint di destinazione Timestream

```
aws dms modify-endpoint --endpoint-identifier timestream-target-demo
--endpoint-type target --engine-name timestream
--service-access-role-arn arn:aws:iam::123456789012:role/my-role
--timestream-settings
{
  "MemoryDuration": 20,
  "MagneticDuration": 3,
}
```

Utilizzo della mappatura degli oggetti per la migrazione dei dati in un argomento Timestream

AWS DMS utilizza le regole di mappatura delle tabelle per mappare i dati dall'origine all'argomento di destinazione Timestream. Per mappare i dati a un argomento di destinazione, è necessario utilizzare una regola di mappatura delle tabelle denominata mappatura degli oggetti. La mappatura degli oggetti consente di definire il modo in cui i record di dati dell'origine vengono mappati ai record di dati pubblicati nell'argomento Timestream.

Gli argomenti Timestream non dispongono di una struttura preimpostata oltre a una chiave di partizione.

Note

Non è necessario utilizzare la mappatura degli oggetti. È possibile utilizzare la normale mappatura delle tabelle per varie trasformazioni. Tuttavia, il tipo di chiave della partizione segue questi comportamenti predefiniti:

- La chiave primaria viene utilizzata come chiave di partizione per il pieno carico.
- Se non vengono utilizzate le impostazioni delle attività di applicazione parallela, `schema.table` viene usato come chiave di partizione per la CDC.
- Se vengono utilizzate le impostazioni delle attività di applicazione parallela, la chiave primaria viene utilizzata come chiave di partizione per CDC.

Per creare una regola di mappatura degli oggetti, è necessario impostare il parametro `rule-type` su `object-mapping`. Questa regola specifica il tipo di mappatura degli oggetti da utilizzare. Di seguito è riportata la struttura per la regola.

```
{
  "rules": [
    {
      "rule-type": "object-mapping",
      "rule-id": "id",
      "rule-name": "name",
      "rule-action": "valid object-mapping rule action",
      "object-locator": {
        "schema-name": "case-sensitive schema name",
        "table-name": ""
      }
    }
  ]
}
```

```
{
  "rules": [
    {
      "rule-type": "object-mapping",
      "rule-id": "1",
      "rule-name": "timestream-map",
      "rule-action": "map-record-to-record",

```

```
    "target-table-name": "tablename",
    "object-locator": {
      "schema-name": "",
      "table-name": ""
    },
    "mapping-parameters": {
      "timestream-dimensions": [
        "column_name1",
        "column_name2"
      ],
      "timestream-timestamp-name": "time_column_name",
      "timestream-multi-measure-name": "column_name1or2",
      "timestream-hash-measure-name": true or false,
      "timestream-memory-duration": x,
      "timestream-magnetic-duration": y
    }
  }
]
```

AWS DMS attualmente supporta `map-record-to-record` e `map-record-to-document` come i soli valori validi per il parametro `rule-action`. I valori `map-record-to-record` e `map-record-to-document` specificano le operazioni eseguite per impostazione predefinita da AWS DMS sui record che non vengono esclusi sulla base dell'elenco di attributi `exclude-columns`. Questi valori non influiscono in alcun modo sulle mappature degli attributi.

Utilizza `map-record-to-record` per la migrazione da un database relazionale a un argomento Timestream. Questo tipo di regola utilizza il valore `taskResourceId.schemaName.tableName` del database relazionale come chiave di partizione nell'argomento Timestream e crea un attributo per ogni colonna del database di origine. Quando utilizzi `map-record-to-record`, per qualsiasi colonna della tabella di origine non presente nell'elenco di attributi `exclude-columns`, AWS DMS crea un attributo corrispondente nell'argomento di destinazione. Questo attributo corrispondente viene creato indipendentemente dal fatto che tale colonna di origine venga utilizzata o meno in una mappatura degli attributi.

Per comprendere il funzionamento di `map-record-to-record`, è opportuno esaminarne il comportamento in azione. Per questo esempio, supponiamo che tu stia iniziando con una riga di tabella del database relazionale con la struttura e i dati seguenti.

FirstName	LastName	StoreId	HomeAddress	HomePhone	WorkAddress	WorkPhone	DateofBirth
Randy	Marsh	5	221B Baker Street	123456789 0	31 Spooner Street, Quahog	987654321 0	02/29/198 8

Per eseguire la migrazione di queste informazioni da uno schema denominato `Test` a un argomento Timestream, crea le regole per mappare i dati sull'argomento di destinazione. La regola seguente illustra la mappatura.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "rule-action": "include",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      }
    },
    {
      "rule-type": "object-mapping",
      "rule-id": "2",
      "rule-name": "DefaultMapToTimestream",
      "rule-action": "map-record-to-record",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Customers"
      }
    }
  ]
}
```

Dato un argomento Timestream e una chiave di partizione (in questo caso, `taskResourceId.schemaName.tableName`), il seguente esempio illustra il formato di record risultante per l'argomento di destinazione Timestream utilizzando i dati di esempio:

```
{
  "FirstName": "Randy",
  "LastName": "Marsh",
  "StoreId": "5",
  "HomeAddress": "221B Baker Street",
  "HomePhone": "1234567890",
  "WorkAddress": "31 Spooner Street, Quahog",
  "WorkPhone": "9876543210",
  "DateOfBirth": "02/29/1988"
}
```

Limitazioni relative all'utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service

Quando si utilizza Amazon Timestream come destinazione si applicano le seguenti limitazioni:

- **Dimensioni e timestamp:** Timestream utilizza le dimensioni e i timestamp dei dati di origine come chiave primaria composta e non consente di alterare questi valori. Ciò significa che se modifichi il timestamp o le dimensioni di un record nel database di origine, il database Timestream prova a creare un nuovo record. Quindi, se modifichi la dimensione o il timestamp di un record in modo che corrisponda a quello di un altro record esistente, AWS DMS aggiorna i valori dell'altro record anziché creare un nuovo record o aggiornare il record precedente corrispondente.
- **Comandi DDL:** la versione corrente di AWS DMS supporta solo i comandi DDL `CREATE TABLE` e `DROP TABLE`.
- **Limitazioni relative ai record:** Timestream include delle limitazioni per i record, ad esempio la dimensione del record e la dimensione della misura. Per ulteriori informazioni, consultare [Quote](#) nella [Guida per gli sviluppatori di Amazon Timestream](#).
- **Eliminazione di record e valori nulli:** Timestream non supporta l'eliminazione di record. Per supportare la migrazione dei record eliminati dall'origine, AWS DMS cancella i campi corrispondenti nei record del database di destinazione Timestream. AWS DMS modifica i valori nei campi del record di destinazione corrispondente impostando 0 per i campi numerici, null per i campi di testo e false per i campi booleani.
- Timestream come destinazione non supporta origini diverse da database relazionali.
- AWS DMS supporta Timestream come destinazione solo nelle seguenti regioni:
 - Stati Uniti orientali (Virginia settentrionale)
 - Stati Uniti orientali (Ohio)

- US West (Oregon)
- Europa (Irlanda)
- Europa (Francoforte)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)
- Timestream come destinazione non supporta l'impostazione di `TargetTablePrepMode` su `TRUNCATE_BEFORE_LOAD`. Ti consigliamo di utilizzare `DROP_AND_CREATE` per questa impostazione.

Utilizzo di Amazon RDS per Db2 e IBM Db2 LUW come destinazione per AWS DMS

È possibile migrare i dati a un database Amazon RDS per Db2 o Db2 on-premise da un database Db2 LUW utilizzando AWS Database Migration Service (AWS DMS).

Per informazioni sulle versioni di Db2 LUW supportate da AWS DMS come destinazione, consulta [Obiettivi per AWS DMS](#).

Puoi utilizzare il protocollo Secure Sockets Layer (SSL) per crittografare le connessioni tra l'endpoint Db2 LUW e l'istanza di replica. Per ulteriori informazioni sull'utilizzo di SSL con un endpoint Db2 LUW, consulta [Utilizzo di SSL con AWS Database Migration Service](#).

Limitazioni relative all'utilizzo di Db2 LUW come destinazione per AWS DMS

Quando si utilizza un database Db2 LUW come destinazione per AWS DMS, si applicano le seguenti limitazioni: Per le limitazioni relative all'utilizzo di Db2 LUW come origine, consulta [Limitazioni nell'utilizzo di Db2 LUW come fonte per AWS DMS](#).

- AWS DMS supporta Db2 LUW come destinazione solo quando l'origine è Db2 LUW o Db2 for z/OS.
- L'utilizzo di Db2 LUW come destinazione non supporta le repliche con la modalità LOB completa.
- L'utilizzo di Db2 LUW come destinazione non supporta il tipo di dati XML nella fase di pieno carico. Questa è una limitazione dell'utilità IBM `dbload`. Per ulteriori informazioni, consulta [The `dbload` utility](#) nella documentazione IBM Informix Servers.
- AWS DMS tronca i campi BLOB con valori corrispondenti alle virgolette doppie ("). Questa è una limitazione dell'utilità IBM `dbload`.

Impostazioni degli endpoint quando si utilizza Db2 LUW come destinazione per AWS DMS

È possibile utilizzare le impostazioni degli endpoint per configurare il database di destinazione Db2 LUW in modo simile a come si usano gli attributi aggiuntivi di connessione. Le impostazioni vengono specificate quando si crea l'endpoint di destinazione utilizzando la console AWS DMS o il comando `create-endpoint` nella [AWS CLI](#), con la sintassi JSON `--ibm-db2-settings '{"EndpointSetting": "value", ...}'`.

La tabella riportata di seguito mostra le impostazioni degli endpoint che è possibile utilizzare con Db2 LUW come destinazione.

Nome	Description
KeepCsvFiles	Se il valore è true, AWS DMS salva nella destinazione Db2 LUW tutti i file .csv utilizzati per replicare i dati. DMS utilizza questi file per l'analisi e la risoluzione dei problemi.
LoadTimeout	La quantità di tempo (in millisecondi) prima che AWS DMS generi il timeout delle operazioni eseguite da DMS sulla destinazione Db2. Il valore predefinito è di 1200 (20 minuti).
MaxFileSize	Specifica la dimensione massima (in KB) dei file .csv utilizzati per il trasferimento dei dati a Db2 LUW.
WriteBufferSize	La dimensione (in KB) del buffer di scrittura dei file in memoria utilizzato durante la generazione di file .csv sul disco locale nell'istanza di replica DMS. Il valore predefinito è 1024 (1 MB).

Configurazione degli endpoint VPC come endpoint di origine e di destinazione AWS DMS

AWS DMS supporta gli endpoint del cloud privato virtuale (VPC) Amazon come origini e destinazioni. AWS DMS può connettersi a qualsiasi database di origine o destinazione AWS con endpoint Amazon

VPC purché nel VPC AWS DMS siano definiti esplicitamente i percorsi verso questi database di origine e di destinazione.

Supportando gli endpoint Amazon VPC, AWS DMS semplifica la gestione della sicurezza di rete end-to-end per tutte le attività di replica senza ulteriori configurazioni e impostazioni di rete. L'utilizzo degli endpoint VPC per tutti gli endpoint di origine e di destinazione garantisce che tutto il traffico rimanga all'interno del VPC e sotto il tuo controllo. Gli aggiornamenti a AWS DMS 3.4.7 e versioni successive richiedono la configurazione di AWS DMS per utilizzare gli endpoint VPC o per usare percorsi pubblici verso tutti gli endpoint di origine e di destinazione che interagiscono con i seguenti Amazon Web Services:

- Amazon S3
- Amazon Kinesis
- AWS Secrets Manager
- Amazon DynamoDB
- Amazon Redshift
- Servizio OpenSearch di Amazon

Potresti aver bisogno di endpoint VPC per supportare AWS DMS a partire dalla versione 3.4.7, come descritto di seguito.

Chi è interessato dalla migrazione a AWS DMS 3.4.7 e versioni successive?

Si è interessati se si utilizza uno o più degli endpoint AWS DMS elencati in precedenza e questi endpoint non sono instradabili pubblicamente o non hanno endpoint VPC già associati.

Chi non è interessato dalla migrazione a AWS DMS 3.4.7 e versioni successive?

Non si è interessati se:

- Non utilizzi uno o più degli endpoint AWS DMS elencati in precedenza.
- Utilizzi uno qualsiasi degli endpoint elencati in precedenza e questi sono instradabili pubblicamente.
- Utilizzi uno qualsiasi degli endpoint elencati in precedenza a cui sono associati endpoint VPC.

Preparazione di una migrazione a AWS DMS 3.4.7 e versioni successive

Per evitare errori delle attività AWS DMS quando utilizzi uno degli endpoint descritti in precedenza, esegui una delle seguenti operazioni prima di aggiornare AWS DMS alla versione 3.4.7 o successiva:

- Rendi gli endpoint AWS DMS interessati instradabili pubblicamente. Ad esempio, aggiungi una route gateway Internet (IGW) a un VPC già utilizzato dall'istanza di replica AWS DMS per rendere instradabili pubblicamente tutti gli endpoint di origine e di destinazione.
- Crea gli endpoint VPC per accedere a tutti gli endpoint di origine e di destinazione utilizzati da AWS DMS come descritto di seguito.

Per gli endpoint VPC esistenti che utilizzi per gli endpoint di origine e di destinazione AWS DMS, assicurati che applichino una policy di attendibilità conforme al documento di policy XML `dms-vpc-role`. Per ulteriori informazioni sul documento di policy XML, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

In alternativa, configura le istanze di replica come endpoint VPC aggiungendo un endpoint VPC al VPC che le contiene. Se hai configurato le istanze di replica senza endpoint pubblici, l'aggiunta di un endpoint VPC accessibile pubblicamente al VPC che contiene le istanze di replica le rende accessibili pubblicamente. Non sono necessarie altre operazioni per associare in modo specifico le istanze di replica all'endpoint VPC.

Note

Servizi diversi potrebbero avere configurazioni dell'endpoint VPC univoche. Ad esempio, quando si utilizza AWS Secrets Manager, in genere non è necessario modificare la tabella di routing. Verifica sempre i requisiti specifici per ogni servizio.

Creazione di un endpoint VPC sul VPC contenente l'istanza di replica

1. Accedere ad AWS Management Console e aprire la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nella barra dei menu della console VPC, scegli la stessa Regione AWS dell'istanza di replica AWS DMS.
3. Nel riquadro di navigazione VPC scegli Endpoint.
4. In Endpoint scegli Crea endpoint.

5. Puoi facoltativamente specificare un tag per il nome. Ad esempio, **my-endpoint-DynamoDB-01**.
6. In Servizi, solo per S3 o DynamoDB scegli un Nome servizio con Tipo impostato su Gateway.
7. In VPC scegli lo stesso VPC dell'istanza di replica AWS DMS per creare l'endpoint.
8. In Tabelle di routing scegli tutti i valori ID tabella di routing disponibili.
9. Per specificare il controllo degli accessi scegli Accesso completo in Policy. Se desideri utilizzare uno strumento di creazione di policy per specificare il controllo degli accessi, scegli Personalizzato. In ogni caso, utilizza una policy di attendibilità conforme al documento di policy JSON `dms-vpc-role`. Per ulteriori informazioni sul documento di policy, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).
10. In Endpoint verifica che lo Stato dell'endpoint VPC appena creato sia Disponibile.

Per ulteriori informazioni sulla configurazione degli endpoint VPC per un'istanza di replica AWS DMS, consulta [Configurazioni di rete per la migrazione del database](#). Per ulteriori informazioni sulla creazione di endpoint VPC di interfaccia per l'accesso ai servizi AWS in generale, consulta [Accesso a Servizio AWS utilizzando un endpoint VPC dell'interfaccia](#) nella Guida di AWS PrivateLink. Per informazioni sulla disponibilità regionale di AWS DMS per gli endpoint VPC, consulta la [tabella delle regioni AWS](#).

Istruzioni DDL supportate da AWS DMS

Durante il processo di migrazione dei dati, puoi eseguire istruzioni DDL (Data Definition Language) nel database di origine. Queste istruzioni vengono replicate nel database di destinazione dal server di replica.

Le istruzioni DDL supportate includono le seguenti:

- Create table (Crea tabella)
- Drop table (Elimina tabella)
- Rename table (Rinomina tabella)
- Tronca tabella
- Add column (Aggiungi colonna)
- Drop column (Elimina colonna)
- Rename column (Rinomina colonna)

- Change column data type (Modifica tipo di dati della colonna)

DMS non acquisisce tutte le istruzioni DDL supportate per alcuni tipi di motori di origine. Inoltre, DMS gestisce le istruzioni DDL in modo diverso quando le applica a motori di destinazione specifici. Per informazioni su quali istruzioni DDL sono supportate per un'origine specifica e su come vengono applicate a una destinazione, consulta l'argomento della documentazione specifico per l'endpoint di origine e di destinazione.

È possibile utilizzare le impostazioni delle attività per configurare il modo in cui DMS gestisce l'approccio DDL durante l'acquisizione dei dati di modifica (CDC). Per ulteriori informazioni, consulta [Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche](#).

Utilizzo delle attività di AWS DMS

L'attività AWS Database Migration Service (AWS DMS) è il luogo dove si svolge tutto il lavoro. Puoi specificare le tabelle (o le viste) e gli schemi da utilizzare per la migrazione e qualsiasi elaborazione speciale, ad esempio i requisiti di registrazione, i dati della tabella di controllo e la gestione degli errori.

Un'attività può essere composta da tre fasi principali:

- Migrazione dei dati esistenti (pieno carico)
- L'applicazione delle modifiche memorizzate nella cache
- Replica continua (acquisizione dei dati di modifica)

Per ulteriori informazioni e una panoramica sul modo in cui le attività di migrazione AWS DMS migrano i dati, consulta [Visualizzazione di alto livello di AWS DMS](#).

Quando crei un'attività di migrazione, devi conoscere diversi elementi:

- Prima di poter creare un'attività, ricordati di creare un endpoint di origine, un endpoint di destinazione e un'istanza di replica.
- Puoi specificare molte impostazioni delle attività per configurare in modo personalizzato l'attività di migrazione. Puoi impostare tali opzioni mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o l'API AWS DMS. Queste impostazioni includono la specifica del modo in cui gli errori di migrazione sono gestiti, la registrazione degli errori e le informazioni sulla tabella di controllo. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).
- Una volta creata un'attività, puoi eseguirla immediatamente. Le tabelle di destinazione con le definizioni dei metadati necessarie vengono automaticamente create e caricate e puoi specificare la replica continua.
- Per impostazione predefinita, AWS DMS avvia l'attività non appena viene creata. Tuttavia, in alcune situazioni, potresti volere posticipare l'inizio dell'attività. Ad esempio, quando utilizzi AWS CLI, potresti disporre di un processo che crea un'attività e un processo diverso che avvia l'attività in base a un evento di attivazione. Se necessario, puoi posticipare l'inizio dell'attività.
- Puoi monitorare, arrestare o riavviare le attività mediante la console, AWS CLI o l'API AWS DMS. Per informazioni sull'interruzione di un'attività utilizzando l'API AWS DMS, consulta [StopReplicationTask](#) nella [Documentazione di riferimento delle API AWS DMS](#).

Di seguito sono riportate alcune operazioni che puoi eseguire quando utilizzi un'attività AWS DMS.

Attività	Documentazione di riferimento
<p>Creazione di un'attività</p> <p>Quando crei un'attività, specifichi l'origine, la destinazione, l'istanza di replica e le eventuali impostazioni di migrazione.</p>	<p>Creazione di un'attività</p>
<p>Creazione di un'attività di replica continua</p> <p>Puoi configurare un'attività per fornire la replica continua tra l'origine e la destinazione.</p>	<p>Creazione di attività per la replica continua mediante AWS DMS</p>
<p>Applicazione delle impostazioni dell'attività</p> <p>Ogni attività dispone di impostazioni che puoi configurare in base alle esigenze della migrazione del database. Puoi creare queste impostazioni in un file JSON o puoi specificare alcune di esse mediante la console AWS DMS. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta Esempio di impostazioni delle attività.</p>	<p>Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service</p>
<p>Utilizzo della mappatura delle tabelle</p> <p>La mappatura delle tabelle specifica le impostazioni aggiuntive delle attività per le tabelle che utilizzano</p>	<p>Regole di selezione</p> <p>Operazioni e regole di selezione</p> <p>Regole di trasformazione</p>

Attività	Documentazione di riferimento
<p>diversi tipi di regole. Queste regole consentono di specificare l'origine dati, lo schema di origine, le tabelle e le viste, i dati, le eventuali trasformazioni di tabelle e dati che devono verificarsi durante l'attività e le impostazioni relative alla migrazione e di tali tabelle e colonne dall'origine alla destinazione.</p>	<p>Operazioni e regole di trasformazione</p> <p>Regole per le impostazioni delle tabelle</p> <p>Regole e operazioni delle impostazioni di tabella e raccolta</p>
<p>Esecuzione di valutazioni delle attività di pre-migrazione</p> <p>È possibile abilitare ed eseguire le valutazioni delle attività di pre-migrazione che mostrano i problemi relativi a un database di origine e di destinazione supportato che possono causare difficoltà durante una migrazione. Sono inclusi problemi come tipi di dati non supportati, indici e chiavi primarie non corrispondenti e altre impostazioni delle attività in conflitto. Queste valutazioni di pre-migrazione vengono eseguite prima dell'esecuzione dell'attività per identificare potenziali problemi prima che si verifichino durante una migrazione.</p>	<p>Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività</p>

Attività	Documentazione di riferimento
<p data-bbox="110 226 370 258">Convalida dei dati</p> <p data-bbox="110 306 634 579">La convalida dei dati è un'impostazione dell'attività che puoi utilizzare in modo che AWS DMS confronti i dati sul datastore di destinazione con i dati provenienti dal datastore di origine.</p>	<p data-bbox="688 226 1146 258">Convalida dei dati in AWS DMS.</p>
<p data-bbox="110 625 410 657">Modifica di un'attività</p> <p data-bbox="110 705 599 789">Quando un'attività viene arrestata, puoi modificarne le impostazioni.</p>	<p data-bbox="688 625 987 657">Modifica di un'attività</p>
<p data-bbox="110 835 480 867">Spostamento di un'attività</p> <p data-bbox="110 915 623 1041">Quando un'attività viene interrotta, è possibile spostarla in un'istanza di replica diversa.</p>	<p data-bbox="688 835 1055 867">Spostamento di un'attività</p>
<p data-bbox="110 1087 615 1171">Ricaricamento delle tabelle durante un'attività</p> <p data-bbox="110 1220 600 1346">Puoi ricaricare una tabella durante un'attività se si verifica un errore durante l'esecuzione.</p>	<p data-bbox="688 1087 1333 1119">Ricaricamento delle tabelle durante un'attività</p>
<p data-bbox="110 1392 388 1423">Applicazione di filtri</p> <p data-bbox="110 1472 643 1839">Puoi utilizzare i filtri di origine per limitare il numero e il tipo di record trasferiti dall'origine alla destinazione. Ad esempio, puoi specificare che solo i dipendenti con un'ubicazione di sede vengano spostati al database di destinazione. I filtri vengono applicati su una colonna di dati.</p>	<p data-bbox="688 1392 1024 1423">Utilizzo di filtri di origine</p>

Attività	Documentazione di riferimento
Monitoraggio di un'attività Vi sono diversi modi per ottenere informazioni sulle prestazioni di un'attività e sulle tabelle utilizzate dall'attività.	Monitoraggio delle attività AWS DMS
Gestione dei log delle attività Puoi visualizzare ed eliminare i log delle attività mediante l'API AWS DMS o l'AWS CLI.	Visualizzazione e gestione dei log delle attività AWS DMS

Argomenti

- [Creazione di un'attività](#)
- [Creazione di attività per la replica continua mediante AWS DMS](#)
- [Modifica di un'attività](#)
- [Spostamento di un'attività](#)
- [Ricaricamento delle tabelle durante un'attività](#)
- [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#)
- [Utilizzo di filtri di origine](#)
- [Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività](#)
- [Specifica dei dati supplementari per le impostazioni delle attività](#)

Creazione di un'attività

Per creare un'attività di AWS DMS migrazione, procedi come segue:

- Creare un endpoint di origine, un endpoint di destinazione e un'istanza di replica prima della creazione di un'attività di migrazione.
- Scegliere un metodo di migrazione:

- **Migrazione dei dati al database di destinazione:** questo processo crea file o tabelle nel database di destinazione e definisce automaticamente i metadati necessari sulla destinazione. Popola inoltre le tabelle con i dati provenienti dall'origine. I dati delle tabelle vengono caricati in parallelo per una maggiore efficienza. Questo processo è l'opzione Migra dati esistenti in AWS Management Console e viene richiamato `Full Load` nell'API.
- **Acquisizione delle modifiche durante la migrazione:** questo processo acquisisce le modifiche al database di origine che si verificano mentre i dati vengono migrati dall'origine alla destinazione. Quando la migrazione dei dati richiesti originariamente è stata completata, il processo Change Data Capture (CDC) applica le modifiche acquisite al database di destinazione. Le modifiche vengono acquisite e applicate come unità delle singole transazioni sottoposte a commit e puoi aggiornare più tabelle di destinazione diverse come un singolo commit di origine. Questo approccio garantisce l'integrità delle transazioni nel database di destinazione. Questo processo è l'opzione Migra dati esistenti e replica le modifiche in corso nella console ed è denominato `full-load-and-cdc` nell'API.
- **Replica delle sole modifiche dei dati sul database di origine:** questo processo legge il file di log di ripristino del sistema di gestione di database (DBMS) di origine e raggruppa le voci per ogni transazione. In alcuni casi, non è AWS DMS possibile applicare le modifiche alla destinazione entro un periodo di tempo ragionevole (ad esempio, se la destinazione non è accessibile). In questi casi, AWS DMS memorizza nel buffer le modifiche sul server di replica per il tempo necessario. Non rilegge i log DBMS di origine, operazione che può richiedere molto tempo. Questo processo è l'opzione Replicate data changes only (Replica solo le modifiche dei dati) nella console AWS DMS .
- Determina il modo in cui l'attività deve gestire gli oggetti binari di grandi dimensioni (LOB) sull'origine. Per ulteriori informazioni, consulta [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#).
- Specifica le impostazioni delle attività di migrazione. Questi valori includono la configurazione della registrazione, la specifica dei dati scritti nella tabella di controllo di migrazione, il modo in cui gli errori sono gestiti e altre impostazioni. Per ulteriori informazioni sulle impostazioni delle attività, consulta [Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service](#).
- Configura la mappatura delle tabelle per definire le regole per selezionare e filtrare i dati che stai migrando. Per ulteriori informazioni sulla mappatura delle tabelle, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#). Prima di specificare la mappatura, consulta la sezione della documentazione sulla mappatura del tipo di dati per il database di origine e di destinazione.

- Abilita ed esegui le valutazioni delle attività di pre-migrazione prima di eseguire l'attività. Per ulteriori informazioni sulle valutazioni di pre-migrazione, consulta [Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività](#).
- Specificare gli eventuali dati supplementari necessari affinché l'attività esegua la migrazione dei dati. Per ulteriori informazioni, consulta [Specifiche dei dati supplementari per le impostazioni delle attività](#).

Puoi scegliere di avviare un'attività non appena hai completato la specifica delle informazioni per tale attività nella pagina Create task (Crea attività). In alternativa, puoi avviare l'attività dalla pagina Dashboard anche in un secondo momento.

Nella procedura seguente si presuppone che siano già stati specificati gli endpoint e le informazioni sull'istanza di replica. Per ulteriori informazioni sulla configurazione degli endpoint, consulta [Creazione di endpoint di origine e destinazione](#).

Per creare un'attività di migrazione

1. [Accedere AWS Management Console e aprire la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

Se hai effettuato l'accesso come utente AWS Identity and Access Management (IAM), assicurati di disporre delle autorizzazioni di accesso AWS DMS appropriate. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Nel riquadro di navigazione scegli Attività di migrazione del database e seleziona Crea attività.
3. Nella sezione Configurazione dell'attività della pagina Crea attività di migrazione del database specifica le opzioni dell'attività. Nella tabella seguente vengono illustrate le impostazioni.

Create database migration task

Task configuration

Task identifier

Type a unique identifier for the task

Descriptive Amazon Resource Name (ARN) - *optional*

A friendly name to override the default DMS ARN. You cannot modify it after creation.

Friendly-ARN-name

Replication instance

Choose a replication instance

Source database endpoint

Choose a source database endpoint

Target database endpoint

Choose a target database endpoint

Migration type [Info](#)

Migrate existing data

Per questa opzione

Eeguire questa operazione

Identificativo dell'attività

Immetti un nome per l'attività.

Per questa opzione	Eeguire questa operazione
Nome della risorsa Amazon (ARN) descrittivo: facoltativo	Un nome descrittivo per sovrascrivere l' AWS DMS ARN predefinito. Non puoi modificare il nome dopo aver creato l'attività.
Replication instance (Istanza di replica)	Mostra l'istanza di replica da utilizzare.
Endpoint del database di origine	Mostra l'endpoint di origine da utilizzare.
Endpoint del database di destinazione	Mostra l'endpoint di destinazione da utilizzare.
Tipo di migrazione	Scegli il metodo di migrazione da utilizzare. È possibile scegliere di migrare al database di destinazione solo i dati esistenti o inviare al database di destinazione le modifiche continue in aggiunta ai dati migrati.

4. Nella sezione Impostazioni delle attività specifica i valori per la modifica dell'attività, la modalità di preparazione della tabella di destinazione, l'attività di arresto, le impostazioni LOB, la convalida e la registrazione.

Per questa opzione	Eeguire questa operazione
Modalità di modifica	Scegli se utilizzare la procedura guidata o l'editor JSON per specificare le impostazioni delle attività. Se scegli la procedura guidata verranno visualizzate le seguenti opzioni.
Modalità di avvio CDC per le transazioni di origine	Questa impostazione è visibile solo se si sceglie Replica solo le modifiche ai dati per Tipo di migrazione nella sezione precedente. Disabilita la modalità di avvio CDC personalizzata: se scegli questa opzione, puoi avviare l'attività automaticamente utilizzando l'opzione Automaticamente al momento della creazione riportata di seguito o manualmente utilizzando la console.

Per questa opzione	Eseguire questa operazione
	Abilita la modalità di avvio CDC personalizzata: se scegli questa opzione, puoi specificare un'ora di inizio UTC personalizzata per avviare l'elaborazione delle modifiche.

Per questa opzione	Eseguire questa operazione
Modalità di preparazione della tabella di destinazione	<p>Questa impostazione è visibile solo se scegli Migra i dati esistenti o Migrazione dei dati esistenti e replica delle modifiche in corso per Tipo di migrazione nella sezione precedente.</p> <p>Non fare nulla: in modalità Non fare nulla, AWS DMS presuppone che le tabelle di destinazione siano state create in precedenza sulla destinazione. Se le tabelle non sono vuote, potrebbero verificarsi dei conflitti durante la migrazione dei dati e causare un errore nell'attività DMS. Se la tabella di destinazione non esiste, DMS la crea automaticamente. La struttura delle tabelle rimane invariata e gli eventuali dati esistenti rimangono nelle tabelle. La modalità Nessuna azione va bene per le attività solo CDC quando le tabelle di destinazione sono state compilate dall'origine e la replica continua viene applicata per mantenere sincronizzate l'origine e la destinazione. Per creare anticipatamente le tabelle, puoi utilizzare AWS Schema Conversion Tool (AWS SCT). Per ulteriori informazioni, vedere Installazione. AWS SCT</p> <p>Rilascia tabelle nella destinazione: nella modalità Rilascia tabelle nella destinazione AWS DMS rilascia le tabelle di destinazione e le ricrea prima di avviare la migrazione. Questo approccio garantisce che le tabelle di destinazione siano vuote all'inizio della migrazione. AWS DMS crea solo gli oggetti necessari per migrare in modo efficiente i dati: tabelle, chiavi primarie e, in alcuni casi, indici univoci. AWS DMS non crea indici secondari, vincoli di chiave non primari o valori predefiniti per i dati delle colonne. Se stai eseguendo un'attività di caricamento completo più CDC o solo CDC, è consigliabile sospendere la migrazione a questo punto. Quindi, creare indici secondari che</p>

Per questa opzione	Eseguire questa operazione
	<p>supportano il filtro per le istruzioni di aggiornamento ed eliminazione.</p> <p>Potrebbe essere necessario eseguire alcune operazioni di configurazione sul database di destinazione se utilizzi la modalità Drop tables on target (Elimina tabelle nella destinazione). Ad esempio, per un target Oracle, non è AWS DMS possibile creare uno schema (utente del database) per motivi di sicurezza. In questo caso, si precrea l'utente dello schema in modo da AWS DMS poter creare le tabelle all'inizio della migrazione. Per la maggior parte degli altri tipi di destinazione, AWS DMS crea lo schema e tutte le tabelle associate con i parametri di configurazione appropriati.</p> <p>Tronca: in modalità Truncate, AWS DMS tronca tutte le tabelle di destinazione prima dell'inizio della migrazione. Se la tabella di destinazione non esiste, DMS la crea automaticamente. La struttura delle tabelle rimane invariata, ma le tabelle vengono troncate nella destinazione. La modalità Truncate (Tronca) è l'ideale per le migrazioni di caricamento completo o di caricamento completo più CDC in cui lo schema di destinazione è stato creato anticipatamente prima che la migrazione venga avviata. Per creare anticipatamente le tabelle, puoi utilizzare AWS SCT. Per ulteriori informazioni, vedere Installazione. AWS SCT</p> <div data-bbox="727 1591 1510 1818"><p> Note</p><p>Se la destinazione è MongoDB, la modalità Tronca non tronca le tabelle nella destinazione. Elimina invece la raccolta e perde tutti</p></div>

Per questa opzione	Eeguire questa operazione
	<p>gli indici. Evita la modalità Tronca quando la destinazione è MongoDB.</p>
<p>Stop task after full load completes (Interrompi l'attività al termine del caricamento completo)</p>	<p>Questa impostazione è visibile solo se scegli Migrazione dei dati esistenti e replica delle modifiche in corso per Tipo di migrazione nella sezione precedente.</p> <p>Non interrompere: non interrompe l'attività, bensì applica immediatamente le modifiche memorizzate nella cache e continua.</p> <p>Interrompi prima di applicare le modifiche memorizzate nella cache: interrompe l'attività prima dell'applicazione delle modifiche memorizzate nella cache. Con questo approccio puoi aggiungere indici secondari che potrebbero accelerare l'applicazione delle modifiche.</p> <p>Interrompi dopo l'applicazione delle modifiche memorizzate nella cache: interrompe l'attività dopo l'applicazione delle modifiche memorizzate nella cache. Con questo approccio puoi aggiungere le chiavi esterne se stai utilizzando l'applicazione transazionale.</p>

Per questa opzione	Eseguire questa operazione
Include LOB columns in replication (Includi le colonne LOB nella replica)	<p>Non includere le colonne LOB: le colonne LOB vengono escluse dalla migrazione.</p> <p>Modalità LOB completa: migra LOB completi indipendentemente dalle dimensioni. AWS DMS migra i LOB a tratti in blocchi controllati dal parametro LOB Chunk size. Questa modalità è più lenta rispetto alla modalità LOB limitata.</p> <p>Modalità LOB limitata: tronca i LOB in base al valore del parametro Dimensione massima dei LOB. Questa modalità è più veloce rispetto alla modalità LOB completa.</p>
Dimensione massima dei LOB (KB)	In Modalità LOB limitata, le colonne LOB che superano l'impostazione Dimensione LOB massima vengono troncate in base al valore specificato in Dimensione LOB massima.
Enable validation (Abilita convalida)	Abilita la convalida dei dati per verificare che i dati vengano migrati in modo accurato dall'origine alla destinazione. Per ulteriori informazioni, consulta Convalida dei dati in AWS DMS .
CloudWatch Abilita i log	Abilita la registrazione da parte di Amazon CloudWatch.

- Nella sezione Valutazione di pre-migrazione scegli se eseguire una valutazione di pre-migrazione. Una valutazione di pre-migrazione ti avvisa dei potenziali problemi di migrazione prima di iniziare l'attività di migrazione del database. Per ulteriori informazioni, consulta [Abilitazione e utilizzo delle valutazioni preliminari alla migrazione](#).
- Nella sezione Configurazione di avvio dell'attività di migrazione specifica se avviare l'attività automaticamente dopo la creazione.
- Nella sezione Tag specifica i tag necessari per organizzare l'attività. I tag possono essere utilizzati per gestire le policy e i ruoli IAM e tenere traccia dei costi di DMS. Per ulteriori informazioni, consulta [Assegnazione di tag alle risorse](#).

8. Dopo aver completato le impostazioni delle attività, scegli **Create task** (Crea attività).

Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service

Ogni attività dispone di impostazioni che puoi configurare in base alle esigenze della migrazione del database. Puoi creare queste impostazioni in un file JSON oppure, con alcune impostazioni, puoi specificare le impostazioni utilizzando la AWS DMS console. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Di seguito sono elencati i diversi principali tipi di impostazioni delle attività.

Argomenti

- [Esempio di impostazioni delle attività](#)
- [Impostazioni delle attività dei metadati di destinazione](#)
- [Impostazioni delle attività di caricamento completo](#)
- [Impostazioni delle attività Time Travel](#)
- [Registrazione delle impostazioni delle attività](#)
- [Impostazioni delle attività delle tabelle di controllo](#)
- [Impostazioni delle attività di buffer del flusso](#)
- [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#)
- [Impostazioni delle attività di convalida dei dati](#)
- [Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche](#)
- [Impostazioni dell'attività di sostituzione dei caratteri](#)
- [Impostazioni dell'attività immagine precedente](#)
- [Impostazioni delle attività per la gestione degli errori](#)
- [Salvataggio delle impostazioni delle attività](#)

Impostazioni delle attività	Documentazione di riferimento
Creazione di un report di valutazione dell'attività	Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività

Impostazioni delle attività	Documentazione di riferimento
<p>Puoi creare un report di valutazione dell'attività che mostra i tipi di dati non supportati che potrebbero causare problemi durante la migrazione. Puoi eseguire questo report sull'attività prima di eseguire l'attività per individuare i potenziali problemi.</p>	
<p>Creazione di un'attività</p> <p>Quando crei un'attività, specifichi l'origine, la destinazione, l'istanza di replica e le eventuali impostazioni di migrazione.</p>	<p>Creazione di un'attività</p>
<p>Creazione di un'attività di replica continua</p> <p>Puoi configurare un'attività per fornire la replica continua tra l'origine e la destinazione.</p>	<p>Creazione di attività per la replica continua mediante AWS DMS</p>
<p>Applicazione delle impostazioni dell'attività</p> <p>Ogni attività dispone di impostazioni che puoi configurare in base alle esigenze della migrazione del database. Queste impostazioni vengono create in un file JSON oppure, con alcune impostazioni, è possibile specificare le impostazioni utilizzando la AWS DMS console.</p>	<p>Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service</p>

Impostazioni delle attività	Documentazione di riferimento
<p>Convalida dei dati</p> <p>Utilizza la convalida dei dati per AWS DMS confrontare i dati del data store di destinazione con i dati del data store di origine.</p>	<p>Convalida dei dati in AWS DMS</p>
<p>Modifica di un'attività</p> <p>Quando un'attività viene arrestata, puoi modificarne le impostazioni.</p>	<p>Modifica di un'attività</p>
<p>Ricaricamento delle tabelle durante un'attività</p> <p>Puoi ricaricare una tabella durante un'attività se si verifica un errore durante l'esecuzione.</p>	<p>Ricaricamento delle tabelle durante un'attività</p>
<p>Utilizzo della mappatura delle tabelle</p> <p>La mappatura delle tabelle utilizza diversi tipi di regole per specificare le impostazioni delle attività per l'origine dati, lo schema di origine, i dati e le eventuali trasformazioni che devono verificarsi durante l'attività.</p>	<p>Regole di selezione Operazioni e regole di selezione</p> <p>Regole di trasformazione Operazioni e regole di trasformazione</p>

Impostazioni delle attività	Documentazione di riferimento
<p>Applicazione di filtri</p> <p>Puoi utilizzare i filtri di origine per limitare il numero e il tipo di record trasferiti dall'origine alla destinazione. Ad esempio, puoi specificare che solo i dipendenti con un'ubicazione di sede vengano spostati al database di destinazione. I filtri vengono applicati su una colonna di dati.</p>	<p>Utilizzo di filtri di origine</p>
<p>Monitoraggio di un'attività</p> <p>Vi sono diversi modi per ottenere informazioni sulle prestazioni di un'attività e sulle tabelle utilizzate dall'attività.</p>	<p>Monitoraggio delle attività AWS DMS</p>
<p>Gestione dei log delle attività</p> <p>Puoi visualizzare ed eliminare i registri delle attività utilizzando l' AWS DMS API o. AWS CLI</p>	<p>Visualizzazione e gestione dei log delle attività AWS DMS</p>

Esempio di impostazioni delle attività

È possibile utilizzare il AWS Management Console o il AWS CLI per creare un'attività di replica. [Se si utilizza AWS CLI, si impostano le impostazioni dell'attività creando un file JSON, quindi specificando l'URI file://del file JSON come ReplicationTaskSettingsparametro dell'operazione Task.CreateReplication](#)

L'esempio seguente mostra come utilizzare to AWS CLI richiamare l'operazione:
CreateReplicationTask

```
aws dms create-replication-task \  
--replication-task-identifier MyTask \  

```

```
--source-endpoint-arn arn:aws:dms:us-  
west-2:123456789012:endpoint:ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890ABC \  
--target-endpoint-arn arn:aws:dms:us-  
west-2:123456789012:endpoint:ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890ABC \  
--replication-instance-arn arn:aws:dms:us-  
west-2:123456789012:rep:ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890ABC \  
--migration-type cdc \  
--table-mappings file://tablemappings.json \  
--replication-task-settings file://settings.json
```

L'esempio precedente utilizza un file di mappatura delle tabelle chiamato `tablemappings.json`. Per gli esempi di mappatura delle tabelle, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#).

Un file JSON delle impostazioni delle attività può apparire come segue:

```
{  
  "TargetMetadata": {  
    "TargetSchema": "",  
    "SupportLobs": true,  
    "FullLobMode": false,  
    "LobChunkSize": 64,  
    "LimitedSizeLobMode": true,  
    "LobMaxSize": 32,  
    "InlineLobMaxSize": 0,  
    "LoadMaxFileSize": 0,  
    "ParallelLoadThreads": 0,  
    "ParallelLoadBufferSize": 0,  
    "ParallelLoadQueuesPerThread": 1,  
    "ParallelApplyThreads": 0,  
    "ParallelApplyBufferSize": 100,  
    "ParallelApplyQueuesPerThread": 1,  
    "BatchApplyEnabled": false,  
    "TaskRecoveryTableEnabled": false  
  },  
  "FullLoadSettings": {  
    "TargetTablePrepMode": "DO_NOTHING",  
    "CreatePkAfterFullLoad": false,  
    "StopTaskCachedChangesApplied": false,  
    "StopTaskCachedChangesNotApplied": false,  
    "MaxFullLoadSubTasks": 8,  
  }  
}
```



```
"TransactionConsistencyTimeout": 600,
"CommitRate": 10000
},
"TTSettings" : {
"EnableTT" : true,
"TTS3Settings": {
"EncryptionMode": "SSE_KMS",
"ServerSideEncryptionKmsKeyId": "arn:aws:kms:us-west-2:112233445566:key/
myKMSKey",
"ServiceAccessRoleArn": "arn:aws:iam::112233445566:role/dms-tt-s3-access-role",
"BucketName": "myttbucket",
"BucketFolder": "myttfolder",
"EnableDeletingFromS3OnTaskDelete": false
},
"TTRecordSettings": {
"EnableRawData" : true,
"OperationsToLog": "DELETE,UPDATE",
"MaxRecordSize": 64
}
},
"Logging": {
"EnableLogging": false
},
"ControlTablesSettings": {
"ControlSchema": "",
"HistoryTimeslotInMinutes":5,
"HistoryTableEnabled": false,
"SuspendedTablesTableEnabled": false,
"StatusTableEnabled": false
},
"StreamBufferSettings": {
"StreamBufferCount": 3,
"StreamBufferSizeInMB": 8
},
"ChangeProcessingTuning": {
"BatchApplyPreserveTransaction": true,
"BatchApplyTimeoutMin": 1,
"BatchApplyTimeoutMax": 30,
"BatchApplyMemoryLimit": 500,
"BatchSplitSize": 0,
"MinTransactionSize": 1000,
"CommitTimeout": 1,
"MemoryLimitTotal": 1024,
"MemoryKeepTime": 60,
```

```
"StatementCacheSize": 50
},
"ChangeProcessingDdlHandlingPolicy": {
  "HandleSourceTableDropped": true,
  "HandleSourceTableTruncated": true,
  "HandleSourceTableAltered": true
},
"LoopbackPreventionSettings": {
  "EnableLoopbackPrevention": true,
  "SourceSchema": "LOOP-DATA",
  "TargetSchema": "loop-data"
},
"CharacterSetSettings": {
  "CharacterReplacements": [ {
    "SourceCharacterCodePoint": 35,
    "TargetCharacterCodePoint": 52
  }, {
    "SourceCharacterCodePoint": 37,
    "TargetCharacterCodePoint": 103
  }
],
"CharacterSetSupport": {
  "CharacterSet": "UTF16_PlatformEndian",
  "ReplaceWithCharacterCodePoint": 0
}
},
"BeforeImageSettings": {
  "EnableBeforeImage": false,
  "FieldName": "",
  "ColumnFilter": "pk-only"
},
"ErrorBehavior": {
  "DataErrorPolicy": "LOG_ERROR",
  "DataTruncationErrorPolicy": "LOG_ERROR",
  "DataErrorEscalationPolicy": "SUSPEND_TABLE",
  "DataErrorEscalationCount": 50,
  "TableErrorPolicy": "SUSPEND_TABLE",
  "TableErrorEscalationPolicy": "STOP_TASK",
  "TableErrorEscalationCount": 50,
  "RecoverableErrorCount": 0,
  "RecoverableErrorInterval": 5,
  "RecoverableErrorThrottling": true,
  "RecoverableErrorThrottlingMax": 1800,
```

```

    "ApplyErrorDeletePolicy": "IGNORE_RECORD",
    "ApplyErrorInsertPolicy": "LOG_ERROR",
    "ApplyErrorUpdatePolicy": "LOG_ERROR",
    "ApplyErrorEscalationPolicy": "LOG_ERROR",
    "ApplyErrorEscalationCount": 0,
    "FullLoadIgnoreConflicts": true
  },
  "ValidationSettings": {
    "EnableValidation": false,
    "ValidationMode": "ROW_LEVEL",
    "ThreadCount": 5,
    "PartitionSize": 10000,
    "FailureMaxCount": 1000,
    "RecordFailureDelayInMinutes": 5,
    "RecordSuspendDelayInMinutes": 30,
    "MaxKeyColumnSize": 8096,
    "TableFailureMaxCount": 10000,
    "ValidationOnly": false,
    "HandleCollationDiff": false,
    "RecordFailureDelayLimitInMinutes": 1,
    "SkipLobColumns": false,
    "ValidationPartialLobSize": 0,
    "ValidationQueryCdcDelaySeconds": 0
  }
}

```

Impostazioni delle attività dei metadati di destinazione

Di seguito sono descritte le impostazioni dei metadati di destinazione. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

- **TargetSchema:** il nome dello schema della tabella di destinazione. Se questa opzione di metadati è vuota, viene utilizzato lo schema della tabella di origine. Se non è definito alcuno schema di origine, AWS DMS aggiunge automaticamente il prefisso del proprietario per il database di destinazione a tutte le tabelle. Questa opzione deve essere lasciata vuota per endpoint di destinazione di tipo MySQL. La ridenominazione di uno schema nella mappatura dei dati ha la precedenza su questa impostazione.

- **Impostazioni LOB:** impostazioni che determinano il modo in cui vengono gestiti gli oggetti di grandi dimensioni (LOB). Impostando `SupportLobs=true`, è necessario impostare su `true` una delle seguenti opzioni:
 - **FullLobMode:** se si imposta questa opzione su `true`, è necessario specificare un valore per l'opzione `LobChunkSize`. Inserisci le dimensioni, in kilobyte, dei chunk LOB da utilizzare durante la replica dei dati sulla destinazione. L'opzione `FullLobMode` è ideale per LOB di dimensioni molto grandi, ma tende a rallentare le operazioni di caricamento. Il valore consigliato per `LobChunkSize` è 64 kilobyte. L'aumento del valore di `LobChunkSize` su valori superiori a 64 kilobyte può causare errori nelle attività.
 - **InlineLobMaxSize**— Questo valore determina quali LOB vengono AWS DMS trasferiti in linea durante un carico completo. Il trasferimento di LOB di piccole dimensioni è un'operazione più efficiente rispetto alla ricerca di tali LOB da una tabella di origine. Durante un carico completo, AWS DMS controlla tutti i LOB ed esegue un trasferimento in linea per i LOB inferiori a `InlineLobMaxSize`. AWS DMS trasferisce tutti i LOB più grandi di quelli in `InlineLobMaxSize`. Il valore predefinito per `InlineLobMaxSize` è 0 e l'intervallo è compreso tra 1 e 102400 kilobyte (100 MB). Imposta un valore per `InlineLobMaxSize` solo se sai che la maggior parte dei LOB ha dimensioni inferiori al valore specificato in `InlineLobMaxSize`.
 - **LimitedSizeLobMode:** se si imposta questa opzione su `true`, è necessario specificare un valore per l'opzione `LobMaxSize`. Inserisci le dimensioni massime, in kilobyte, per un singolo LOB. Il valore massimo consigliato per `LobMaxSize` è 102400 kilobyte (100 MB).

Per ulteriori informazioni sui criteri per l'utilizzo di queste impostazioni dei LOB per le attività, consulta [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#). È inoltre possibile controllare la gestione dei LOB per le singole tabelle. Per ulteriori informazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

- **LoadMaxFileSize:** un'opzione per gli endpoint di destinazione basati su CSV come MySQL, PostgreSQL e Amazon Redshift che supportano l'uso di file con valori separati da virgole (.csv) per il caricamento dei dati. `LoadMaxFileSizedefinisce` la dimensione massima su disco dei dati archiviati e scaricati, come i file.csv. Questa opzione sostituisce l'attributo di connessione dell'endpoint di destinazione `maxFileSize`. Puoi fornire valori da 0, che indica che questa opzione non ignora l'attributo di connessione, fino a 100.000 KB.
- **BatchApplyEnabled:** determina se ogni transazione viene applicata singolarmente o se le modifiche sono sottoposte a commit in batch. Il valore predefinito è `false`.

Quando `BatchApplyEnabled` è impostato su `true`, DMS richiede una chiave primaria (PK) o una chiave unica (UK) nelle tabelle di origine. Senza PK o UK nelle tabelle di origine, vengono applicati solo gli inserimenti in batch, ma non gli aggiornamenti e le eliminazioni in batch.

Quando `BatchApplyEnabled` è impostato su `true`, AWS DMS genera un messaggio di errore se una tabella di destinazione ha un vincolo univoco e una chiave primaria. Le tabelle di destinazione con un vincolo univoco e una chiave primaria non sono supportate quando `BatchApplyEnabled` è impostato su `true`.

Quando `BatchApplyEnabled` è impostato su `true` e AWS DMS rileva un errore nei dati da una tabella con la politica di gestione degli errori predefinita, l'AWS DMS operazione passa dalla modalità batch alla one-by-one modalità per il resto delle tabelle. Per modificare questo comportamento, è possibile impostare l'azione "SUSPEND_TABLE" nelle seguenti policy nella proprietà di gruppo "ErrorBehavior" del file JSON delle impostazioni delle attività:

- `DataErrorPolicy`
- `ApplyErrorDeletePolicy`
- `ApplyErrorInsertPolicy`
- `ApplyErrorUpdatePolicy`

Per ulteriori informazioni sulla proprietà di gruppo "ErrorBehavior", vedi l'esempio di file JSON delle impostazioni delle attività in [Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service](#). Dopo aver impostato questi criteri su "SUSPEND_TABLE", l'AWS DMS attività sospende quindi gli errori nei dati su tutte le tabelle che li generano e continua in modalità batch per tutte le tabelle.

Puoi utilizzare il parametro `BatchApplyEnabled` con il parametro `BatchApplyPreserveTransaction`. Se `BatchApplyEnabled` è impostato su `true`, il parametro `BatchApplyPreserveTransaction` determina l'integrità transazionale.

Se `BatchApplyPreserveTransaction` è impostata su `true`, l'integrità transazionale viene conservata ed è garantito che un batch contenga tutte le modifiche all'interno di una transazione dall'origine.

Se `BatchApplyPreserveTransaction` è impostato su `false`, per migliorare le prestazioni possono verificarsi vuoti temporanei nell'integrità transazionale.

Il parametro `BatchApplyPreserveTransaction` si applica solo a endpoint di destinazione Oracle ed è rilevante solo quando il parametro `BatchApplyEnabled` è impostato su `true`.

Quando le colonne LOB sono incluse nella replica, è possibile usare `BatchApplyEnabled` solo in modalità LOB limitata.

Per ulteriori informazioni sull'utilizzo di queste impostazioni per l'acquisizione dei dati di modifica (CDC), consulta [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).

- `MaxFullLoadSubTasks`: indica il numero massimo di tabelle da caricare in parallelo. Il valore predefinito è 8; il valore massimo è 49.
- `ParallelLoadThreads`— specifica il numero di thread AWS DMS utilizzati per caricare ogni tabella nel database di destinazione. Questo parametro prevede valori massimi per le destinazioni non RDBMS. Il valore massimo per una destinazione DynamoDB è 200. Il valore massimo per un target Amazon Kinesis Data Streams, Apache Kafka o OpenSearch Amazon Service è 32. Puoi chiedere di aumentare questo limite massimo. `ParallelLoadThreads` si applica alle attività di pieno carico. Per ulteriori informazioni sulle impostazioni che consentono il caricamento in parallelo di singole tabelle, consultare [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Questa impostazione si applica ai seguenti tipi di motori di endpoint:

- DynamoDB
- Flusso di dati Amazon Kinesis
- MSK Amazon
- OpenSearch Servizio Amazon
- Amazon Redshift

AWS DMS supporta `ParallelLoadThreads` MySQL come attributo di connessione aggiuntivo. `ParallelLoadThreads` non si applica a MySQL come impostazione delle attività.

- `ParallelLoadBufferSize` : specifica il numero massimo di record da archiviare nel buffer utilizzato dai thread di caricamento parallelo per caricare i dati nella destinazione. Il valore predefinito è 50. Il valore massimo è 1.000. Questa impostazione è attualmente valida solo quando DynamoDB, Kinesis, Apache Kafka o è la destinazione. OpenSearch Utilizzare questo parametro con `ParallelLoadThreads`; `ParallelLoadBufferSize` è valido solo quando è presente più di un thread. Per ulteriori informazioni sulle impostazioni che consentono il caricamento in parallelo di singole tabelle, consultare [Regole e operazioni delle impostazioni di tabella e raccolta](#).

- `ParallelLoadQueuesPerThread`: specifica il numero di code a cui ogni thread simultaneo accede per estrarre i record di dati dalle code e generare un caricamento batch per una destinazione. Il valore di default è 1. Questa impostazione è attualmente valida solo quando la destinazione è Kinesis o Apache Kafka.
- `ParallelApplyThreads`: specifica il numero di thread simultanei da AWS DMS utilizzare durante un caricamento CDC per inviare i record di dati a un endpoint di destinazione Amazon DocumentDB, Kinesis, Amazon MSK o Amazon Redshift. OpenSearch Il valore predefinito è zero (0).

Questa impostazione si applica solo ai CDC. Questa impostazione non è valida per il pieno carico.

Questa impostazione si applica ai seguenti tipi di motori di endpoint:

- Amazon DocumentDB (compatibile con MongoDB)
- Flusso di dati Amazon Kinesis
- Amazon Managed Streaming per Apache Kafka
- OpenSearch Servizio Amazon
- Amazon Redshift
- `ParallelApplyBufferSize`: specifica il numero massimo di record da archiviare in ogni coda di buffer per i thread simultanei da inviare a un endpoint di destinazione Amazon DocumentDB, Kinesis, Amazon MSK o Amazon Redshift durante un OpenSearch caricamento CDC. Il valore predefinito è 100. Il valore massimo è 1000. Utilizzare questa opzione quando `ParallelApplyThreads` specifica più di un thread.
- `ParallelApplyQueuesPerThread`: specifica il numero di code a cui ogni thread accede per estrarre i record di dati dalle code e generare un caricamento in batch per Amazon DocumentDB, Kinesis, Amazon MSK o endpoint durante il CDC. OpenSearch Il valore predefinito è 1.

Impostazioni delle attività di caricamento completo

Di seguito sono descritte le impostazioni di pieno carico. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

- Per indicare come gestire il caricamento della destinazione all'avvio del caricamento completo, specifica uno dei seguenti valori per l'opzione `TargetTablePrepMode`:
 - `DO_NOTHING`: i dati e i metadati della tabella di destinazione esistente rimangono invariati.

- **DROP_AND_CREATE**: la tabella esistente viene eliminata e, al suo posto, viene creata una nuova tabella.
- **TRUNCATE_BEFORE_LOAD**: i dati vengono troncati senza modificare i metadati della tabella.
- Per ritardare la creazione della chiave primaria o dell'indice univoco finché non viene completato il pieno carico, imposta l'opzione `CreatePkAfterFullLoad` su `true`.
- Per attività di caricamento completo e abilitate per CDC, puoi impostare le seguenti opzioni per `Stop task after full load completes`:
 - `StopTaskCachedChangesApplied`: imposta questa opzione su `true` per interrompere un'attività dopo il completamento di un pieno carico e l'applicazione delle modifiche memorizzate nella cache.
 - `StopTaskCachedChangesNotApplied`: imposta questa opzione su `true` per arrestare un'attività prima che le modifiche memorizzate nella cache vengano applicate.
- Imposta l'opzione `MaxFullLoadSubTasks` per indicare il numero massimo di tabelle da caricare in parallelo. Il valore predefinito è 8; il valore il massimo è 49.
- Imposta l'opzione `ParallelLoadThreads` per indicare quanti thread simultanei vengono utilizzati da DMS durante un processo di pieno carico per eseguire il push dei record di dati a un endpoint di destinazione. Il valore predefinito è zero (0).

Important

`MaxFullLoadSubTasks` controlla il numero di tabelle o segmenti di tabella da caricare in parallelo. `ParallelLoadThreads` controlla il numero di thread utilizzati da un'attività di migrazione per eseguire i carichi in parallelo. Queste impostazioni sono moltiplicative. Pertanto, il numero totale di thread utilizzati durante un'operazione di pieno carico è approssimativamente il risultato del valore di `ParallelLoadThreads` moltiplicato per il valore di `MaxFullLoadSubTasks` (`ParallelLoadThreads * MaxFullLoadSubtasks`).

Se si creano attività con un numero elevato di attività secondarie di pieno carico e un numero elevato di thread di caricamento parallelo, l'attività può consumare troppa memoria e non riuscire.

- È possibile impostare il numero di secondi di AWS DMS attesa per la chiusura delle transazioni prima di iniziare un'operazione a pieno carico. A tale scopo, se le transazioni sono aperte all'avvio dell'attività, imposta l'opzione `TransactionConsistencyTimeout`. Il valore predefinito è 600 (10 minuti). AWS DMS avvia il caricamento completo dopo il raggiungimento del valore di timeout,

anche se ci sono transazioni aperte. Un' full-load-only attività non aspetta 10 minuti ma inizia immediatamente.

- Per indicare il numero massimo di record che possono essere trasferiti contemporaneamente, imposta l'opzione `CommitRate`. Il valore predefinito è 10000 e il valore massimo è 50000.

Impostazioni delle attività Time Travel

Per registrare ed eseguire il debug delle attività di replica, puoi utilizzare AWS DMS Time Travel. Con questo approccio usi Amazon S3 per archiviare e crittografare i log con le chiavi di crittografia. Solo con l'accesso al tuo bucket S3 Time Travel, puoi recuperare i log S3 utilizzando filtri data-ora, quindi visualizzare, scaricare e offuscare i log secondo le tue necessità. In questo modo, puoi andare in sicurezza indietro nel tempo per analizzare le attività del database. Time Travel funziona indipendentemente dalla CloudWatch registrazione. Per ulteriori informazioni sulla CloudWatch registrazione, vedere. [Registrazione delle impostazioni delle attività](#)

Puoi utilizzare Time Travel in tutte le AWS regioni con endpoint AWS DMS di origine Oracle, Microsoft SQL Server e PostgreSQL supportati e endpoint di destinazione PostgreSQL e MySQL supportati. AWS DMS è possibile attivare Time Travel solo per le attività di pieno carico e acquisizione dei dati di modifica (CDC) e per le attività di sola CDC. Per attivare Time Travel o modificare le impostazioni esistenti di Time Travel, assicurati che l'attività di replica sia arrestata.

Le impostazioni Time Travel includono le seguenti proprietà `TTSettings`:

- `EnableTT`: se questa opzione è impostata su `true`, la registrazione Time Travel è attivata per l'attività. Il valore predefinito è `false`.

Tipo: Booleano

Campo obbligatorio: no

- `EncryptionMode`: il tipo di crittografia lato server utilizzato nel bucket S3 per archiviare dati e log. Puoi specificare `"SSE_S3"` (valore predefinito) oppure `"SSE_KMS"`.

Puoi cambiare `EncryptionMode` da `"SSE_KMS"` a `"SSE_S3"`, ma non viceversa.

• Tipo: stringa

Campo obbligatorio: no

- `ServerSideEncryptionKmsKeyId`— Se specifichi `for`, fornisci l'ID per la tua chiave gestita personalizzata. `"SSE_KMS"` `EncryptionMode` AWS KMS Assicurati che alla chiave che utilizzi

sia associata una policy che attivi le autorizzazioni utente AWS Identity and Access Management (IAM) e consenta l'uso della chiave.

L'opzione "SSE_KMS" supporta solo la chiave KMS simmetrica gestita dal cliente.

▪Tipo: stringa

Obbligatorio: solo se imposti EncryptionMode su "SSE_KMS".

- **ServiceAccessRoleArn**: il nome della risorsa Amazon (ARN) utilizzato dal servizio per accedere al ruolo IAM. Imposta il nome del ruolo su `dms-tt-s3-access-role`. Questa è un'impostazione obbligatoria che consente di AWS DMS scrivere e leggere oggetti da un bucket S3.

▪Tipo: stringa

Obbligatorio: se Time Travel è attivo.

Di seguito è riportato un esempio di policy per questo ruolo.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "s3:ListBucket",
        "s3>DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::S3bucketName*",
        "arn:aws:kms:us-east-1:112233445566:key/1234a1a1-1m2m-1z2z-d1d2-12dmstt1234"
      ]
    }
  ]
}
```

Di seguito è riportato un esempio di policy di trust per questo ruolo.

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

- **BucketName**: il nome del bucket S3 per archiviare i log Time Travel. Assicurati di creare questo bucket S3 prima di attivare i log Time Travel.

▪Tipo: stringa

Obbligatorio: se Time Travel è attivo.

- **BucketFolder**: un parametro facoltativo per impostare un nome di cartella nel bucket S3. Se specifichi questo parametro, DMS crea i log Time Travel nel percorso `"/BucketName/BucketFolder/taskARN/YYYY/MM/DD/hh"`. Se non specifichi questo parametro, AWS DMS crea il percorso predefinito come `"/BucketName/dms-time-travel-logs/taskARN/YYYY/MM/DD/hh"`

▪Tipo: stringa

Campo obbligatorio: no

- **EnableDeletingFromS3OnTaskDelete**— Quando questa opzione è impostata su `true`, AWS DMS elimina i registri di Time Travel da S3 se l'attività viene eliminata. Il valore predefinito è `false`.

▪Tipo: stringa

Campo obbligatorio: no

- **EnableRawData**: quando questa opzione è impostata su `true`, i dati non elaborati DML (Data Manipulation Language) per i log Time Travel vengono visualizzati sotto la colonna `raw_data`

dei log Time Travel. Per informazioni dettagliate, consulta [Utilizzo dei log Time Travel](#). Il valore predefinito è `false`. Quando questa opzione è impostata su `false`, viene acquisito solo il tipo di DML.

▀Tipo: stringa

Campo obbligatorio: no

- **RawDataFormat**— Nelle AWS DMS versioni 3.5.0 e successive, quando `EnableRawData` è impostato su `true` Questa proprietà specifica un formato per i dati non elaborati DML in un log Time Travel e può essere presentato come:
 - "TEXT": nomi e valori di colonna analizzati e leggibili per gli eventi DML acquisiti durante la CDC come campi Raw.
 - "HEX": il codice esadecimale originale per i nomi e i valori di colonna acquisiti per gli eventi DML durante la CDC.

Questa proprietà si applica alle origini di database Oracle e Microsoft SQL Server.

▀Tipo: stringa

Campo obbligatorio: no

- **OperationsToLog**: specifica il tipo di operazioni DML per accedere ai log Time Travel. È possibile specificare una delle seguenti opzioni:
 - "INSERT"
 - "UPDATE"
 - "DELETE"
 - "COMMIT"
 - "ROLLBACK"
 - "ALL"

Il valore predefinito è "ALL".

▀Tipo: stringa

Campo obbligatorio: no

- **MaxRecordSize**: specifica la dimensione massima dei record dei log Time Travel registrati per ogni riga. Utilizza questa proprietà per controllare l'aumento delle dimensioni dei log Time Travel per le tabelle particolarmente utilizzate. Il valore predefinito è 64 KB.

Tipo: integer

Campo obbligatorio: no

Per ulteriori informazioni sull'attivazione e l'utilizzo dei log Time Travel, consulta i seguenti argomenti.

Argomenti

- [Attivazione dei log Time Travel per un'attività](#)
- [Utilizzo dei log Time Travel](#)
- [Con quale frequenza AWS DMS carica i registri di Time Travel su S3](#)

Attivazione dei log Time Travel per un'attività

È possibile attivare Time Travel per un' AWS DMS attività utilizzando le impostazioni dell'attività descritte in precedenza. Assicurati che l'attività di replica sia interrotta prima di attivare Time Travel.

Per attivare Time Travel, utilizzare il AWS CLI

1. Crea un file JSON di configurazione delle attività DMS e aggiungi una sezione TTSettings come indicato di seguito. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

```
.
.
.
  },
  "TTSettings" : {
    "EnableTT" : true,
    "TTS3Settings": {
      "EncryptionMode": "SSE_KMS",
      "ServerSideEncryptionKmsKeyId": "arn:aws:kms:us-west-2:112233445566:key/myKMSKey",
      "ServiceAccessRoleArn": "arn:aws:iam::112233445566:role/dms-tt-s3-access-role",
      "BucketName": "myttbucket",
      "BucketFolder": "myttfolder",
      "EnableDeletingFromS3OnTaskDelete": false
    },
    "TTRecordSettings": {
```

```

    "EnableRawData" : true,
    "OperationsToLog": "DELETE,UPDATE",
    "MaxRecordSize": 64
  },
  .
  .
  .

```

2. In un'azione dell'attività appropriata, specifica questo file JSON utilizzando l'opzione `--replication-task-settings`. Ad esempio, il frammento di codice della CLI che segue specifica questo file di impostazioni Time Travel come parte di `create-replication-task`.

```

aws dms create-replication-task
--target-endpoint-arn arn:aws:dms:us-
east-1:112233445566:endpoint:ELS507YTYV452CAZR2EYBNQGILFHQIFVPWFRQAY \
--source-endpoint-arn arn:aws:dms:us-
east-1:112233445566:endpoint:HNX2BWIIN5ZYFF7F6UFFZVWTDFFSMTN0V2FTXZA \
--replication-instance-arn arn:aws:dms:us-
east-1:112233445566:rep:ERLHG2UA52EEJJKFYNYWRPCG6T7EPUAB5AWBUJQ \
--migration-type full-load-and-cdc --table-mappings 'file:///FilePath/
mappings.json' \
--replication-task-settings 'file:///FilePath/task-settings-tt-enabled.json' \
--replication-task-identifier test-task
.
.
.

```

Qui, il nome di questo file di impostazioni Time Travel è `task-settings-tt-enabled.json`.

Allo stesso modo, è possibile specificare questo file come parte dell'azione `modify-replication-task`.

Nota la particolare gestione dei log Time Travel per le seguenti azioni dell'attività:

- `start-replication-task`: quando si esegue un'attività di replica, se un bucket S3 utilizzato per Time Travel non è accessibile, l'attività viene contrassegnata come `FAILED`.
- `stop-replication-task`— Quando l'attività si interrompe, invia AWS DMS immediatamente tutti i registri Time Travel attualmente disponibili per l'istanza di replica al bucket S3 utilizzato per Time Travel.

Durante l'esecuzione di un'attività di replica, è possibile modificare il valore `EncryptionMode` da `"SSE_KMS"` a `"SSE_S3"` ma non viceversa.

Se la dimensione dei log Time Travel per un'attività in corso supera 1 GB, DMS esegue il push dei log a S3 entro cinque minuti dal raggiungimento della dimensione. Dopo l'esecuzione di un'attività, se il bucket S3 o la chiave KMS diventano inaccessibili, DMS interrompe il push dei log a questo bucket. Se scopri che i log non vengono trasferiti nel bucket S3, controlla S3 e le autorizzazioni. AWS KMS Per maggiori dettagli sulla frequenza con cui DMS esegue il push dei log a S3, consulta [Con quale frequenza AWS DMS carica i registri di Time Travel su S3](#).

Per attivare Time Travel per un'attività esistente dalla console, utilizza l'opzione dell'editor JSON in Impostazioni delle attività per aggiungere una sezione `TTSettings`.

Utilizzo dei log Time Travel

I log Time Travel sono file CSV (Comma-Separated Value, valori separati da virgole) con i campi seguenti.

```
log_timestamp
component
dms_source_code_location
transaction_id
event_id
event_timestamp
lsn/scn
primary_key
record_type
event_type
schema_name
table_name
statement
action
result
raw_data
```

Dopo che i log Time Travel sono disponibili in S3, puoi accedervi direttamente ed eseguire query con strumenti come Amazon Athena. Oppure puoi scaricare i log come qualsiasi altro file da S3.

L'esempio seguente mostra un log Time Travel in cui vengono registrate le transazioni per una tabella chiamata `mytable`. I fine riga per il log seguente sono aggiunti per motivi di leggibilità.

```
"log_timestamp ", "tt_record_type", "dms_source_code_location ", "transaction_id",
```

```
"event_id", "event_timestamp", "scn_lsn", "primary_key", "record_type", "event_type",
"schema_name", "table_name", "statement", "action", "result", "raw_data"
"2021-09-23T01:03:00:778230", "SOURCE_CAPTURE", "postgres_endpoint_wal_engine.c:00819",
"609284109", "565612992", "2021-09-23 01:03:00.765321+00", "00000E9C/D53AB518", "", "DML",
"UPDATE (3)", "dmstest", "mytable", "", "Migrate", "", "table dmstest.mytable:
UPDATE: id[bigint]:2244937 phone_number[character varying]:'phone-number-482'
age[integer]:82 gender[character]:'f' isactive[character]:'true '
date_of_travel[timestamp without time zone]:'2021-09-23 01:03:00.76593'
description[text]:'TEST DATA TEST DATA TEST DATA TEST DATA'"
```

Con quale frequenza AWS DMS carica i registri di Time Travel su S3

Per ridurre al minimo l'utilizzo dello storage dell'istanza di replica, AWS DMS scarica periodicamente i log di Time Travel da essa.

I log Time Travel vengono sottoposti al push nel bucket Amazon S3 nei seguenti casi:

- Se la dimensione corrente dei log supera 1 GB, AWS DMS carica i log su S3 entro cinque minuti. Pertanto, AWS DMS può effettuare fino a 12 chiamate all'ora verso S3 e per ogni attività in esecuzione. AWS KMS
- AWS DMS carica i log su S3 ogni ora, indipendentemente dalla dimensione dei log.
- Quando un'attività viene interrotta, carica AWS DMS immediatamente i registri dei viaggi nel tempo su S3.

Registrazione delle impostazioni delle attività

La registrazione utilizza Amazon CloudWatch per registrare le informazioni durante il processo di migrazione. Utilizzando le impostazioni delle attività di registrazione, puoi specificare quali attività di componente vengono registrate e quale quantità di informazioni viene scritta nel log. Le impostazioni delle attività di registrazione vengono scritte in un file JSON. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Puoi attivare la CloudWatch registrazione in diversi modi. È possibile selezionare l'EnableLoggingopzione AWS Management Console quando si crea un'attività di migrazione. In alternativa, è possibile impostare l'EnableLoggingopzione su true quando si crea un'attività utilizzando l' AWS DMS API. Puoi inoltre specificare "EnableLogging": true nel JSON della sezione di registrazione delle impostazioni delle attività.

Quando lo `EnableLogging` imposti su `true`, AWS DMS assegna il nome del CloudWatch gruppo e il nome dello stream come segue. Non è possibile impostare questi valori direttamente.

- `CloudWatchLogGroup`: `dms-tasks-<REPLICATION_INSTANCE_IDENTIFIER>`
- `CloudWatchLogStream`: `dms-task-<REPLICATION_TASK_EXTERNAL_RESOURCE_ID>`

`<REPLICATION_INSTANCE_IDENTIFIER>` è l'identificativo dell'istanza di replica.

`<REPLICATION_TASK_EXTERNAL_RESOURCE_ID>` è il valore della sezione `<resourcename>` dell'ARN dell'attività. Per informazioni su come AWS DMS genera gli ARN delle risorse, consulta.

[Creazione di un Amazon Resource Name \(ARN\) per AWS DMS](#)

CloudWatch si integra con AWS Identity and Access Management (IAM) e puoi specificare quali CloudWatch azioni può eseguire un utente del tuo AWS account. Per ulteriori informazioni sull'utilizzo di IAM in CloudWatch, consulta [Gestione delle identità e degli accessi per Amazon CloudWatch](#) e [Registrazione delle chiamate CloudWatch API Amazon](#) nella Amazon CloudWatch User Guide.

Per eliminare i log delle attività, puoi impostare `DeleteTaskLogs` su `true` nel file JSON della sezione di registrazione delle impostazioni delle attività.

È possibile specificare la registrazione per i seguenti tipi di eventi:

- `FILE_FACTORY`: la file factory gestisce i file utilizzati per l'applicazione e il caricamento in batch e gli endpoint Amazon S3.
- `METADATA_MANAGER`: il gestore dei metadati gestisce i metadati di origine e di destinazione, il partizionamento e lo stato della tabella durante la replica.
- `SORTER`: `SORTER` riceve gli eventi in entrata dal processo `SOURCE_CAPTURE`. Gli eventi vengono raggruppati in transazioni e passati al componente di servizio `TARGET_APPLY`. Se il processo `SOURCE_CAPTURE` produce eventi più velocemente di quanto il componente `TARGET_APPLY` possa consumare, il componente `SORTER` memorizza gli eventi backlog nella cache su disco o in un file swap. Gli eventi memorizzati nella cache sono una causa comune di esaurimento dello storage nelle istanze di replica.

Il componente di servizio `SORTER` gestisce gli eventi memorizzati nella cache, raccoglie le statistiche CDC e riporta la latenza delle attività.

- `SOURCE_CAPTURE`: i dati di replica continua (CDC) vengono acquisiti dal database o dal servizio di origine e passati al componente di servizio `SORTER`.

- SOURCE_UNLOAD: i dati vengono scaricati dal database o dal servizio di origine durante il pieno carico.
- TABLES_MANAGER: il gestore delle tabelle tiene traccia delle tabelle acquisite, gestisce l'ordine di migrazione delle tabelle e raccoglie le statistiche delle tabelle.
- TARGET_APPLY: i dati e le istruzioni DDL (Data Definition Language) vengono applicati al database di destinazione.
- TARGET_LOAD: i dati vengono caricati nel database di destinazione.
- TASK_MANAGER: il gestore attività gestisce le attività in esecuzione e le suddivide in attività secondarie per l'elaborazione parallela dei dati.
- TRANSFORMATION: eventi di trasformazione basati sulla mappatura delle tabelle. Per ulteriori informazioni, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#).
- VALIDATOR/ VALIDATOR_EXT: il componente di servizio VALIDATOR verifica che i dati siano stati migrati con precisione dall'origine alla destinazione. Per ulteriori informazioni, consulta [Convalida dei dati](#).

I seguenti componenti di registrazione generano una grande quantità di log quando si utilizza il livello di gravità del log `LOGGER_SEVERITY_DETAILED_DEBUG`:

- COMMON
- ADDONS
- DATA_STRUCTURE
- COMMUNICATION
- FILE_TRANSFER
- FILE_FACTORY

Livelli di registrazione diversi da `DEFAULT` sono raramente necessari per questi componenti durante la risoluzione dei problemi. Si sconsiglia di modificare il livello di registrazione `DEFAULT` per questi componenti a meno che non sia specificamente richiesto da AWS Support.

Dopo aver specificato una delle opzioni precedenti, è possibile specificare la quantità di informazioni registrate, come illustrato nel seguente elenco.

I livelli di gravità sono in ordine dal più basso al più alto livello di informazioni. I livelli più elevati includono sempre informazioni dai livelli inferiori.

- `LOGGER_SEVERITY_ERROR`: i messaggi di errore vengono scritti nel log.
- `LOGGER_SEVERITY_WARNING`: gli avvisi e i messaggi di errore vengono scritti nel log.
- `LOGGER_SEVERITY_INFO`: i messaggi informativi, gli avvisi e i messaggi di errore vengono scritti nel log.
- `LOGGER_SEVERITY_DEFAULT`: i messaggi informativi, gli avvisi e i messaggi di errore vengono scritti nel log.
- `LOGGER_SEVERITY_DEBUG`: i messaggi di debug, i messaggi informativi, gli avvisi e i messaggi di errore vengono scritti nel log.
- `LOGGER_SEVERITY_DETAILED_DEBUG`: tutte le informazioni vengono scritte nel log.

Nell'esempio JSON seguente vengono illustrate le impostazioni delle attività per la registrazione di tutte le operazioni e i livelli di gravità.

```
...
  "Logging": {
    "EnableLogging": true,
    "LogComponents": [
      {
        "Id": "FILE_FACTORY",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "METADATA_MANAGER",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "SORTER",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "SOURCE_CAPTURE",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "SOURCE_UNLOAD",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "TABLES_MANAGER",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "TARGET_APPLY",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      }, {
        "Id": "TARGET_LOAD",
```

```
    "Severity": "LOGGER_SEVERITY_INFO"
  },{
    "Id": "TASK_MANAGER",
    "Severity": "LOGGER_SEVERITY_DEBUG"
  },{
    "Id": "TRANSFORMATION",
    "Severity": "LOGGER_SEVERITY_DEBUG"
  },{
    "Id": "VALIDATOR",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  }
],
"CloudWatchLogGroup": null,
"CloudWatchLogStream": null
},
...
```

Impostazioni delle attività delle tabelle di controllo

Le tabelle di controllo forniscono informazioni su un' AWS DMS attività. Inoltre, forniscono statistiche utili che puoi utilizzare per pianificare e gestire sia l'attività di migrazione corrente che le attività future. È possibile applicare queste impostazioni delle attività in un file JSON o scegliendo Impostazioni avanzate nella pagina Crea attività della AWS DMS console. Viene sempre creata la tabella `Applica eccezioni (dmslogs.aws_dms_apply_exceptions)` nelle destinazioni del database. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

AWS DMS crea tabelle di controllo solo durante le attività Full Load + CDC o solo CDC e non durante le attività Full Load Only.

Per le attività di pieno carico e CDC (migrazione dei dati esistenti e replica delle modifiche in corso) e sola CDC (solo replica delle modifiche ai dati), puoi anche creare tabelle aggiuntive, tra cui le seguenti:

- Stato della replica (`dmslogs.aws_dms_status`): questa tabella fornisce i dettagli sull'attività corrente. Tali dettagli includono lo stato dell'attività, la quantità di memoria utilizzata dall'attività e il numero di modifiche non ancora applicate alla destinazione. Questa tabella indica anche la posizione nel database di origine in cui AWS DMS è attualmente in lettura. Inoltre, indica se l'attività è pieno carico o acquisizione dei dati di modifica (CDC).
- Tabelle sospese (`dmslogs.aws_dms_suspended_tables`): Questa tabella fornisce un elenco delle tabelle sospese, nonché il motivo per il quale sono state sospese.

- Cronologia della replica (dmslogs.aws_dms_history): questa tabella fornisce informazioni sulla cronologia delle repliche. Queste informazioni includono il numero e il volume di record elaborati durante l'attività, la latenza al termine di un'attività CDC e altre statistiche.

La tabella Apply Exceptions (dmslogs.aws_dms_apply_exceptions) contiene i parametri seguenti.

Colonna	Type	Descrizione
TASK_NAME	nvarchar	L'ID della risorsa dell' AWS DMS attività. L'ID risorsa è disponibile nell'ARN dell'attività.
TABLE_OWNER	nvarchar	Il proprietario della tabella.
TABLE_NAME	nvarchar	Il nome della tabella.
ERROR_TIME	timestamp	L'ora in cui si è verificata l'eccezione (errore).
STATEMENT	nvarchar	L'istruzione che era in esecuzione quando si è verificato l'errore.
ERRORE	nvarchar	Il nome e la descrizione dell'errore.

La tabella Replication Status (Stato replica) (dmslogs.aws_dms_status) contiene lo stato corrente dell'attività e il database di destinazione. Dispone delle seguenti impostazioni.

Colonna	Type	Descrizione
SERVER_NAME	nvarchar	Il nome del computer in cui l'attività di replica è in esecuzione.
TASK_NAME	nvarchar	L'ID della risorsa dell' AWS DMS attività. L'ID risorsa è disponibile nell'ARN dell'attività.
TASK_STATUS	varchar	Uno dei seguenti valori:

Colonna	Type	Descrizione
		<ul style="list-style-type: none"> • FULL LOAD • CHANGE PROCESSING (CDC) • NON IN ESECUZIONE <p>Lo stato dell'attività è impostato su FULL LOAD purché vi sia almeno una tabella in caricamento completo. Dopo che tutte le tabelle sono state caricate, lo stato dell'attività viene modificato in CHANGE PROCESSING se CDC è abilitato. L'attività è impostata su NON IN ESECUZIONE prima di avviarla o dopo il completamento dell'attività.</p>
STATUS_TIME	timestamp	Il timestamp dello stato dell'attività.
PENDING_CHANGES	int	Il numero di record di modifiche che sono stati confermati nel database di origine e memorizzati nella memoria cache e nel disco dell'istanza di replica.
DISK_SWAP_SIZE	int	La quantità di spazio su disco utilizzata da transazioni precedenti o di cui è stato eseguito l'offload.
TASK_MEMORY	int	Memoria attualmente utilizzata, in MB.
SOURCE_CURRENT_POSITION	varchar	La posizione nel database di origine da cui AWS DMS è attualmente in corso la lettura.

Colonna	Type	Descrizione
SOURCE_CURRENT_TIMESTAMP	timestamp	Il timestamp nel database di origine da cui AWS DMS è attualmente in corso la lettura.
SOURCE_TAIL_POSITION	varchar	La posizione della transazione di inizio meno recente di cui non è stato eseguito il commit. Questo valore è la posizione più recente da cui puoi eseguire il ripristino senza perdere alcuna modifica.
SOURCE_TAIL_TIMESTAMP	timestamp	Il timestamp della transazione di inizio meno recente di cui non è stato eseguito il commit. Questo valore è il timestamp più recente da cui puoi eseguire il ripristino senza perdere alcuna modifica.
SOURCE_TIMESTAMP_APPLIED	timestamp	Il timestamp per il commit dell'ultima transazione. In un processo di applicazione in blocco, questo valore è il timestamp per il commit dell'ultima transazione nel batch.

La tabella sospesa (`dmslogs.aws_dms_suspended_tables`) contiene i seguenti parametri.

Colonna	Type	Descrizione
SERVER_NAME	nvarchar	Il nome del computer in cui l'attività di replica è in esecuzione.
TASK_NAME	nvarchar	Il nome dell'attività AWS DMS
TABLE_OWNER	nvarchar	Il proprietario della tabella.

Colonna	Type	Descrizione
TABLE_NAME	nvarchar	Il nome della tabella.
SUSPEND_REASON	nvarchar	Motivo della sospensione.
SUSPEND_TIMESTAMP	timestamp	L'ora della sospensione.

La tabella Replication History (Cronologia repliche) (`dmslogs.aws_dms_history`) contiene i parametri seguenti.

Colonna	Type	Descrizione
SERVER_NAME	nvarchar	Il nome del computer in cui l'attività di replica è in esecuzione.
TASK_NAME	nvarchar	L'ID della risorsa dell' AWS DMS attività. L'ID risorsa è disponibile nell'ARN dell'attività.
TIMESLOT_TYPE	varchar	Uno dei seguenti valori: <ul style="list-style-type: none"> • FULL LOAD • CHANGE PROCESSING (CDC) <p>Se l'attività in esecuzione è sia di caricamento completo che CDC, nell'intervallo temporale vengono scritti due record di cronologia.</p>
TIMESLOT	timestamp	Il timestamp finale dell'intervallo temporale.
TIMESLOT_DURATION	int	La durata dell'intervallo temporale, in minuti.

Colonna	Type	Descrizione
TIMESLOT_LATENCY	int	La latenza di destinazione al termine dell'intervallo temporale, in secondi. Questo valore si applica solo agli intervalli temporali CDC.
RECORDS	int	Il numero di record elaborati durante l'intervallo temporale.
TIMESLOT_VOLUME	int	Il volume e i dati elaborati in MB.

La tabella Errore di convalida (`awsdms_validation_failures_v1`) contiene tutti gli errori di convalida dei dati per un'attività. Per ulteriori informazioni, consulta [Risoluzione dei problemi relativi alla convalida dei dati](#).

Le impostazioni delle tabelle di controllo aggiuntive includono le seguenti:

- `HistoryTimeslotInMinutes`: utilizza questa opzione per indicare la lunghezza di ogni intervallo temporale nella tabella Cronologia repliche. Il valore predefinito è 5 minuti.
- `ControlSchema`— Utilizzare questa opzione per indicare il nome dello schema del database per le tabelle di controllo della AWS DMS destinazione. Se non immetti alcuna informazione per questa opzione, le tabelle vengono copiate nella posizione predefinita del database, come indicato di seguito:
 - PostgreSQL, Pubblico
 - Oracle, lo schema di destinazione
 - Microsoft SQL Server, dbo nel database di destinazione
 - MySQL, `awsdms_control`
 - MariaDB, `awsdms_control`
 - Amazon Redshift, pubblico
 - DynamoDB, creato come singole tabelle nel database
 - IBM Db2 LUW, `awsdms_control`

Impostazioni delle attività di buffer del flusso

È possibile configurare le impostazioni dello stream buffer utilizzando AWS CLI, incluso quanto segue. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

- `StreamBufferCount`: utilizza questa opzione per specificare il numero di buffer del flusso di dati per l'attività di migrazione. Il numero di buffer del flusso predefinito è 3. Se si aumenta il valore di questa impostazione, la velocità di estrazione dei dati potrebbe aumentare. Tuttavia, queste prestazioni dipendono notevolmente dall'ambiente di migrazione, incluso il sistema di origine e la classe dell'istanza del server di replica. Il valore predefinito è sufficiente per la maggior parte dei casi.
- `StreamBufferSizeInMB`: utilizza questa opzione per indicare le dimensioni massime di ogni buffer del flusso di dati. Le dimensioni predefinite sono di 8 MB. Potresti dover aumentare il valore per questa opzione se utilizzi LOB di dimensioni molto grandi. Potresti inoltre dover aumentare il valore se ricevi un messaggio nei file di log in cui viene indicato che le dimensioni di buffer del flusso sono insufficienti. Per il calcolo delle dimensioni di questa opzione, puoi utilizzare la seguente equazione: $[\text{Max LOB size (or LOB chunk size)}] * [\text{number of LOB columns}] * [\text{number of stream buffers}] * [\text{number of tables loading in parallel per task(MaxFullLoadSubTasks)}] * 3$
- `CtrlStreamBufferSizeInMB`: utilizza questa opzione per impostare le dimensioni massime di buffer del flusso di controllo. Il valore è in megabyte e può essere compreso tra 1 e 8. Il valore predefinito è 5. Potresti dover aumentare questo valore se utilizzi un numero molto elevato di tabelle, ad esempio decine di migliaia di tabelle.

Impostazioni di ottimizzazione dell'elaborazione delle modifiche

Le seguenti impostazioni determinano il modo in cui AWS DMS gestisce le modifiche per le tabelle di destinazione durante l'acquisizione dei dati delle modifiche (CDC). Molte di queste impostazioni dipendono dal valore del parametro di metadati di destinazione `BatchApplyEnabled`. Per ulteriori informazioni sul parametro `BatchApplyEnabled`, consulta [Impostazioni delle attività dei metadati di destinazione](#). Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Le impostazioni di ottimizzazione dell'elaborazione delle modifiche includono le seguenti:

Le impostazioni seguenti si applicano solo quando il parametro dei metadati di destinazione `BatchApplyEnabled` è impostato su `true`.

- **BatchApplyPreserveTransaction**: se è impostato su `true`, l'integrità transazionale viene conservata ed è garantito che un batch contenga tutte le modifiche all'interno di una transazione dall'origine. Il valore predefinito è `true`. Questa impostazione si applica solo agli endpoint di destinazione Oracle.

Se il parametro è impostato su `false`, per migliorare le prestazioni possono verificarsi vuoti temporanei nell'integrità transazionale. Non vi è alcuna garanzia che tutte le modifiche in una transazione dall'origine vengano applicate alla destinazione in un singolo batch.

Per impostazione predefinita, AWS DMS elabora le modifiche in modalità transazionale, che preserva l'integrità delle transazioni. Se puoi permetterti vuoti temporanei nell'integrità delle transazioni, puoi utilizzare in alternativa l'opzione di applicazione ottimizzata in batch. Questa opzione raggruppa in modo efficiente le transazioni e le applica in batch per garantire l'efficienza. L'utilizzo dell'opzione di applicazione ottimizzata in batch viola quasi sempre i vincoli di integrità referenziale. Pertanto, ti consigliamo di disattivare questi vincoli durante il processo di migrazione e di riattivarli nel processo di conversione.

- **BatchApplyTimeoutMin**— Imposta la quantità minima di tempo di AWS DMS attesa, in secondi, tra ogni applicazione di modifiche in batch. Il valore predefinito è 1.
- **BatchApplyTimeoutMax**— Imposta il tempo massimo, in secondi, di AWS DMS attesa tra ogni applicazione di modifiche in batch prima del timeout. Il valore predefinito è 30.
- **BatchApplyMemoryLimit**: imposta la quantità di memoria massima (in MB) da utilizzare per l'elaborazione in modalità di applicazione ottimizzata in batch. Il valore predefinito è 500.
- **BatchSplitSize**: imposta il numero massimo di modifiche applicate in un singolo batch. Il valore predefinito è 0 e indica che non viene applicato alcun limite.

Le impostazioni seguenti si applicano solo quando il parametro dei metadati di destinazione `BatchApplyEnabled` è impostato su `false`.

- **MinTransactionSize**: imposta il numero minimo di modifiche da includere in ciascuna transazione. Il valore predefinito è 1000.
- **CommitTimeout**— Imposta il tempo massimo in secondi AWS DMS per la raccolta delle transazioni in batch prima di dichiarare un timeout. Il valore predefinito è 1.

Per la replica bidirezionale, l'impostazione seguente si applica solo quando il parametro dei metadati di destinazione `BatchApplyEnabled` è impostato su `false`.

- **LoopbackPreventionSettings**: queste impostazioni forniscono la prevenzione del loopback per ogni attività di replica in corso in qualsiasi coppia di attività coinvolte nella replica bidirezionale. La prevenzione del loopback impedisce l'applicazione di modifiche identiche in entrambe le direzioni della replica bidirezionale, che può danneggiare i dati. Per ulteriori informazioni sulla replica bidirezionale, consulta [Esecuzione della replica bidirezionale](#).

AWS DMS tenta di conservare i dati della transazione in memoria fino a quando la transazione non viene completamente confermata all'origine, alla destinazione o a entrambi. Tuttavia, le transazioni di dimensioni superiori a quelle della memoria allocata o di cui non viene eseguito il commit entro il limite di tempo specificato vengono scritte su disco.

Le impostazioni seguenti si applicano all'ottimizzazione dell'elaborazione delle modifiche indipendentemente dalla modalità di elaborazione delle modifiche.

- **MemoryLimitTotal**: imposta le dimensioni massime (in MB) che tutte le transazioni possono occupare in memoria prima di essere scritte su disco. Il valore predefinito è 1024.
- **MemoryKeepTime**: imposta il periodo di tempo massimo in secondi in cui ciascuna transazione può rimanere in memoria prima di essere scritta su disco. La durata viene calcolata a partire dal momento in cui è AWS DMS iniziata l'acquisizione della transazione. Il valore predefinito è 60.
- **StatementCacheSize**: imposta il numero massimo di istruzioni preparate da archiviare nel server per l'esecuzione successiva quando vengono applicate le modifiche sulla destinazione. Il valore predefinito è 50. Il valore massimo è 200.

Di seguito è riportato un esempio di come le impostazioni delle attività che gestiscono l'ottimizzazione dell'elaborazione delle modifiche vengono visualizzate in un file JSON di impostazione delle attività:

```
"ChangeProcessingTuning": {
  "BatchApplyPreserveTransaction": true,
  "BatchApplyTimeoutMin": 1,
  "BatchApplyTimeoutMax": 30,
  "BatchApplyMemoryLimit": 500,
  "BatchSplitSize": 0,
  "MinTransactionSize": 1000,
  "CommitTimeout": 1,
  "MemoryLimitTotal": 1024,
  "MemoryKeepTime": 60,
  "StatementCacheSize": 50
}
```

Per controllare la frequenza delle scritture su una destinazione Amazon S3 durante un'attività di replica dei dati, puoi configurare gli attributi aggiuntivi di connessione `cdcMaxBatchInterval` e `cdcMinFileSize`. In tal modo le prestazioni possono risultare migliori durante l'analisi dei dati senza ulteriori operazioni di sovraccarico. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#).

Impostazioni delle attività di convalida dei dati

Puoi assicurarti che i dati vengano migrati in modo accurato dall'origine alla destinazione. Se abiliti la convalida per un'attività, AWS DMS inizia a confrontare i dati di origine e di destinazione immediatamente dopo il caricamento completo di una tabella. Per ulteriori informazioni sulle attività di convalida dei dati, i requisiti, l'ambito del supporto dei database, nonché le metriche indicate, consulta [Convalida dei dati in AWS DMS](#). Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Le impostazioni di convalida dei dati e i relativi valori sono i seguenti:

- `EnableValidation`: abilita la convalida dei dati quando è impostato su `true`. In caso contrario, la convalida è disattivata per l'attività. Il valore predefinito è `false`.
- `ValidationMode`: controlla in che modo DMS convalida i dati nella tabella di destinazione rispetto alla tabella di origine. AWS DMS fornisce questa impostazione per l'estensibilità futura. Attualmente, l'unico valore predefinito e valido è `ROW_LEVEL`. AWS DMS convalida tutte le righe tra le tabelle di origine e di destinazione.
- `FailureMaxCount`: specifica il numero massimo di record per i quali la convalida non riesce prima che questa venga sospesa per l'attività. Il valore predefinito è 10,000. Se si desidera che la convalida continui indipendentemente dal numero di record per i quali la convalida non riesce, impostare un valore superiore al numero di record nell'origine.
- `HandleCollationDiff`: quando questa opzione è impostata su `true`, la convalida calcola le differenze di collazione per le colonne negli endpoint PostgreSQL e Microsoft SQL Server durante l'identificazione dei record di origine e di destinazione da confrontare. Altrimenti, per la convalida tali differenze di collazione per le colonne vengono ignorate. Le regole di confronto per le colonne possono determinare l'ordine delle righe, che è importante per la convalida dei dati. L'impostazione di `HandleCollationDiff` su `true` risolve automaticamente tali differenze di collazione e impedisce falsi positivi nella convalida dei dati. Il valore predefinito è `false`.

- **RecordFailureDelayInMinutes**: specifica il ritardo in minuti prima della segnalazione dei dettagli relativi a qualsiasi errore di convalida.
- **RecordFailureDelayLimitInMinutes**: specifica il ritardo prima della segnalazione dei dettagli relativi a qualsiasi errore di convalida. Di solito, AWS DMS utilizza la latenza dell'attività per riconoscere il ritardo effettivo delle modifiche alla destinazione per evitare falsi positivi. Questa impostazione sostituisce il valore di ritardo effettivo e consente di impostare un ritardo maggiore prima di restituire i parametri di convalida. Il valore predefinito è 0.
- **RecordSuspendDelayInMinutes**: specifica il ritardo in minuti prima che le tabelle vengano sospese dalla convalida a causa della soglia di errore impostata in `FailureMaxCount`.
- **SkipLobColumns**— Quando questa opzione è impostata su `true`, AWS DMS salta la convalida dei dati per tutte le colonne LOB nella parte della tabella relativa alla convalida dell'attività. Il valore predefinito è `false`.
- **TableFailureMaxCount**: specifica il numero massimo di righe in una tabella per le quali la convalida non riesce prima che questa venga sospesa per la tabella. Il valore predefinito è 1,000.
- **ThreadCount**— specifica il numero di thread di esecuzione utilizzati durante la convalida. AWS DMS Ogni thread seleziona `not-yet-validated` i dati dall'origine e dalla destinazione per confrontarli e convalidarli. Il valore predefinito è 5. Se `ThreadCount` imposti un numero più alto, AWS DMS puoi completare la convalida più velocemente. Tuttavia, in tal caso AWS DMS esegue più query simultanee, utilizzando più risorse sull'origine e sulla destinazione.
- **ValidationOnly**: quando questa opzione è impostata su `true`, l'attività esegue la convalida dei dati senza alcuna migrazione o replica dei dati. Il valore predefinito è `false`. Non è possibile modificare l'impostazione `ValidationOnly` dopo la creazione dell'attività.

È necessario `TargetTablePrepMode` impostare su `DO_NOTHING` (impostazione predefinita per un'attività di sola convalida) e impostare il tipo di migrazione su uno dei seguenti:

- **Caricamento completo**: imposta il tipo di migrazione dell'attività su `Migrare i dati esistenti nella AWS DMS console`. Oppure, nell' `AWS DMS API`, imposta il tipo di migrazione su `FULL-LOAD`.
- **CDC**: imposta Tipo di migrazione dell'attività su `Replica delle sole modifiche dei dati nella console AWS DMS`. Oppure, nell' `AWS DMS API`, imposta il tipo di migrazione su `CDC`.

Indipendentemente dal tipo di migrazione scelto, i dati non vengono migrati o replicati durante un'attività di sola convalida.

Per ulteriori informazioni, consulta [Attività di sola convalida](#).

⚠ Important

L'impostazione `ValidationOnly` è immutabile. Non può essere modificata per un'attività già creata.

- `ValidationPartialLobSize`: indica se si desidera eseguire una convalida parziale per le colonne LOB anziché convalidare tutti i dati memorizzati nella colonna. Questo potrebbe essere utile per migrare solo una parte dei dati LOB e non l'intero set di dati LOB. Il valore è espresso in unità KB. Il valore predefinito è 0, che significa che AWS DMS convalida tutti i dati della colonna LOB. Ad esempio, `"ValidationPartialLobSize": 32` significa che convalida AWS DMS solo i primi 32 KB dei dati della colonna sia nell'origine che nella destinazione.
- `PartitionSize`: specifica la dimensione del batch dei record da leggere per il confronto sia dall'origine che dalla destinazione. Il valore predefinito è 10.000.
- `ValidationQueryCdcDelaySeconds`: il periodo di tempo in cui viene ritardata la prima query di convalida sia sull'origine che sulla destinazione per ogni aggiornamento CDC. Può aiutare a ridurre il conflitto di risorse quando la latenza di migrazione è elevata. Un'attività di sola convalida imposta automaticamente questa opzione su 180 secondi. Il valore predefinito è 0.

Ad esempio, il seguente file JSON consente la convalida dei dati con un numero di thread doppio rispetto all'impostazione predefinita. Inoltre, calcola anche le differenze nell'ordine dei record a causa delle differenze di collazione per le colonne negli endpoint PostgreSQL. Fornisce inoltre un ritardo di notifica della convalida per calcolare il tempo aggiuntivo di elaborazione degli errori di convalida.

```
"ValidationSettings": {
  "EnableValidation": true,
  "ThreadCount": 10,
  "HandleCollationDiff": true,
  "RecordFailureDelayLimitInMinutes": 30
}
```

ℹ Note

Per un endpoint Oracle, AWS DMS utilizza `DBMS_CRYPTO` per convalidare i BLOB. Se l'endpoint Oracle utilizza i BLOB, concedi l'autorizzazione `execute` per `DBMS_CRYPTO`

all'account utente che accede all'endpoint Oracle. Per farlo, esegui l'istruzione riportata di seguito.

```
grant execute on sys.dbms_crypto to dms_endpoint_user;
```

Impostazioni delle attività per la gestione di DDL durante l'elaborazione delle modifiche

Le seguenti impostazioni determinano il modo in cui AWS DMS gestisce le modifiche DDL (Data Definition Language) per le tabelle di destinazione durante l'acquisizione dei dati delle modifiche (CDC). Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Le impostazioni delle attività per gestire l'elaborazione delle modifiche DDL includono quanto segue:

- `HandleSourceTableDropped` – Imposta questa opzione su `true` per eliminare la tabella di destinazione quando la tabella di origine viene eliminata.
- `HandleSourceTableTruncated`: imposta questa opzione su `true` per troncatura la tabella di destinazione quando la tabella di origine viene troncata.
- `HandleSourceTableAltered`: imposta questa opzione su `true` per modificare la tabella di destinazione quando la tabella di origine viene modificata.

Di seguito è riportato un esempio di come le impostazioni delle attività che gestiscono l'elaborazione delle modifiche DDL vengono visualizzate in un file JSON di impostazione delle attività:

```
"ChangeProcessingDdlHandlingPolicy": {  
  "HandleSourceTableDropped": true,  
  "HandleSourceTableTruncated": true,  
  "HandleSourceTableAltered": true  
},
```

Note

Per informazioni sulle istruzioni DDL supportate per un endpoint specifico, consulta l'argomento che descrive l'endpoint.

Impostazioni dell'attività di sostituzione dei caratteri

È possibile specificare che l'attività di replica esegua sostituzioni di caratteri nel database di destinazione per tutte le colonne del database di origine con il tipo di dati `or. AWS DMS STRING` `WSTRING`. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Puoi configurare la sostituzione dei caratteri per qualsiasi attività con endpoint dai seguenti database di origine e di destinazione:

- Database di origine:
 - Oracle
 - Microsoft SQL Server
 - MySQL
 - PostgreSQL
 - SAP Adaptive Server Enterprise (ASE)
 - IBM Db2 LUW
- Database di destinazione:
 - Oracle
 - Microsoft SQL Server
 - MySQL
 - PostgreSQL
 - SAP Adaptive Server Enterprise (ASE)
 - Amazon Redshift

Puoi specificare le sostituzioni dei caratteri utilizzando il parametro `CharacterSetSettings` nelle impostazioni delle attività. Queste sostituzioni dei caratteri si verificano per i caratteri specificati utilizzando il valore del punto di codice Unicode in notazione esadecimale. Puoi implementare le sostituzioni in due fasi, nel seguente ordine se sono specificate entrambe:

1. Sostituzione di caratteri individuali: AWS DMS può sostituire i valori dei caratteri selezionati sull'origine con valori sostitutivi specificati dei caratteri corrispondenti sulla destinazione. Utilizza la matrice `CharacterReplacements` in `CharacterSetSettings` per selezionare tutti i caratteri di origine con i punti di codice Unicode specificati. Utilizza questa matrice anche per specificare i punti di codice di sostituzione per i caratteri corrispondenti sulla destinazione.

Per selezionare tutti i caratteri sull'origine che hanno un determinato punto di codice, imposta un'istanza di `SourceCharacterCodePoint` nella matrice `CharacterReplacements` su tale punto di codice. Successivamente, specifica il punto di codice di sostituzione per tutti i caratteri destinazione equivalenti impostando l'istanza corrispondente di `TargetCharacterCodePoint` in questa matrice. Per eliminare i caratteri di destinazione anziché sostituirli, imposta le istanze appropriate di `TargetCharacterCodePoint` su zero (0). Puoi sostituire o eliminare tutti i valori diversi di caratteri di destinazione desiderati specificando coppie aggiuntive di impostazioni `SourceCharacterCodePoint` e `TargetCharacterCodePoint` nella matrice `CharacterReplacements`. Se specifichi lo stesso valore per più istanze di `SourceCharacterCodePoint`, il valore dell'ultima impostazione corrispondente di `TargetCharacterCodePoint` si applica alla destinazione.

Ad esempio, supponiamo di specificare i seguenti valori per `CharacterReplacements`.

```
"CharacterSetSettings": {
  "CharacterReplacements": [ {
    "SourceCharacterCodePoint": 62,
    "TargetCharacterCodePoint": 61
  }, {
    "SourceCharacterCodePoint": 42,
    "TargetCharacterCodePoint": 41
  }
]
}
```

In questo esempio, AWS DMS sostituisce tutti i caratteri con il valore esadecimale 62 del punto di codice sorgente sulla destinazione con caratteri con il valore del punto di codice 61. Inoltre, AWS DMS sostituisce tutti i caratteri con il codice sorgente punto 42 sulla destinazione con caratteri con il valore del punto di codice 41. In altre parole, AWS DMS sostituisce tutte le istanze della lettera 'b' sulla destinazione con la lettera 'a'. Analogamente, AWS DMS sostituisce tutte le istanze della lettera 'B' sulla destinazione con la lettera 'A'.

2. Convalida e sostituzione del set di caratteri: una volta completata la sostituzione dei singoli caratteri, è AWS DMS possibile verificare che tutti i caratteri di destinazione abbiano punti di codice Unicode validi nel singolo set di caratteri specificato. Puoi utilizzare `CharacterSetSupport` in `CharacterSetSettings` per configurare la verifica e la modifica di questo carattere di destinazione. Per specificare il set di caratteri di verifica, imposta `CharacterSet` in `CharacterSetSupport` sul valore di stringa del set di caratteri. Di seguito,

i possibili valori per `CharacterSet`. È possibile AWS DMS modificare i caratteri di destinazione non validi in uno dei seguenti modi:

- Specifica un singolo punto di codice Unicode sostitutivo per tutti i caratteri di destinazione non validi, indipendentemente dal punto di codice corrente. Per configurare questo punto di codice sostitutivo, imposta `ReplaceWithCharacterCodePoint` in `CharacterSetSupport` sul valore specificato.
- Configura l'eliminazione di tutti i caratteri di destinazione non validi impostando `ReplaceWithCharacterCodePoint` su zero (0).

Ad esempio, supponiamo di specificare i seguenti valori per `CharacterSetSupport`.

```
"CharacterSetSettings": {
  "CharacterSetSupport": {
    "CharacterSet": "UTF16_PlatformEndian",
    "ReplaceWithCharacterCodePoint": 0
  }
}
```

In questo esempio, AWS DMS elimina tutti i caratteri trovati sulla destinazione che non sono validi nel set di caratteri. "UTF16_PlatformEndian" Pertanto, vengono eliminati tutti i caratteri specificati con il valore esadecimale 2FB6. Questo valore non è valido perché si tratta di un punto di codice Unicode a 4 byte e i set di caratteri UTF16 accettano solo caratteri con punti di codice a 2 byte.

Note

L'attività di replica completa tutte le sostituzioni dei caratteri specificate prima di avviare qualsiasi trasformazione globale o a livello di tabella specificata tramite la mappatura delle tabelle. Per ulteriori informazioni sulla mappatura delle tabelle, consulta [Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività](#).

La sostituzione dei caratteri non supporta i tipi di dati LOB. È incluso qualsiasi tipo di dati che DMS considera LOB. Ad esempio, il tipo di dati Extended in Oracle è considerato LOB. Per ulteriori informazioni sui tipi di dati di origine, consulta [Tipi di dati di origine per Oracle](#).

I valori che AWS DMS supportano for `CharacterSet` vengono visualizzati nella tabella seguente.

UTF-8	ibm-860_P100-1995	ibm-280_P100-1995
UTF-16	ibm-861_P100-1995	ibm-284_P100-1995
UTF-16BE	ibm-862_P100-1995	ibm-285_P100-1995
UTF-16LE	ibm-863_P100-1995	ibm-290_P100-1995
UTF-32	ibm-864_X110-1999	ibm-297_P100-1995
UTF-32BE	ibm-865_P100-1995	ibm-420_X120-1999
UTF-32LE	ibm-866_P100-1995	ibm-424_P100-1995
UTF16_PlatformEndian	ibm-867_P100-1998	ibm-500_P100-1995
UTF16_OppositeEndian	ibm-868_P100-1995	ibm-803_P100-1999
UTF32_PlatformEndian	ibm-869_P100-1995	ibm-838_P100-1995
UTF32_OppositeEndian	ibm-878_P100-1996	ibm-870_P100-1995
UTF-16BE,version=1	ibm-901_P100-1999	ibm-871_P100-1995
UTF-16LE,version=1	ibm-902_P100-1999	ibm-875_P100-1995
UTF-16,version=1	ibm-922_P100-1999	ibm-918_P100-1995
UTF-16,version=2	ibm-1168_P100-2002	ibm-930_P120-1999
UTF-7	ibm-4909_P100-1999	ibm-933_P110-1995
IMAP-mailbox-name	ibm-5346_P100-1998	ibm-935_P110-1999
SCSU	ibm-5347_P100-1998	ibm-937_P110-1999
BOCU-1	ibm-5348_P100-1997	ibm-939_P120-1999
CESU-8	ibm-5349_P100-1998	ibm-1025_P100-1995
ISO-8859-1	ibm-5350_P100-1998	ibm-1026_P100-1995

US-ASCII	ibm-9447_P100-2002	ibm-1047_P100-1995
gb18030	ibm-9448_X100-2005	ibm-1097_P100-1995
ibm-912_P100-1995	ibm-9449_P100-2002	ibm-1112_P100-1995
ibm-913_P100-2000	ibm-5354_P100-1998	ibm-1122_P100-1999
ibm-914_P100-1995	ibm-1250_P100-1995	ibm-1123_P100-1995
ibm-915_P100-1995	ibm-1251_P100-1995	ibm-1130_P100-1997
ibm-1089_P100-1995	ibm-1252_P100-2000	ibm-1132_P100-1998
ibm-9005_X110-2007	ibm-1253_P100-1995	ibm-1137_P100-1999
ibm-813_P100-1995	ibm-1254_P100-1995	ibm-4517_P100-2005
ibm-5012_P100-1999	ibm-1255_P100-1995	ibm-1140_P100-1997
ibm-916_P100-1995	ibm-5351_P100-1998	ibm-1141_P100-1997
ibm-920_P100-1995	ibm-1256_P110-1997	ibm-1142_P100-1997
iso-8859_10-1998	ibm-5352_P100-1998	ibm-1143_P100-1997
iso-8859_11-2001	ibm-1257_P100-1995	ibm-1144_P100-1997
ibm-921_P100-1995	ibm-5353_P100-1998	ibm-1145_P100-1997
iso-8859_14-1998	ibm-1258_P100-1997	ibm-1146_P100-1997
ibm-923_P100-1998	macos-0_2-10.2	ibm-1147_P100-1997
ibm-942_P12A-1999	macos-6_2-10.4	ibm-1148_P100-1997
ibm-943_P15A-2003	macos-7_3-10.2	ibm-1149_P100-1997
ibm-943_P130-1999	macos-29-10.2	ibm-1153_P100-1999
ibm-33722_P12A_P12 A-2009_U2	macos-35-10.2	ibm-1154_P100-1999

ibm-33722_P120-1999	ibm-1051_P100-1995	ibm-1155_P100-1999
ibm-954_P101-2007	ibm-1276_P100-1995	ibm-1156_P100-1999
euc-jp-2007	ibm-1006_P100-1995	ibm-1157_P100-1999
ibm-1373_P100-2002	ibm-1098_P100-1995	ibm-1158_P100-1999
windows-950-2000	ibm-1124_P100-1996	ibm-1160_P100-1999
ibm-950_P110-1999	ibm-1125_P100-1997	ibm-1164_P100-1999
ibm-1375_P100-2008	ibm-1129_P100-1997	ibm-1364_P110-2007
ibm-5471_P100-2006	ibm-1131_P100-1997	ibm-1371_P100-1999
ibm-1386_P100-2001	ibm-1133_P100-1997	ibm-1388_P103-2001
windows-936-2000	ISO_2022,locale=ja ,version=0	ibm-1390_P110-2003
ibm-1383_P110-1999	ISO_2022,locale=ja ,version=1	ibm-1399_P110-2003
ibm-5478_P100-1995	ISO_2022,locale=ja ,version=2	ibm-5123_P100-1999
euc-tw-2014	ISO_2022,locale=ja ,version=3	ibm-8482_P100-1999
ibm-964_P110-1999	ISO_2022,locale=ja ,version=4	ibm-16684_P110-2003
ibm-949_P110-1999	ISO_2022,locale=ko ,version=0	ibm-4899_P100-1998
ibm-949_P11A-1999	ISO_2022,locale=ko ,version=1	ibm-4971_P100-1999

ibm-970_P110_P110-2006_U2	ISO_2022,locale=zh,version=0	ibm-9067_X100-2005
ibm-971_P100-1995	ISO_2022,locale=zh,version=1	ibm-12712_P100-1998
ibm-1363_P11B-1998	ISO_2022,locale=zh,version=2	ibm-16804_X110-1999
ibm-1363_P110-1997	HZ	ibm-37_P100-1995,swaplfnl
windows-949-2000	x11-compound-text	ibm-1047_P100-1995,swaplfnl
windows-874-2000	ISCII,version=0	ibm-1140_P100-1997,swaplfnl
ibm-874_P100-1995	ISCII,version=1	ibm-1141_P100-1997,swaplfnl
ibm-1162_P100-1999	ISCII,version=2	ibm-1142_P100-1997,swaplfnl
ibm-437_P100-1995	ISCII,version=3	ibm-1143_P100-1997,swaplfnl
ibm-720_P100-1997	ISCII,version=4	ibm-1144_P100-1997,swaplfnl
ibm-737_P100-1997	ISCII,version=5	ibm-1145_P100-1997,swaplfnl
ibm-775_P100-1996	ISCII,version=6	ibm-1146_P100-1997,swaplfnl
ibm-850_P100-1995	ISCII,version=7	ibm-1147_P100-1997,swaplfnl

ibm-851_P100-1995	ISCII,version=8	ibm-1148_P100-1997 ,swaplfnl
ibm-852_P100-1995	LMBCS-1	ibm-1149_P100-1997 ,swaplfnl
ibm-855_P100-1995	ibm-37_P100-1995	ibm-1153_P100-1999 ,swaplfnl
ibm-856_P100-1995	ibm-273_P100-1995	ibm-12712_P100-199 8,swaplfnl
ibm-857_P100-1995	ibm-277_P100-1995	ibm-16804_X110-199 9,swaplfnl
ibm-858_P100-1997	ibm-278_P100-1995	ebcdic-xml-us

Impostazioni dell'attività immagine precedente

Quando si scrivono aggiornamenti CDC a una destinazione di flusso di dati come Kinesis o Apache Kafka, è possibile visualizzare i valori originali di una riga del database di origine prima della modifica da un aggiornamento. Per rendere possibile ciò, AWS DMS compila un'immagine precedente degli eventi di aggiornamento in base ai dati forniti dal motore di database di origine. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

Per farlo, usa il parametro `BeforeImageSettings` che aggiunge un nuovo attributo JSON a ogni operazione di aggiornamento con valori raccolti dal sistema di database di origine.

Assicurati di applicare `BeforeImageSettings` solo alle attività di pieno carico e CDC o alle attività di sola CDC. Le attività di pieno carico e CDC migrano i dati esistenti e replicano le modifiche in corso. Le attività di sola CDC replicano solo le modifiche ai dati.

Non applicare `BeforeImageSettings` alle attività a pieno carico.

Le possibili opzioni per `BeforeImageSettings` sono le seguenti:

- `EnableBeforeImage`: si attiva prima dell'acquisizione dell'immagine quando è impostata su `true`. Il valore predefinito è `false`.

- **FieldName**: assegna un nome al nuovo attributo JSON. Quando **EnableBeforeImage** è **true**, **FieldName** è richiesto e non può essere vuoto.
- **ColumnFilter**: specifica una colonna da aggiungere utilizzando l'acquisizione dell'immagine precedente. Per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella, utilizzare il valore predefinito, **pk-only**. Per aggiungere qualsiasi colonna con un valore immagine prima, utilizzare **all**. L'immagine precedente non supporta tipi di dati LOB (oggetti binari di grandi dimensioni) come CLOB e BLOB.

L'esempio seguente mostra l'utilizzo di **BeforeImageSettings**.

```
"BeforeImageSettings": {  
  "EnableBeforeImage": true,  
  "FieldName": "before-image",  
  "ColumnFilter": "pk-only"  
}
```

Per informazioni sulle impostazioni dell'immagine precedente per Kinesis, incluse le impostazioni di mappatura delle tabelle aggiuntive, consulta [Utilizzo di un'immagine precedente per visualizzare i valori originali delle righe CDC per un flusso di dati Kinesis come destinazione](#).

Per informazioni sulle impostazioni dell'immagine precedente per Kafka, incluse le impostazioni di mappatura delle tabelle aggiuntive, consulta [Utilizzo di un'immagine precedente per visualizzare i valori originali delle righe CDC per Apache Kafka come destinazione](#).

Impostazioni delle attività per la gestione degli errori

Puoi impostare il comportamento di gestione degli errori dell'attività di replica utilizzando le impostazioni seguenti. Per informazioni su come utilizzare un file di configurazione dell'attività per impostare le impostazioni dell'attività, consulta [Esempio di impostazioni delle attività](#).

- **DataErrorPolicy**— Determina l'azione intrapresa da AWS DMS in caso di errore relativo all'elaborazione dei dati a livello di record. Alcuni esempi di errori di elaborazione dei dati includono gli errori di conversione, gli errori di trasformazione e i dati non validi. Il valore predefinito è **LOG_ERROR**.
 - **IGNORE_RECORD**: l'attività continua e i dati per tale record vengono ignorati. Il conteggio degli errori per la proprietà **DataErrorEscalationCount** viene incrementato. Pertanto, se imposti un limite agli errori per una tabella, questo errore viene conteggiato fino al raggiungimento del limite.

- **LOG_ERROR**: l'attività continua e l'errore viene scritto nel log delle attività.
- **SUSPEND_TABLE**: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
- **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
- **DataTruncationErrorPolicy**: determina l'azione effettuata da AWS DMS quando i dati sono troncati. Il valore predefinito è **LOG_ERROR**.
 - **IGNORE_RECORD**: l'attività continua e i dati per tale record vengono ignorati. Il conteggio degli errori per la proprietà **DataErrorEscalationCount** viene incrementato. Pertanto, se imposti un limite agli errori per una tabella, questo errore viene conteggiato fino al raggiungimento del limite.
 - **LOG_ERROR**: l'attività continua e l'errore viene scritto nel log delle attività.
 - **SUSPEND_TABLE**: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
- **DataErrorEscalationPolicy**: determina l'azione effettuata da AWS DMS quando il numero massimo di errori (impostato nel parametro **DataErrorEscalationCount**) viene raggiunto. Il valore predefinito è **SUSPEND_TABLE**.
 - **SUSPEND_TABLE**: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
- **DataErrorEscalationCount**: imposta il numero massimo di errori che possono verificarsi per i dati per un record specifico. Quando questo numero viene raggiunto, i dati per la tabella che contiene il record di errore vengono gestiti in base al set di policy in **DataErrorEscalationPolicy**. Il valore predefinito è 0.
- **EventErrorPolicy**— Determina l'azione intrapresa da AWS DMS quando si verifica un errore durante l'invio di un evento relativo all'attività. I valori possibili sono:
 - **IGNORE**: l'attività continua e tutti i dati associati all'evento vengono ignorati.
 - **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
- **TableErrorPolicy**: determina l'azione effettuata da AWS DMS quando si verifica un errore durante l'elaborazione dei dati o dei metadati per una tabella specifica. Questo errore si applica solo ai dati di tabella generali e non è correlato a un record specifico. Il valore predefinito è **SUSPEND_TABLE**.

- `SUSPEND_TABLE`: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
- `STOP_TASK`: l'attività viene interrotta ed è necessario l'intervento manuale.
- `TableErrorEscalationPolicy`: determina l'azione effettuata da AWS DMS quando il numero massimo di errori (impostato mediante il parametro `TableErrorEscalationCount`) viene raggiunto. L'impostazione predefinita e l'unica disponibile per l'utente è `STOP_TASK`, in base alla quale l'attività viene arrestata ed è necessario l'intervento manuale.
- `TableErrorEscalationCount`: il numero massimo di errori che possono verificarsi per i dati o i metadati generali per una tabella specifica. Quando questo numero viene raggiunto, i dati per la tabella vengono gestiti in base al set di policy in `TableErrorEscalationPolicy`. Il valore predefinito è 0.
- `RecoverableErrorCount`: il numero massimo di tentativi effettuati per riavviare un'attività quando si verifica un errore ambientale. Dopo che il sistema ha tentato di riavviare l'attività il numero specificato di volte, l'attività viene arrestata ed è necessario l'intervento manuale. Il valore predefinito è -1, che indica di tentare di riavviare AWS DMS l'attività all'infinito. Quando si imposta questo valore su -1, il numero di tentativi effettuati da DMS varia in base al tipo di errore restituito nel modo seguente:
 - Stato di esecuzione, errore ripristinabile: se si verifica un errore recuperabile, ad esempio una connessione persa o un errore nell'applicazione di un obiettivo, DMS riprova l'operazione nove volte.
 - Stato iniziale, errore recuperabile: DMS riprova l'operazione sei volte.
 - Stato di esecuzione, errore irreversibile gestito da DMS: DMS riprova l'operazione sei volte.
 - Stato in esecuzione, errore irreversibile non gestito da DMS: DMS non riprova l'operazione.

Per fare in modo che non venga mai tentato di riavviare un'attività, imposta il valore su 0.

Si consiglia di impostare `RecoverableErrorCount` e impostare valori tali `RecoverableErrorInterval` da consentire un numero sufficiente di tentativi a intervalli sufficienti per consentire il corretto ripristino dell'attività DMS. Se si verifica un errore irreversibile, nella maggior parte degli scenari DMS interrompe i tentativi di riavvio.

- `RecoverableErrorInterval`— Il numero di secondi che AWS DMS attende tra un tentativo e l'altro per riavviare un'attività. Il predefinito è 5.
- `RecoverableErrorThrottling`: se abilitato, l'intervallo tra i tentativi di riavvio di un'attività viene aumentato in una serie in base al valore di `RecoverableErrorInterval`. Ad esempio, se

`RecoverableErrorInterval` è impostato su 5 secondi, il tentativo successivo verrà eseguito dopo 10 secondi, quindi 20, 40 secondi e così via. Il valore predefinito è `true`.

- `RecoverableErrorThrottlingMax`— Il numero massimo di secondi che AWS DMS attende tra i tentativi di riavvio di un'attività, se abilitata. `RecoverableErrorThrottling` Il valore predefinito è 1800.
- `RecoverableErrorStopRetryAfterThrottlingMax`— Se impostato su `true`, interrompe il riavvio dell'attività dopo aver raggiunto il numero massimo di secondi di AWS DMS attesa tra i tentativi di ripristino, per. `RecoverableErrorThrottlingMax`
- `ApplyErrorDeletePolicy`: determina quale azione viene effettuata da AWS DMS se si verifica un conflitto con un'operazione DELETE. Il valore predefinito è `IGNORE_RECORD`. I valori possibili sono i seguenti:
 - `IGNORE_RECORD`: l'attività continua e i dati per tale record vengono ignorati. Il conteggio degli errori per la proprietà `ApplyErrorEscalationCount` viene incrementato. Pertanto, se imposti un limite agli errori per una tabella, questo errore viene conteggiato fino al raggiungimento del limite.
 - `LOG_ERROR`: l'attività continua e l'errore viene scritto nel log delle attività.
 - `SUSPEND_TABLE`: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - `STOP_TASK`: l'attività viene interrotta ed è necessario l'intervento manuale.
- `ApplyErrorInsertPolicy`: determina quale azione viene effettuata da AWS DMS se si verifica un conflitto con un'operazione INSERT. Il valore predefinito è `LOG_ERROR`. I valori possibili sono i seguenti:
 - `IGNORE_RECORD`: l'attività continua e i dati per tale record vengono ignorati. Il conteggio degli errori per la proprietà `ApplyErrorEscalationCount` viene incrementato. Pertanto, se imposti un limite agli errori per una tabella, questo errore viene conteggiato fino al raggiungimento del limite.
 - `LOG_ERROR`: l'attività continua e l'errore viene scritto nel log delle attività.
 - `SUSPEND_TABLE`: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - `STOP_TASK`: l'attività viene interrotta ed è necessario l'intervento manuale.
 - `INSERT_RECORD`: se è presente un record di destinazione esistente con la stessa chiave primaria del record di origine inserito, il record di destinazione viene aggiornato.

- **ApplyErrorUpdatePolicy**: determina quale azione viene effettuata da AWS DMS se si verifica un conflitto con un'operazione UPDATE. Il valore predefinito è LOG_ERROR. I valori possibili sono i seguenti:
 - **IGNORE_RECORD**: l'attività continua e i dati per tale record vengono ignorati. Il conteggio degli errori per la proprietà `ApplyErrorEscalationCount` viene incrementato. Pertanto, se imposti un limite agli errori per una tabella, questo errore viene conteggiato fino al raggiungimento del limite.
 - **LOG_ERROR**: l'attività continua e l'errore viene scritto nel log delle attività.
 - **SUSPEND_TABLE**: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
 - **UPDATE_RECORD**— Se manca il record di destinazione, il record di destinazione mancante viene inserito nella tabella di destinazione. AWS DMS disabilita completamente il supporto delle colonne LOB per l'attività. La selezione di questa opzione richiede l'abilitazione del log supplementare completo per tutte le colonne della tabella di origine se Oracle è il database di origine.
- **ApplyErrorEscalationPolicy**— Determina l'azione intrapresa da AWS DMS quando viene raggiunto il numero massimo di errori (impostato utilizzando il `ApplyErrorEscalationCount` parametro). Il valore predefinito è LOG_ERROR:
 - **LOG_ERROR**: l'attività continua e l'errore viene scritto nel log delle attività.
 - **SUSPEND_TABLE**: l'attività continua, ma i dati provenienti dalla tabella con il record di errore vengono spostati in uno stato di errore e i dati non vengono replicati.
 - **STOP_TASK**: l'attività viene interrotta ed è necessario l'intervento manuale.
- **ApplyErrorEscalationCount**: questa opzione imposta il numero massimo di conflitti APPLY che possono verificarsi per una tabella specifica durante un'operazione di elaborazione delle modifiche. Quando questo numero viene raggiunto, i dati della tabella vengono gestiti in base alla policy impostata nel parametro `ApplyErrorEscalationPolicy`. Il valore predefinito è 0.
- **ApplyErrorFailOnTruncationDdl**: imposta questa opzione su `true` per causare l'errore dell'attività quando un troncamento viene eseguito su una qualsiasi delle tabelle tracciate durante l'operazione CDC. Il valore predefinito è `false`.

Questo approccio non funziona con PostgreSQL 11.x o versioni precedenti oppure qualsiasi altro endpoint di origine che non replica il troncamento della tabella DDL.

- `FailOnNoTablesCaptured`: imposta questa opzione su `true` per causare l'errore dell'attività quando le mappature della tabella definite per un'attività non trovano alcuna tabella all'avvio dell'attività. Il valore predefinito è `false`.
- `FailOnTransactionConsistencyBreached`: questa opzione si applica alle attività mediante Oracle come origine con l'operazione CDC. Il valore predefinito è `false`. Impostala su `true` per causare l'errore dell'attività quando una transazione viene aperta per un periodo di tempo maggiore rispetto al timeout specificato e può essere eliminata.

Quando un'attività CDC inizia con Oracle, AWS DMS attende per un periodo di tempo limitato la chiusura della transazione aperta più vecchia prima di avviare CDC. Se la transazione aperta più vecchia non si chiude fino al raggiungimento del timeout, nella maggior parte dei casi AWS DMS avvia CDC, ignorando quella transazione. Se questa opzione è impostata su `true`, l'attività ha esito negativo.

- `FullLoadIgnoreConflicts`— Imposta questa opzione in modo da `true` AWS DMS ignorare gli errori «zero righe interessate» e «duplicati» quando si applicano gli eventi memorizzati nella cache. Se impostato su `false`, AWS DMS riporta tutti gli errori invece di ignorarli. Il valore predefinito è `true`.

Tieni presente che gli errori di caricamento delle tabelle in Redshift come destinazione sono riportati in `STL_LOAD_ERRORS`. Per ulteriori informazioni, consulta [STL_LOAD_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Salvataggio delle impostazioni delle attività

Puoi salvare le impostazioni per un'attività come file JSON, se desideri riutilizzare le impostazioni per un'altra attività. Le impostazioni delle attività da copiare in un file JSON sono disponibili nella sezione Dettagli della panoramica di un'attività.

Note

Quando riutilizzi le impostazioni delle attività per altre attività, rimuovi `CloudWatchLogGroup` gli eventuali attributi `CloudWatchLogStream`. In caso contrario, viene visualizzato il seguente errore: MESSAGGIO DI ERRORE DI SISTEMA: Impostazioni attività `CloudWatchLogGroup` o `CloudWatchLogStream` non può essere impostato al momento della creazione.

Ad esempio, il seguente file JSON contiene le impostazioni salvate per un'attività.

```
{
  "TargetMetadata": {
    "TargetSchema": "",
    "SupportLobs": true,
    "FullLobMode": false,
    "LobChunkSize": 0,
    "LimitedSizeLobMode": true,
    "LobMaxSize": 32,
    "InlineLobMaxSize": 0,
    "LoadMaxFileSize": 0,
    "ParallelLoadThreads": 0,
    "ParallelLoadBufferSize": 0,
    "BatchApplyEnabled": false,
    "TaskRecoveryTableEnabled": false,
    "ParallelLoadQueuesPerThread": 0,
    "ParallelApplyThreads": 0,
    "ParallelApplyBufferSize": 0,
    "ParallelApplyQueuesPerThread": 0
  },
  "FullLoadSettings": {
    "TargetTablePrepMode": "DO_NOTHING",
    "CreatePkAfterFullLoad": false,
    "StopTaskCachedChangesApplied": false,
    "StopTaskCachedChangesNotApplied": false,
    "MaxFullLoadSubTasks": 8,
    "TransactionConsistencyTimeout": 600,
    "CommitRate": 10000
  },
  "Logging": {
    "EnableLogging": true,
    "LogComponents": [
      {
        "Id": "TRANSFORMATION",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      },
      {
        "Id": "SOURCE_UNLOAD",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
      },
      {
        "Id": "IO",
```

```
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "TARGET_LOAD",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "PERFORMANCE",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "SOURCE_CAPTURE",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "SORTER",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "REST_SERVER",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "VALIDATOR_EXT",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "TARGET_APPLY",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "TASK_MANAGER",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "TABLES_MANAGER",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "METADATA_MANAGER",
    "Severity": "LOGGER_SEVERITY_DEFAULT"
  },
  {
    "Id": "FILE_FACTORY",
```



```

        "Severity": "LOGGER_SEVERITY_DEFAULT"
    },
    {
        "Id": "COMMON",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
    },
    {
        "Id": "ADDONS",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
    },
    {
        "Id": "DATA_STRUCTURE",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
    },
    {
        "Id": "COMMUNICATION",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
    },
    {
        "Id": "FILE_TRANSFER",
        "Severity": "LOGGER_SEVERITY_DEFAULT"
    }
]
},
"ControlTablesSettings": {
    "ControlSchema": "",
    "HistoryTimeslotInMinutes": 5,
    "HistoryTableEnabled": false,
    "SuspendedTablesTableEnabled": false,
    "StatusTableEnabled": false,
    "FullLoadExceptionTableEnabled": false
},
"StreamBufferSettings": {
    "StreamBufferCount": 3,
    "StreamBufferSizeInMB": 8,
    "CtrlStreamBufferSizeInMB": 5
},
"ChangeProcessingDdlHandlingPolicy": {
    "HandleSourceTableDropped": true,
    "HandleSourceTableTruncated": true,
    "HandleSourceTableAltered": true
},
"ErrorBehavior": {
    "DataErrorPolicy": "LOG_ERROR",

```

```

    "DataTruncationErrorPolicy": "LOG_ERROR",
    "DataErrorEscalationPolicy": "SUSPEND_TABLE",
    "DataErrorEscalationCount": 0,
    "TableErrorPolicy": "SUSPEND_TABLE",
    "TableErrorEscalationPolicy": "STOP_TASK",
    "TableErrorEscalationCount": 0,
    "RecoverableErrorCount": -1,
    "RecoverableErrorInterval": 5,
    "RecoverableErrorThrottling": true,
    "RecoverableErrorThrottlingMax": 1800,
    "RecoverableErrorStopRetryAfterThrottlingMax": true,
    "ApplyErrorDeletePolicy": "IGNORE_RECORD",
    "ApplyErrorInsertPolicy": "LOG_ERROR",
    "ApplyErrorUpdatePolicy": "LOG_ERROR",
    "ApplyErrorEscalationPolicy": "LOG_ERROR",
    "ApplyErrorEscalationCount": 0,
    "ApplyErrorFailOnTruncationDdl": false,
    "FullLoadIgnoreConflicts": true,
    "FailOnTransactionConsistencyBreached": false,
    "FailOnNoTablesCaptured": true
  },
  "ChangeProcessingTuning": {
    "BatchApplyPreserveTransaction": true,
    "BatchApplyTimeoutMin": 1,
    "BatchApplyTimeoutMax": 30,
    "BatchApplyMemoryLimit": 500,
    "BatchSplitSize": 0,
    "MinTransactionSize": 1000,
    "CommitTimeout": 1,
    "MemoryLimitTotal": 1024,
    "MemoryKeepTime": 60,
    "StatementCacheSize": 50
  },
  "PostProcessingRules": null,
  "CharacterSetSettings": null,
  "LoopbackPreventionSettings": null,
  "BeforeImageSettings": null,
  "FailTaskWhenCleanTaskResourceFailed": false
}

```

Impostazione del supporto LOB per i database di origine in un task AWS DMS

Talvolta può risultare difficile eseguire la migrazione dei LOB (oggetti binari di grandi dimensioni) tra sistemi. AWS DMS offre una serie di opzioni per facilitare l'ottimizzazione delle colonne LOB. Per vedere da quali e quando i tipi di dati vengono considerati LOB AWS DMS, consulta la AWS DMS documentazione.

Quando esegui la migrazione dei dati da un database a un altro, puoi modificare il modo in cui i LOB vengono archiviati, in particolare per le migrazioni eterogenee. Per farlo, non è necessario eseguire la migrazione dei dati LOB.

Se decidi di includere i LOB, puoi quindi specificare le altre impostazioni LOB:

- La modalità LOB determina il modo in cui i LOB sono gestiti:
 - Modalità LOB completa: in modalità LOB completa, tutti i LOB dall'origine alla destinazione indipendentemente dalle dimensioni. AWS DMS In questa configurazione, non AWS DMS dispone di informazioni sulla dimensione massima prevista dei LOB. Di conseguenza, i LOB vengono migrati uno alla volta, pezzo per pezzo. La modalità LOB completa può essere piuttosto lenta.
 - Modalità LOB limitata: in modalità LOB limitata imposta una dimensione massima per i LOB che DMS dovrà accettare. Questa opzione consente a DMS di pre-allocare la memoria e caricare i dati LOB in blocco. I LOB che superano le dimensioni massime vengono troncati e verrà emesso un avviso sul file di log. In modalità LOB limitata puoi ottenere un notevole miglioramento delle prestazioni rispetto alla modalità LOB completa. È consigliabile utilizzare la limited LOB mode (Modalità LOB limitata) quando possibile. Il valore massimo consigliato è 102400 KB (100 MB).

Note

L'utilizzo dell'opzione Dimensione massima LOB (K) con un valore superiore a 63 KB influisce sulle prestazioni di un carico completo configurato per l'esecuzione in modalità LOB limitata. Durante un pieno carico, DMS alloca la memoria moltiplicando il valore della dimensione massima LOB (K) per la frequenza di commit e il prodotto viene moltiplicato per il numero di colonne LOB. Quando DMS non è in grado di preallocare la memoria, DMS inizia a consumare memoria SWAP e ciò influisce sulle prestazioni del pieno carico. Pertanto, se riscontri problemi di prestazioni quando utilizzi la modalità LOB limitata, prendi in considerazione la possibilità di ridurre la frequenza di commit fino a raggiungere un livello di prestazioni accettabile. Puoi anche vagliare l'utilizzo della

modalità LOB in linea per gli endpoint supportati una volta compresa la distribuzione LOB della tabella.

Per convalidare una dimensione LOB limitata, è necessario impostare `ValidationPartialLobSize` sullo stesso valore di `LobMaxSize (K)`.

- Modalità LOB in linea: in modalità LOB in linea, si imposta la dimensione massima LOB che DMS trasferisce in linea. I LOB più piccoli della dimensione specificata vengono trasferiti in linea. I LOB più grandi della dimensione specificata vengono replicati utilizzando la modalità LOB completa. È possibile selezionare questa opzione per replicare LOB di piccole e grandi dimensioni quando la maggior parte dei LOB è piccola. DMS non supporta la modalità LOB in linea per gli endpoint che non supportano la modalità LOB completa, come S3 e Redshift.

Note

Con Oracle, i LOB vengono trattati come tipi di dati VARCHAR, quando possibile. Questo approccio significa che li AWS DMS recupera dal database in blocco, il che è notevolmente più veloce rispetto ad altri metodi. Poiché la dimensione massima di una stringa VARCHAR in Oracle è 32 K, la dimensione di un LOB limitato inferiore a 32 K è ottimale quando il database di origine è Oracle.

- Quando un'attività è configurata per l'esecuzione in Limited LOB mode (Modalità LOB limitata), l'opzione Max LOB size (K) (Dimensione LOB massima (K)) imposta le dimensioni massime del LOB che AWS DMS accetta. Qualsiasi LOB di dimensioni superiori viene troncato in corrispondenza di tale valore.
- Quando un'operazione è configurata per utilizzare la modalità LOB completa, AWS DMS recupera i LOB in parti. L'opzione LOB chunk size (K) (Dimensione blocco LOB (kb)) determina le dimensioni di ciascuna porzione. Quando imposti questa opzione, presta particolare attenzione alle dimensioni massime del pacchetto consentite dalla configurazione di rete. Se le dimensioni del blocco di LOB superano le dimensioni massime del pacchetto consentite, potresti visualizzare degli errori di disconnessione. Il valore consigliato per `LobChunkSize` è 64 kilobyte. L'aumento del valore di `LobChunkSize` su valori superiori a 64 kilobyte può causare errori nelle attività.
- Quando un'attività è configurata per l'esecuzione in modalità LOB in linea, l'impostazione `InlineLobMaxSize` determina quali LOB DMS trasferisce in linea.

Note

Puoi utilizzare i tipi di dati LOB solo con le tabelle e le viste che includono una chiave primaria.

Per ulteriori informazioni sulle impostazioni delle attività per specificare queste opzioni, consultare [Impostazioni delle attività dei metadati di destinazione](#)

Creazione di più attività

In alcuni scenari di migrazione, potrebbe essere necessario creare diverse attività di migrazione. Le attività funzionano in modo indipendente e possono essere eseguite simultaneamente. Ogni attività ha il proprio processo di caricamento iniziale, CDC e di lettura dei log. Le tabelle correlate tramite DML (Data Manipulation Language) devono far parte della stessa attività.

Di seguito sono riportati alcuni motivi per creare più attività per una migrazione:

- Le tabelle di destinazione per le attività risiedono su database diversi, ad esempio nel caso in cui esegui il fan-out o la suddivisione di un sistema in più sistemi.
- Per suddividere la migrazione di una tabella di grandi dimensioni in più attività, puoi utilizzare i filtri.

Note

Poiché ogni attività ha il proprio processo di acquisizione delle modifiche e di lettura dei log, le modifiche non sono coordinate tra le attività. Pertanto, quando utilizzi più attività per eseguire una migrazione, assicurati che ogni singola transazione di origine sia interamente contenuta in un'unica attività. È possibile utilizzare più attività per eseguire una migrazione se nessuna singola transazione è suddivisa tra diverse attività.

Creazione di attività per la replica continua mediante AWS DMS

Puoi creare un'attività AWS DMS che acquisisca le modifiche in corso dal datastore di origine. Puoi eseguire tale acquisizione durante la migrazione dei dati. Puoi inoltre creare un'attività che acquisisce le modifiche in corso dopo aver completato la migrazione iniziale (di caricamento completo) a un datastore di destinazione supportato. Questo processo è denominato replica continua o Change

Data Capture (CDC). AWS DMS utilizza questo processo quando replica le modifiche in corso da un datastore di origine. Questo processo funziona raccogliendo le modifiche nei log di database mediante l'API nativa del motore di database.

Note

Puoi eseguire la migrazione delle viste solo utilizzando le attività di caricamento completo. Se l'attività è solo CDC o di caricamento completo che avvia CDC dopo il completamento, la migrazione include solo le tabelle dall'origine. Utilizzando un'attività di solo caricamento completo, puoi eseguire la migrazione delle viste o una combinazione di tabelle e viste. Per ulteriori informazioni, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON](#).

Ogni motore di origine ha requisiti di configurazione specifici per esporre questo flusso di modifica a un determinato account utente. La maggior parte dei motori richiede alcune configurazioni aggiuntive per consentire al processo di acquisizione di utilizzare i dati delle modifiche in modo significativo, senza perdita di dati. Ad esempio, Oracle richiede l'aggiunta di log supplementare e MySQL richiede la registrazione binaria a livello di riga (registrazione binaria).

Per leggere le modifiche in corso dal database di origine, AWS DMS utilizza le operazioni API specifiche del motore per leggere le modifiche dai log delle transazioni del motore di origine. Di seguito sono riportati alcuni esempi del modo in cui AWS DMS esegue tale operazione:

- Per Oracle, AWS DMS utilizza l'API Oracle LogMiner o l'API Binary Reader (API bfile) per leggere le modifiche in corso. AWS DMS legge le modifiche in corso dai log di archivio o redo online in base al numero di modifica sistema (SCN, System Change Number).
- Per Microsoft SQL Server, AWS DMS utilizza MS-Replication o MS-CDC per scrivere le informazioni nel log delle transazioni di SQL Server. Utilizza quindi le funzioni `fn_dump_dblog()` o `fn_dblog()` in SQL Server per leggere le modifiche nel log delle transazioni in base al numero di sequenza dei log (LSN, Log Sequence Number).
- Per MySQL, AWS DMS legge le modifiche dai log binari basati su riga (binlog) e migra tali modifiche alla destinazione.
- Per PostgreSQL, AWS DMS imposta slot di replica logica e utilizza il plugin `test_decoding` per leggere le modifiche dall'origine e migrarle alla destinazione.
- Per Amazon RDS come origine, è consigliabile assicurarsi che i backup siano abilitati per configurare CDC. È inoltre consigliabile assicurarsi che il database di origine sia configurato in

modo da mantenere i log delle modifiche per un periodo di tempo sufficiente; in genere, 24 ore sono sufficienti. Per le impostazioni specifiche di ciascun endpoint, consulta le seguenti risorse:

- Amazon RDS per Oracle: [Configurazione di una fonte Oracle gestita per AWSAWS DMS](#).
- Amazon RDS per MySQL e Aurora MySQL: [Utilizzo di un AWS database compatibile con MySQL gestito come fonte per AWS DMS](#).
- Amazon RDS per SQL Server: [Configurazione della replica continua su un'istanza database di SQL Server nel cloud](#).
- Amazon RDS per PostgreSQL e Aurora PostgreSQL: PostgreSQL mantiene automaticamente il WAL richiesto.

Esistono due tipi di attività di replica continua:

- Pieno carico e CDC: l'attività esegue la migrazione dei dati esistenti, quindi aggiorna il database di destinazione in base alle modifiche al database di origine.
- sola CDC: l'attività migra le modifiche in corso una volta che sono presenti dati nel database di destinazione.

Esecuzione della replica a partire da un punto di inizio CDC

Puoi avviare un'attività di replica continua di AWS DMS (solo CDC) da diversi punti. Questi sono i seguenti:

- Da un'ora di inizio CDC personalizzata: puoi utilizzare la AWS Management Console o AWS CLI per fornire a AWS DMS un timestamp relativo al momento in cui desideri che la replica venga avviata. AWS DMS avvia quindi un'attività di replica continua a partire da quest'ora di inizio CDC personalizzata. AWS DMS converte il timestamp specificato (in UTC) in un punto di inizio nativo, ad esempio un LSN per SQL Server o un SCN per Oracle. AWS DMS utilizza metodi specifici del motore per determinare il punto in cui avviare l'attività di migrazione in base al flusso di modifica del motore di origine.

Note

Solo impostando l'attributo di connessione `StartFromContext` sul timestamp richiesto, Db2 come origine offre un orario di inizio CDC personalizzato.

PostgreSQL come origine non supporta un'ora di inizio CDC personalizzata. Questo è dovuto al fatto che il motore di database PostgreSQL non dispone di un modo per mappare un timestamp a un LSN o SCN come Oracle e SQL Server.

- Da un punto di inizio nativo CDC: puoi inoltre iniziare da un punto nativo nel log delle transazioni del motore di origine. In alcuni casi, potresti preferire questo approccio perché un timestamp può indicare più punti nativi nel log delle transazioni. AWS DMS supporta questa funzionalità per i seguenti endpoint di origine:
 - SQL Server
 - PostgreSQL
 - Oracle
 - MySQL
 - MariaDB

Quando l'attività viene creata, AWS DMS contrassegna il punto di inizio del CDC e non può essere modificato. Per usare un punto di inizio del CDC diverso, devi creare una nuova attività.

Determinazione di un punto di inizio nativo CDC

Un punto di inizio nativo CDC è un punto nel log del motore di database che definisce un'ora in cui puoi iniziare l'operazione CDC. Ad esempio, supponiamo che un dump del blocco dei dati venga applicato alla destinazione. Puoi cercare il punto di inizio nativo per l'attività di sola replica continua. Per evitare incongruenze nei dati, scegli con attenzione il punto di inizio per l'attività di sola replica. DMS acquisisce le transazioni iniziate dopo il punto di inizio del CDC scelto.

Di seguito sono riportati alcuni esempi di come puoi individuare il punto di inizio nativo CDC dai motori di origine supportati:

SQL Server

In SQL Server, un numero di sequenza di log (LSN, Log Sequence Number) è composto da tre parti:

- Numero di sequenza del file di log virtuale (VLF, Virtual Log File)
- Offset di avvio di un blocco di log
- Numero slot

Di seguito è riportato un LSN di esempio: `00000014:00000061:0001`

Per ottenere il punto di inizio per un'attività di migrazione SQL Server in base alle impostazioni di backup del log delle transazioni, utilizza la funzione `fn_dump_dblog()` o `fn_dblog()` in SQL Server.

Per utilizzare il punto di inizio nativo del CDC con SQL Server, crea una pubblicazione su qualsiasi tabella che partecipa alla replica continua. AWS DMS crea la pubblicazione automaticamente quando si utilizza CDC senza usare un punto di inizio nativo del CDC.

PostgreSQL

Per il database di origine PostgreSQL puoi utilizzare un checkpoint di ripristino CDC. Questo valore del checkpoint viene generato in vari punti quando viene eseguita un'attività di replica in corso per il database di origine (l'attività padre). Per ulteriori informazioni sui checkpoint in generale, consulta [Utilizzo di un checkpoint come punto di inizio CDC](#).

Per identificare il checkpoint da utilizzare come punto di partenza nativo, utilizzare la visualizzazione `pg_replication_slots` del database o i dettagli della panoramica dell'attività principale dalla pagina AWS Management Console.

Per trovare i dettagli generali per l'attività padre sulla console

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Dal riquadro di navigazione, scegliere Attività di migrazione del database.
3. Scegliere l'attività principale dall'elenco nella pagina Attività di migrazione del database . Verrà visualizzata la pagina dell'attività principale che mostra i dettagli della panoramica.
4. Individuare il valore del checkpoint in Change data capture (CDC), posizione iniziale Change Data Capture (CDC) e punto di ripristino Change Data Capture (CDC).

Il valore appare simile all'esempio seguente:

```
checkpoint:V1#1#000004AF/B00000D0#0#0#*#0#0
```

Qui, il componente `4AF/B00000D0` è quanto necessario per specificare questo punto di avvio CDC nativo. Impostare il parametro `CdcStartPosition` API DMS su questo valore

quando si crea l'attività CDC per avviare la replica in questo punto iniziale per l'origine PostgreSQL. Per ulteriori informazioni sull'utilizzo dell'AWS CLI per creare quest'attività CDC, consulta [Abilitazione del CDC con un' AWS istanza DB PostgreSQL gestita con AWS DMS](#).

Oracle

Un numero di modifica sistema (SCN, System Change Number) è un timestamp interno logico utilizzato dai database Oracle. Gli SCN ordinano gli eventi che si verificano all'interno del database, operazione necessaria per soddisfare le proprietà ACID di una transazione. I database Oracle utilizzano gli SCN per contrassegnare la posizione in cui tutte le modifiche sono state scritte su disco in modo che un'operazione di ripristino non applichi modifiche già scritte. Oracle utilizza inoltre gli SCN per contrassegnare il punto in cui non esiste alcuna operazione redo per un set di dati in modo che sia possibile arrestare il ripristino.

Per ottenere l'SCN corrente in un database Oracle, esegui il comando seguente.

```
SELECT CURRENT_SCN FROM V$DATABASE
```

Se usi l'SCN o il timestamp per avviare un'attività di CDC, perdi i risultati di tutte le transazioni aperte e non riesci a migrare i risultati. Le transazioni aperte sono transazioni avviate prima della posizione di inizio dell'attività e confermate dopo la posizione di inizio dell'attività. È possibile identificare l'SCN e il timestamp per avviare un'attività di CDC in un punto che includa tutte le transazioni aperte. Per ulteriori informazioni, consulta [Transactions](#) nella documentazione online di Oracle. Con la versione 3.5.1 e successive, AWS DMS supporta le transazioni aperte per un'attività di sola CDC utilizzando l'impostazione dell'endpoint `openTransactionWindow` se si utilizza l'SCN o il timestamp per avviare l'attività.

Quando si utilizza l'impostazione `openTransactionWindow`, è necessario fornire la finestra, espressa in minuti, per gestire le transazioni aperte. AWS DMS sposta la posizione di acquisizione e trova la nuova posizione per avviare l'acquisizione dei dati. AWS DMS utilizza la nuova posizione iniziale per scansionare tutte le transazioni aperte dai log redo Oracle richiesti o dai log redo archiviati.

MySQL

Prima del rilascio di MySQL versione 5.6.3, il numero di sequenza di log (LSN, Log Sequence Number) per MySQL era un valore intero a 4 byte senza segno. In MySQL versione 5.6.3, quando il limite delle dimensioni del file di log redo aumentava da 4 GB a 512 GB, il valore LSN diventava un numero intero a 8 byte senza segno. L'aumento riflette il fatto che erano richiesti

byte aggiuntivi per archiviare informazioni di dimensioni ulteriori. Le applicazioni create su MySQL 5.6.3 o versioni successive che utilizzano valori LSN devono utilizzare variabili a 64 bit piuttosto che a 32 bit per archiviare e confrontare i valori LSN. Per ulteriori informazioni sui valori LSN MySQL, consulta la [documentazione di MySQL](#).

Per ottenere il valore LSN corrente in un database MySQL, esegui il comando seguente.

```
mysql> show master status;
```

La query restituisce un nome file binlog, la posizione e diversi altri valori. Il punto di inizio nativo CDC è una combinazione del nome del file binlog e della posizione, ad esempio `mysql-bin-change.log.000024:373`. In questo esempio, `mysql-bin-change.log.000024` è il nome del file binlog e `373` è la posizione in cui AWS DMS deve iniziare ad acquisire le modifiche.

Utilizzo di un checkpoint come punto di inizio CDC

Un'attività di replica continua migra le modifiche e AWS DMS memorizza nella cache le informazioni di checkpoint specifiche per AWS DMS di tanto in tanto. Il checkpoint che AWS DMS crea contiene le informazioni necessarie affinché il motore di replica conosca il punto di ripristino per il flusso di modifica. Puoi utilizzare il checkpoint per tornare indietro nella cronologia delle modifiche e ripristinare un'attività di migrazione non riuscita. Puoi anche utilizzare un checkpoint per iniziare un'altra attività di replica continua per un'altra destinazione in qualunque momento.

Puoi ottenere le informazioni di checkpoint in uno dei seguenti tre modi:

- Esegui l'operazione API `DescribeReplicationTasks` e visualizza i risultati. Puoi filtrare le informazioni in base all'attività e cercare il checkpoint. Puoi recuperare il checkpoint più recente quando l'attività è in stato arrestato o non riuscito. Queste informazioni vengono perse in caso di eliminazione dell'attività.
- Visualizza la tabella dei metadati denominata `awsdms_txn_state` sull'istanza di destinazione. Puoi eseguire query alla tabella per ottenere le informazioni sul checkpoint. Per creare la tabella dei metadati, imposta il parametro `TaskRecoveryTableEnabled` su `Yes` al momento della creazione di un'attività. Questa impostazione consente a AWS DMS di scrivere in modo continuo le informazioni sul checkpoint nella tabella dei metadati di destinazione. Queste informazioni vengono perse in caso di eliminazione di un'attività.

Di seguito è riportato un esempio di checkpoint nella tabella dei metadati:

```
checkpoint:V1#34#00000132/0F000E48#0#0#*#0#121
```

- Dal riquadro di navigazione, scegli Attività di migrazione del database e seleziona l'attività principale dall'elenco visualizzato nella pagina Attività di migrazione del database. Viene visualizzata la pagina dell'attività principale che mostra i dettagli della panoramica. Individuare il valore del checkpoint in Change data capture (CDC), posizione iniziale Change Data Capture (CDC) e punto di ripristino Change Data Capture (CDC). Il valore di checkpoint è simile all'esempio seguente:

```
checkpoint:V1#1#000004AF/B00000D0#0#0#*#0#0
```

Arresto di un'attività in un punto temporale di commit o del server

Con l'introduzione dei punti di inizio nativi CDC, AWS DMS può inoltre arrestare un'attività nei seguenti punti:

- Un'ora di commit sull'origine
- Un'ora del server sull'istanza di replica

Puoi modificare un'attività e impostare un'ora in UTC per eseguire l'arresto in base alle esigenze. L'attività viene arrestata automaticamente in base all'ora di commit o del server che hai impostato. Oppure, se conosci un'ora appropriata per arrestare l'attività di migrazione al momento della creazione dell'attività, puoi impostare un'ora di arresto quando crei l'attività.

Note

L'inizializzazione di tutte le risorse la prima volta che si avvia una nuova replica AWS DMS serverless può richiedere fino a 40 minuti. Tieni presente che l'opzione `server_time` è applicabile solo dopo il completamento dell'inizializzazione delle risorse.

Esecuzione della replica bidirezionale

È possibile utilizzare le attività AWS DMS per eseguire la replica bidirezionale tra due sistemi. Nella replica bidirezionale, si replicano i dati dalla stessa tabella (o insieme di tabelle) tra due sistemi in entrambe le direzioni.

Ad esempio, è possibile copiare una tabella EMPLOYEE dal database A al database B e replicare le modifiche alla tabella dal database A al database B. È inoltre possibile replicare le modifiche alla tabella EMPLOYEE dal database B al database A. Pertanto, si sta eseguendo la replica bidirezionale.

Note

La replica AWS DMS bidirezionale non è intesa come una soluzione multimaster completa, che include un nodo primario, la risoluzione dei conflitti e così via.

Utilizzare la replica bidirezionale per situazioni in cui i dati su nodi diversi siano segregati operativamente. In altre parole, si supponga di avere un elemento di dati modificato da un'applicazione che opera sul nodo A e che il nodo A esegua la replica bidirezionale con il nodo B. Tale elemento di dati sul nodo A non viene mai modificato da nessuna applicazione che opera sul nodo B.

AWS DMS supporta la replica bidirezionale su questi motori di database:

- Oracle
- SQL Server
- MySQL
- PostgreSQL
- Amazon Aurora edizione compatibile con MySQL
- Amazon Aurora edizione compatibile con PostgreSQL

Creazione di attività di replica bidirezionale

Per abilitare la replica AWS DMS bidirezionale, configurare gli endpoint di origine e di destinazione per entrambi i database (A e B). Ad esempio, configurare un endpoint di origine per il database A, un endpoint di origine per il database B, un endpoint di destinazione per il database A e un endpoint di destinazione per il database B.

Quindi creare due attività: un'attività per l'origine A per spostare i dati nella destinazione B e un'altra attività per l'origine B per spostare i dati nella destinazione A. Inoltre, assicurarsi che ogni attività sia configurata con la prevenzione del loopback. Ciò impedisce che modifiche identiche vengano applicate alle destinazioni di entrambe le attività, danneggiando così i dati di almeno una di esse. Per ulteriori informazioni, consulta [Prevenire il loopback](#).

Per un approccio più semplice, iniziare con set di dati identici nel database A e nel database B. Quindi creare due attività solo CDC, un'attività per replicare i dati da A a B e un'altra attività per replicare i dati da B ad A.

Per utilizzare AWS DMS per creare l'istanza di un nuovo set di dati (database) sul nodo B dal nodo A, effettuare le operazioni seguenti:

1. Utilizzare un'attività di caricamento completo e CDC per spostare i dati dal database A a B. Assicurarsi che nessuna applicazione stia modificando i dati nel database B durante questo periodo.
2. Quando il caricamento completo è completo e prima che le applicazioni siano autorizzate a modificare i dati nel database B, prendere nota dell'ora o della posizione di avvio del CDC del database B. Per istruzioni, vedere [Esecuzione della replica a partire da un punto di inizio CDC](#).
3. Creare un'attività solo CDC che sposta i dati dal database B ad A utilizzando l'ora di inizio o la posizione di avvio del CDC.

Note

Solo un'attività in una coppia bidirezionale può essere a caricamento completo e CDC.

Prevenire il loopback

Per comprendere come prevenite il loopback, si supponga che in un'attività T1 AWS DMS legga i log delle modifiche dal database di origine A e applichi le modifiche al database di destinazione B.

Successivamente, una seconda attività, T2, legge i log delle modifiche dal database di origine B e li applica nuovamente al database di destinazione A. Prima di T2, DMS deve assicurarsi che le stesse modifiche apportate al database di destinazione B dal database di origine A non siano apportate al database di origine A. In altre parole, DMS deve assicurarsi che queste modifiche non vengano riecheggiate (in loop) al database di destinazione A. In caso contrario, i dati nel database A possono essere danneggiati.

Per evitare il loopback delle modifiche, aggiungere le seguenti impostazioni di attività a ogni attività di replica bidirezionale. In questo modo si assicura che il danneggiamento dei dati di loopback non si verifichi in entrambe le direzioni.

```
{  
  . . .  
  
  "LoopbackPreventionSettings": {  
    "EnableLoopbackPrevention": Boolean,
```

```

    "SourceSchema": String,
    "TargetSchema": String
  },
  . . .
}
```

Le impostazioni dell'attività `LoopbackPreventionSettings` determinano se una transazione è nuova o un'eco dall'attività di replica opposta. Quando AWS DMS applica una transazione a un database di destinazione, aggiorna una tabella DMS (`awsdms_loopback_prevention`) con un'indicazione della modifica. Prima di applicare ciascuna transazione a una destinazione, DMS ignora qualsiasi transazione che includa un riferimento a questa tabella `awsdms_loopback_prevention`. Pertanto, non applica la modifica.

Includere queste impostazioni di attività in ogni attività di replica in una coppia bidirezionale. Queste impostazioni consentono la prevenzione del loopback. Specificano inoltre lo schema per ogni database di origine e di destinazione nell'attività che include la tabella `awsdms_loopback_prevention` per ciascun endpoint.

Per consentire a ciascuna attività di identificare tale eco e scartarla, impostare `EnableLoopbackPrevention` su `true`. Per specificare uno schema all'origine che includa `awsdms_loopback_prevention`, impostare `SourceSchema` sul nome dello schema nel database di origine. Per specificare uno schema nella destinazione che include la stessa tabella, impostare `TargetSchema` il nome dello schema nel database di destinazione.

Nell'esempio seguente, le impostazioni `SourceSchema` e `TargetSchema` per un'attività di replica T1 e la relativa attività di replica opposta T2 sono specificate con impostazioni opposte.

Le impostazioni per l'attività T1 sono le seguenti.

```

{
  . . .

  "LoopbackPreventionSettings": {
    "EnableLoopbackPrevention": true,
    "SourceSchema": "LOOP-DATA",
    "TargetSchema": "loop-data"
  },
  . . .
}
```

```
}
```

Le impostazioni per l'attività opposta T2 sono le seguenti.

```
{  
  . . .  
  "LoopbackPreventionSettings": {  
    "EnableLoopbackPrevention": true,  
    "SourceSchema": "loop-data",  
    "TargetSchema": "LOOP-DATA"  
  },  
  . . .  
}
```

Note

Quando si utilizza l'AWS CLI, utilizzare solo i comandi `create-replication-task` o `modify-replication-task` per configurare `LoopbackPreventionSettings` nelle attività di replica bidirezionali.

Limitazioni della replica bidirezionale

La replica bidirezionale per AWS DMS presenta le seguenti limitazioni:

- La prevenzione loopback tiene traccia solo delle istruzioni del linguaggio di manipolazione dei dati (DML). AWS DMS non supporta la prevenzione del loopback del linguaggio di definizione dei dati (DDL). A tale scopo, configurare una delle attività in una coppia bidirezionale per filtrare le istruzioni DDL.
- Le attività che utilizzano la prevenzione del loopback non supportano il commit delle modifiche nei batch. Per configurare un'attività con la prevenzione del loopback, assicurarsi di impostare `BatchApplyEnabled` su `false`.
- La replica bidirezionale DMS non include il rilevamento o la risoluzione dei conflitti. Per rilevare le incongruenze dei dati, utilizzare la convalida dei dati su entrambe le attività.

Modifica di un'attività

Puoi modificare un'attività se devi modificare le impostazioni delle attività, la mappatura delle tabelle o altre impostazioni. È inoltre possibile abilitare ed eseguire le valutazioni di pre-migrazione prima di eseguire l'attività modificata. Puoi modificare un'attività nella console selezionandola e scegliendo Modifica. Puoi inoltre utilizzare il comando CLI o l'operazione API [ModifyReplicationTask](#).

Per la modifica di un'attività vi sono alcune limitazioni. Questi sono i seguenti:

- Non puoi modificare l'endpoint di origine o di destinazione di un'attività.
- Non puoi modificare il tipo di migrazione di un'attività.
- Per essere modificate, le attività eseguite devono avere lo stato Arrestato o Non riuscito.

Spostamento di un'attività

È possibile spostare un'attività in un'istanza di replica diversa quando una delle seguenti situazioni si applica al caso d'uso in questione.

- Utilizzi un'istanza di un determinato tipo e desideri passare a un tipo di istanza diverso.
- L'istanza corrente è sovraccaricata da molte attività di replica e desideri suddividere il carico su più istanze.
- L'archiviazione dell'istanza è piena e desideri spostare le attività da quell'istanza a un'istanza più potente in alternativa al dimensionamento dello spazio di archiviazione o del calcolo.
- Desideri utilizzare una funzionalità appena rilasciata di AWS DMS, ma non vuoi creare una nuova attività e riavviare la migrazione. Preferisci invece avviare un'istanza di replica con una nuova versione di AWS DMS che supporti la funzionalità e spostare l'attività esistente su quell'istanza.

Puoi spostare un'attività nella console selezionandola e scegliendo Sposta. Per spostare l'attività puoi anche utilizzare il comando CLI o l'operazione API `MoveReplicationTask`. È possibile spostare un'attività che ha un motore di database come endpoint di destinazione.

Assicurati che l'istanza di replica di destinazione disponga di spazio di archiviazione sufficiente per ospitare l'attività che viene spostata. Altrimenti, dimensiona l'archiviazione per liberare spazio per l'istanza di replica di destinazione prima di spostare l'attività.

Inoltre, assicurati che l'istanza di replica di destinazione sia creata con la stessa versione del motore AWS DMS o una versione successiva dell'istanza di replica corrente.

Note

- Non è possibile spostare un'attività nella stessa istanza di replica in cui si trova attualmente.
- Non è possibile modificare le impostazioni di un'attività durante uno spostamento.
- Un'attività che hai eseguito deve avere lo stato Interrotto, Non riuscito o Spostamento non riuscito per poterla spostare.

Esistono due stati di attività relativi allo spostamento di un'attività DMS: Spostamento in corso e Spostamento non riuscito. Per ulteriori informazioni sullo stato delle attività, consulta [Stato dell'attività](#).

Dopo aver spostato un'attività, è possibile abilitare ed eseguire valutazioni di pre-migrazione per verificare eventuali problemi preclusivi prima di eseguire l'attività spostata.

Ricaricamento delle tabelle durante un'attività

Mentre un'attività è in esecuzione, puoi ricaricare una tabella di database di destinazione utilizzando i dati provenienti dall'origine. Potresti voler ricaricare una tabella se, durante l'attività, si verifica un errore o i dati vengono modificati a causa di operazioni di partizione (ad esempio, quando si utilizza Oracle). Puoi ricaricare fino a 10 tabelle da un'attività.

Il ricaricamento delle tabelle non interrompe l'attività.

Per ricaricare una tabella, si applicano le condizioni seguenti:

- L'attività deve essere in esecuzione.
- Il metodo di migrazione per l'attività deve essere il caricamento completo o il caricamento completo con CDC.
- Le tabelle duplicate non sono consentite.
- AWS DMS mantiene la definizione di tabella letta in precedenza e non la ricrea durante l'operazione di ricarica. Tutte le istruzioni DDL, quali ALTER TABLE ADD COLUMN o DROP COLUMN, che vengono effettuate sulla tabella prima che questa venga ricaricata possono causare l'errore dell'operazione di ricaricamento.

Note

DMS applica l'impostazione `TargetTablePrepMode` prima di ricaricare la tabella. Se si imposta `TargetTablePrepMode` su `DO_NOTHING`, è necessario prima troncare manualmente la tabella.

AWS Management Console

Per ricaricare una tabella mediante la console AWS DMS

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Scegliere Tasks (Attività) nel riquadro di navigazione.
3. Scegliere l'attività in esecuzione contenente la tabella da ricaricare.
4. Selezionare la scheda Table Statistics (Statistiche tabella).

The screenshot shows the AWS DMS console interface. At the top, there are buttons for 'Create task', 'Assess', 'Modify', 'Start/Resume', 'Stop', and 'Delete'. Below these is a search filter 'Filter: Q Filter'. A table lists tasks with columns for ID, Status, Source, Target, and Type. One task, 'move-data', is highlighted and has a status of 'Running'.

Below the task list, the 'move-data' task is selected, and the 'Table statistics' tab is active. This tab contains buttons for 'Revalidate' and 'Reload table data', with the latter circled in red. Below the buttons is another search filter 'Filter: Q Filter' and a table showing table statistics with columns for Schema, Table, Load State, Inserts, Deletes, Updates, DDLs, and Full Load.

Schema	Table	Load State	Inserts	Deletes	Updates	DDLs	Full Load
employees	departments	Table completed	0	0	0	0	9
employees	dept_emp	Table completed	0	0	0	0	331,6
employees	dept_manager	Table completed	0	0	0	0	24

- Scegliere la tabella da ricaricare. Se l'attività non è più in esecuzione, non è possibile ricaricare la tabella.
- Scegliere Reload table data (Carica di nuovo i dati della tabella).

Quando AWS DMS si prepara a ricaricare una tabella, la console cambia lo stato della tabella in Table is being reloaded (La tabella è in fase di caricamento).

Utilizzo della mappatura delle tabelle per specificare le impostazioni delle attività

La mappatura delle tabelle utilizza diversi tipi di regole per specificare l'origine dati, lo schema di origine, i dati e le eventuali trasformazioni che devono verificarsi durante l'attività. Puoi utilizzare la

mappatura delle tabelle per specificare singole tabelle in un database per eseguire la migrazione e lo schema da utilizzare per la migrazione.

Quando si utilizza la mappatura delle tabelle, è possibile utilizzare i filtri per specificare i dati che si desidera replicare dalle colonne delle tabelle. Inoltre è possibile utilizzare le trasformazioni per modificare schemi, tabelle o viste selezionati prima che vengano scritti nel database di destinazione.

Argomenti

- [Specifica della selezione delle tabelle e delle regole di trasformazione dalla console](#)
- [Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON](#)
- [Operazioni e regole di selezione](#)
- [Caratteri jolly nella mappatura delle tabelle](#)
- [Operazioni e regole di trasformazione](#)
- [Utilizzo delle espressioni delle regole di trasformazione per definire il contenuto delle colonne](#)
- [Regole e operazioni delle impostazioni di tabella e raccolta](#)

Note

Quando si utilizza la mappatura delle tabelle per un endpoint di origine MongoDB, è possibile usare i filtri per specificare i dati da replicare e indicare un nome di database al posto di `schema_name`. In alternativa, puoi usare il valore "%" predefinito.

Specifica della selezione delle tabelle e delle regole di trasformazione dalla console

È possibile utilizzarli AWS Management Console per eseguire la mappatura delle tabelle, inclusa la specificazione della selezione e delle trasformazioni delle tabelle. Nella console, utilizza la sezione Where (Dove) per specificare lo schema, la tabella e l'operazione (includere o escludere). Utilizza la sezione Filter (Filtro) per specificare il nome della colonna in una tabella e le condizioni che desideri applicare a un'attività di replica. Insieme, queste due operazioni creano una regola di selezione.

Puoi includere trasformazioni in una mappatura delle tabelle dopo aver specificato almeno una regola di selezione. Puoi utilizzare le trasformazioni per rinominare uno schema o una tabella, aggiungere un prefisso o un suffisso a uno schema o a una tabella oppure rimuovere la colonna di una tabella.

 Note

AWS DMS non supporta più di una regola di trasformazione per livello di schema, livello di tabella o livello di colonna.

Nella procedura seguente viene illustrato come configurare le regole di selezione in base a una tabella chiamata **Customers** in uno schema denominato **EntertainmentAgencySample**.

Per specificare una selezione delle tabelle, criteri di filtro e trasformazioni mediante la console

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Nella pagina Dashboard scegli Attività di migrazione del database.
3. Scegli Create Task (Crea attività).
4. Nella sezione Configurazione dell'attività inserisci le informazioni sull'attività, tra cui Identificativo dell'attività, Istanza di replica, Endpoint del database di origine, Endpoint del database di destinazione e Tipo di migrazione.

DMS > Database migration tasks > Create database migration task

Create database migration task

Task configuration

Task identifier

Replication instance

Source database endpoint

Target database endpoint

Migration type [Info](#)

5. Nella sezione Mappatura delle tabelle scegli il nome dello schema e quello della tabella. Quando specifichi il nome dello schema o della tabella, puoi utilizzare "%" come valore di carattere jolly. Per informazioni sugli altri caratteri jolly che puoi usare, consulta [the section called "Caratteri jolly nella mappatura delle tabelle"](#). Specifica l'azione da eseguire, per includere o escludere i dati definiti dal filtro.

Table mappings

Editing mode [Info](#)

Wizard
You can enter only a subset of the available table mappings.

JSON editor
You can enter all available table mappings directly in JSON format.

Specify at least one selection rule with an include action. After you do this, you can add one or more transformation rules.

▼ Selection rules

Choose the schema and/or tables you want to include with, or exclude from, your migration task. [Info](#) **Add new selection rule**

▼ where schema name is like 'MySchema' and table name is like '%', include

Schema
Enter a schema

Schema name
Use the % character as a wildcard
MySchema

Table name
Use the % character as a wildcard
%

Action
Choose "Include" to migrate your selected objects, or "Exclude" to ignore them during the migration.
Include

6. Specifica le informazioni di filtro utilizzando i link **Add column filter** (Aggiungi filtro colonna) e **Add condition** (Aggiungi condizione).
 - a. Scegli **Aggiungi filtro colonna** per specificare una colonna e le condizioni.
 - b. Scegli **Add condition** (Aggiungi condizione) per aggiungere condizioni aggiuntive.

L'esempio seguente mostra un filtro per la tabella **Customers** che include **AgencyIDs** tra **01** e **85**.

Source filters [Info](#) **Add column filter**

▼ Column filter 1

Column name
AgencyId

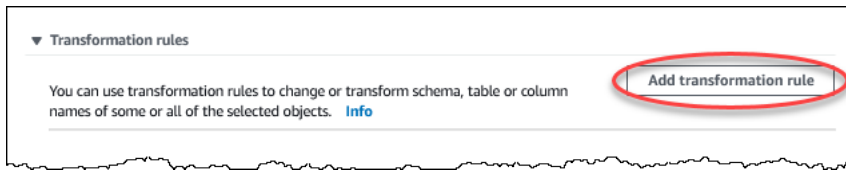
Condition 1
Equal to or between two values

01

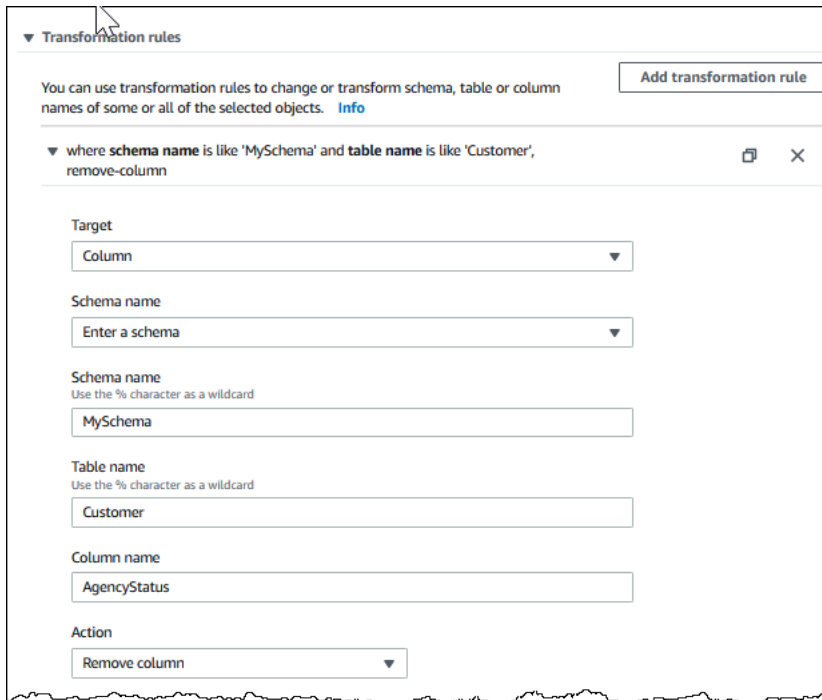
85

Add condition

7. Dopo aver creato le selezioni desiderate, scegli **Aggiungi nuova regola di selezione**.
8. Dopo aver creato almeno una regola di selezione, puoi aggiungere una trasformazione all'attività. Scegli **Add transformation rule** (Aggiungi regola di trasformazione).



- Scegli la destinazione che desideri trasformare, quindi immetti le informazioni aggiuntive richieste. L'esempio seguente mostra una trasformazione che elimina la colonna **AgencyStatus** dalla tabella **Customer**.



- Scegli Add transformation rule (Aggiungi regola di trasformazione).
- Scegli Create task (Crea attività).

Note

AWS DMS non supporta più di una regola di trasformazione per livello di schema o per livello di tabella.

Specifica della selezione delle tabelle e delle regole di trasformazione tramite JSON

Per specificare le mappature delle tabelle che si desidera applicare durante la migrazione, è possibile creare un file JSON. Se si crea un'attività di migrazione utilizzando la console, è possibile cercare

questo file JSON o immetterlo direttamente nella casella di mappatura delle tabelle. Se si utilizza la CLI o l'API per eseguire le migrazioni, è possibile specificare questo file utilizzando il parametro `TableMappings` dell'operazione API `CreateReplicationTask` o `ModifyReplicationTask`.

AWS DMS può elaborare solo file JSON di mappatura delle tabelle con dimensioni fino a 2 MB. Si consiglia di mantenere la dimensione del file JSON della regola di mappatura al di sotto del limite di 2 MB durante l'utilizzo di attività DMS. In questo modo si evitano errori imprevisti durante la creazione o la modifica delle attività. Quando un file di regole di mappatura supera il limite di 2 MB, si consiglia di suddividere le tabelle tra più attività per ridurre le dimensioni del file delle regole di mappatura in modo che rimanga al di sotto di questo limite.

Puoi specificare le tabelle, le viste e gli schemi da utilizzare. Puoi anche eseguire trasformazioni di tabelle, viste e schemi e specificare le impostazioni per il modo in cui AWS DMS carica singole tabelle e viste. Puoi creare regole di mappatura delle tabelle per queste opzioni utilizzando i seguenti tipi di regole:

- Regole `selection`: identificano i tipi e i nomi delle viste, degli schemi e delle tabelle di origine da caricare. Per ulteriori informazioni, consulta [Operazioni e regole di selezione](#).
- Regole `transformation`: specificano determinate modifiche o aggiunte a schemi e tabelle di origine particolari sull'origine prima del caricamento sulla destinazione. Per ulteriori informazioni, consulta [Operazioni e regole di trasformazione](#).

Inoltre, per definire il contenuto di colonne nuove ed esistenti, è possibile utilizzare un'espressione all'interno di una regola di trasformazione. Per ulteriori informazioni, consulta [Utilizzo delle espressioni delle regole di trasformazione per definire il contenuto delle colonne](#).

- Regole `table-settings`: specificano il modo in cui le attività DMS caricano i dati per le singole tabelle. Per ulteriori informazioni, consulta [Regole e operazioni delle impostazioni di tabella e raccolta](#).

Note

Per le destinazioni Amazon S3, è anche possibile aggiungere tag a oggetti S3 mappati a tabelle e schemi selezionati utilizzando il tipo di regola `post-processing` e l'azione della regola `add-tag`. Per ulteriori informazioni, consulta [Applicazione di tag agli oggetti Amazon S3](#).

Per le destinazioni seguenti, puoi specificare come e dove gli schemi e le tabelle selezionati vengono migrati verso la destinazione utilizzando il tipo di regola `object-mapping`:


- Amazon DynamoDB: per ulteriori informazioni, consulta [Utilizzo della mappatura degli oggetti per la migrazione dei dati a DynamoDB](#).
- Amazon Kinesis: per ulteriori informazioni, consulta [Utilizzo della mappatura degli oggetti per la migrazione dei dati a un flusso di dati Kinesis](#).
- Apache Kafka: per ulteriori informazioni, consulta [Utilizzo della mappatura degli oggetti per la migrazione dei dati in un argomento Kafka](#).

Operazioni e regole di selezione

Mediante la mappatura delle tabelle, puoi specificare quali tabelle, viste e schemi desideri utilizzare tramite regole e operazioni di selezione. Per le regole di mappatura delle tabelle che utilizzano il tipo di regola di selezione, sono applicabili i seguenti valori.

Parametro	Valori possibili	Descrizione
<code>rule-type</code>	<code>selection</code>	Una regola di selezione. Quando specifichi una mappatura delle tabelle, devi definire almeno una regola di selezione.
<code>rule-id</code>	Un valore numerico.	Un valore numerico univoco per identificare la regola.
<code>rule-name</code>	Un valore alfanumerico.	Un nome univoco per identificare la regola.
<code>rule-action</code>	<code>include, exclude, explicit</code>	Un valore che include o esclude l'oggetto o gli oggetti selezionati dalla regola. Se è specificato <code>explicit</code> , è possibile selezionare e includere solo un oggetto che corrisponde a una tabella e a uno schema specificati in modo esplicito.
<code>object-selector</code>	Un oggetto con i seguenti parametri:	Il nome di ogni schema e tabella o vista a cui si applica la regola. Puoi

Parametro	Valori possibili	Descrizione
	<ul style="list-style-type: none"> • <code>schema-name</code> : il nome dello schema. • <code>table-name</code> : il nome della tabella. • (Facoltativo) <code>table-type</code> : <code>table</code> <code>view</code> <code>all</code> per indicare se <code>table-name</code> si riferisce solo a tabelle, viste o sia a tabelle sia a viste. Il valore predefinito è <code>table</code>. <p>AWS DMS carica le visualizzazioni solo in un'attività a caricamento completo. Se hai solo attività di caricamento completo e di acquisizione dei dati di modifica (CDC), configura almeno un' <code>full-load-only</code> attività per caricare le visualizzazioni.</p> <p>Non tutti gli endpoint di destinazione accettano le visualizzazioni come fonte di replica, anche a pieno carico (ad esempio Amazon OpenSearch Service). Controlla le limitazioni dell'endpoint di destinazione.</p>	<p>anche specificare se una regola include solo tabelle, solo viste o sia tabelle sia viste. Se <code>rule-action</code> è <code>include</code> oppure <code>exclude</code>, puoi utilizzare il segno di percentuale "%" come carattere jolly per tutto o parte del valore del parametro <code>schema-name</code> e <code>table-name</code>. Per informazioni sugli altri caratteri jolly che puoi usare, consulta the section called "Caratteri jolly nella mappatura delle tabelle". Pertanto, è possibile mettere in corrispondenza questi elementi:</p> <ul style="list-style-type: none"> • Una singola tabella, vista o raccolta in un singolo schema • Una singola tabella, vista o raccolta in alcuni o tutti gli schemi • Alcune o tutte le tabelle e le viste in un singolo schema o le raccolte in un singolo database • Alcune o tutte le tabelle e le viste in alcuni o tutti gli schemi o le raccolte in alcuni o tutti i database <p>Se <code>rule-action</code> è <code>explicit</code>, puoi specificare solo il nome esatto di una tabella o una vista e del suo schema (senza caratteri jolly).</p> <p>Le origini supportate per le viste includono:</p> <ul style="list-style-type: none"> • Oracle • Microsoft SQL Server

Parametro	Valori possibili	Descrizione
		<ul style="list-style-type: none"> • PostgreSQL • IBM Db2 LUW • IBM Db2 z/OS • SAP Adaptive Server Enterprise (ASE) • MySQL • AURORA • AURORA serverless • MariaDB <div data-bbox="974 766 1507 1270" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 20px;"> <p> Note</p> <p>AWS DMS non carica mai una vista di origine in una vista di destinazione. Una vista di origine viene caricata in una tabella equivalente sulla destinazione con lo stesso nome della vista sull'origine.</p> </div> <p>Le origini supportate per i database contenenti raccolte sono:</p> <ul style="list-style-type: none"> • MongoDB • Amazon DocumentDB
load-order	Un integer positivo. Il valore massimo è 2.147.483.647.	La priorità per il caricamento delle tabelle e delle viste. Le tabelle e le viste con valori più alti vengono caricate per prime.

Parametro	Valori possibili	Descrizione
<code>filters</code>	Un array di oggetti .	Uno o più oggetti per filtrare l'origine . È possibile specificare i parametri di oggetti per filtrare una singola colonna nell'origine. Puoi specificare più oggetti per filtrare più colonne. Per ulteriori informazioni, consulta Utilizzo di filtri di origine .

Example Migrazione di tutte le tabelle in uno schema

Nell'esempio seguente viene eseguita la migrazione di tutte le tabelle da uno schema denominato Test nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      },
      "rule-action": "include"
    }
  ]
}
```

Example Migrazione di alcune tabelle in uno schema

Nell'esempio seguente viene eseguita la migrazione di tutte le tabelle tranne quelle che iniziano per DMS da uno schema denominato Test nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
```

```
    "rule-name": "1",
    "object-locator": {
      "schema-name": "Test",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "selection",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "Test",
      "table-name": "DMS%"
    },
    "rule-action": "exclude"
  }
]
}
```

Example Migrazione di una singola tabella specificata in un singolo schema

Nell'esempio seguente la tabella `Customer` viene migrata dallo schema `NewCust` nell'origine all'endpoint di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "NewCust",
        "table-name": "Customer"
      },
      "rule-action": "explicit"
    }
  ]
}
```

Note

È possibile selezionare esplicitamente più tabelle e schemi specificando più regole di selezione.

Example Migrazione di tabelle in un ordine impostato

Nell'esempio seguente vengono migrate due tabelle. La tabella `loadfirst` (con priorità 1) viene inizializzata prima della tabella. `loadsecond`

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "loadsecond"
      },
      "rule-action": "include",
      "load-order": "2"
    },
    {
      "rule-type": "selection",
      "rule-id": "2",
      "rule-name": "2",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "loadfirst"
      },
      "rule-action": "include",
      "load-order": "1"
    }
  ]
}
```


Note

load-order è applicabile per l'inizializzazione della tabella. Il caricamento di una tabella successiva non attende il completamento del caricamento della tabella precedente se MaxFullLoadSubTasks è maggiore di 1.

Example Migrazione di alcune viste in uno schema

L'esempio seguente esegue la migrazione di alcune viste da uno schema denominato Test nell'origine a tabelle equivalenti nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "2",
      "rule-name": "2",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "view_DMS%",
        "table-type": "view"
      },
      "rule-action": "include"
    }
  ]
}
```

Example Migrazione di tutte le tabelle e tutte le viste in uno schema

L'esempio seguente esegue la migrazione di tutte le tabelle e tutte le viste da uno schema denominato report nell'origine a tabelle equivalenti nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "3",
      "rule-name": "3",
      "object-locator": {
        "schema-name": "report",
```

```

        "table-name": "%",
        "table-type": "all"
    },
    "rule-action": "include"
}
]
}

```

Caratteri jolly nella mappatura delle tabelle

Questa sezione descrive i caratteri jolly che è possibile utilizzare per specificare il nomi dello schema e della tabella per la mappatura delle tabelle.

Carattere jolly	Corrispondenze
%	Zero o più caratteri
_	Un singolo personaggio
[_]	Un carattere di sottolineatura letterale
[ab]	Un set di caratteri. Ad esempio, [ab] corrisponde a 'a' o 'b'.
[a-d]	Una serie di personaggi. Ad esempio, [a-d] corrisponde a 'a', 'b', 'c' o 'd'.

Per gli endpoint di origine e di destinazione Oracle, è possibile utilizzare l'attributo aggiuntivo di connessione `escapeCharacter` per specificare un carattere di escape. Un carattere di escape consente di usare nelle espressioni un carattere jolly specificato come se non fosse un carattere wild. Ad esempio, `escapeCharacter=#` consente di utilizzare "#" per fare in modo che in un'espressione un carattere jolly agisca come un normale carattere, come in questo codice di esempio.

```

{
  "rules": [
    {

```

```
        "rule-type": "selection",
        "rule-id": "542485267",
        "rule-name": "542485267",
        "object-locator": { "schema-name": "R00T", "table-name": "TEST#_T%" },
        "rule-action": "include",
        "filters": []
    }
]
}
```

Qui, il carattere di escape '#' fa sì che il carattere jolly '_' si comporti come un carattere normale. AWS DMS seleziona le tabelle nello schema denominato R00T, dove ogni tabella ha un nome TEST_T come prefisso.

Operazioni e regole di trasformazione

Puoi utilizzare le operazioni di trasformazione per specificare le trasformazioni che desideri applicare alla tabella selezionata, allo schema selezionato o alla vista selezionata. Le regole di trasformazione sono opzionali.

Limitazioni

- Non è possibile applicare più di un'azione della regola di trasformazione allo stesso oggetto (schema, tabella, colonna, table-tablespace o index-tablespace). È possibile applicare diverse azioni delle regole di trasformazione a qualsiasi livello, purché ogni azione di trasformazione venga applicata a un oggetto diverso.
- I nomi di tabella e di colonna nelle regole di trasformazione rispettano la distinzione tra maiuscole e minuscole. Ad esempio, è necessario specificare in maiuscolo i nomi delle tabelle e delle colonne per un database Oracle o Db2.
- Le trasformazioni non sono supportate per i nomi di colonna nelle lingue con scrittura sinistrorsa.
- Le trasformazioni non possono essere eseguite su colonne che includono nel nome caratteri speciali (ad esempio #, \, /, -).
- L'unica trasformazione supportata per le colonne mappate a tipi di dati BLOB/CLOB consiste nel rilasciare la colonna sulla destinazione.
- AWS DMS non supporta la replica di due tabelle di origine in un'unica tabella di destinazione. AWS DMS replica i record da una tabella all'altra e da una colonna all'altra, in base alle regole di trasformazione dell'attività di replica. I nomi degli oggetti devono essere univoci per evitare sovrapposizioni.

Ad esempio, una tabella di origine ha una colonna denominata ID e la tabella di destinazione corrispondente ha una colonna preesistente denominata id. Se una regola utilizza un'istruzione ADD-COLUMN per aggiungere una nuova colonna chiamata id e un'istruzione SQLite per popolare la colonna con valori personalizzati, si crea un oggetto duplicato e ambiguo denominato id che non è supportato.

Valori

Per le regole di mappatura delle tabelle che utilizzano il tipo di regola di trasformazione, sono applicabili i seguenti valori.

Parametro	Valori possibili	Descrizione
rule-type	transformation	Un valore che applica la regola a ogni oggetto specificato dalla regola di selezione. Usa transformation a meno che non sia indicato altrimenti.
rule-id	Un valore numerico.	Un valore numerico univoco per identificare la regola. Se si specifica no più regole di trasformazione per lo stesso oggetto (schema, tabella, colonna, spazio tra tabelle o spazio tabellare indicizzato), AWS DMS applica la regola di trasformazione con l'id della regola inferiore.
rule-name	Un valore alfanumerico.	Un nome univoco per identificare la regola.
object-locator	Un oggetto con i seguenti parametri: <ul style="list-style-type: none"> schema-name : il nome dello schema. Per gli endpoint MongoDB e Amazon DocumentD 	Il nome di ogni schema, tabella o vista, spazio tabella di tabella e spazio tabella di indice e di colonna a cui si applica la regola. È possibile utilizzare il simbolo di percentuale "%" come carattere jolly per tutto o

Parametro	Valori possibili	Descrizione
	<p>B, questo è il nome del database che contiene un set di raccolte.</p> <ul style="list-style-type: none"> • <code>table-name</code> : il nome della tabella, della vista o della raccolta. • <code>table-tablespace-name</code> : il nome di uno spazio di tabella di una tabella esistente. • <code>index-tablespace-name</code> : il nome di uno spazio di tabella di un indice esistente. • <code>column-name</code> : il nome di una colonna esistente. • <code>data-type</code> : il nome di un tipo di dati di colonna esistente. 	<p>parte del valore di ciascun parametro <code>object-locator</code> , eccetto <code>data-type</code> . Pertanto, è possibile mettere in corrispondenza questi elementi:</p> <ul style="list-style-type: none"> • Una singola tabella o una singola vista in un singolo schema • Una singola tabella o una singola vista in alcuni o tutti gli schemi • Alcune o tutte le tabelle e tutte le viste in un singolo schema • Alcune o tutte le tabelle e tutte le viste in alcuni o tutti gli schemi • Una o più colonne nella tabella o nelle tabelle, nella vista o nelle viste e nello schema o negli schemi specificati. • Le colonne con un dato <code>data-type</code> quando vengono specificate più colonne. Per i possibili valori di <code>data-type</code> , consulta <code>data-type</code> descritto di seguito in questa tabella. <p>Inoltre, il parametro <code>table-tablespace-name</code> o <code>index-tablespace-name</code> è disponibile solo per la corrispondenza con un endpoint di origine Oracle. In una singola regola puoi specificare <code>table-tablespace-name</code> o <code>index-tablespace-name</code> , ma non entrambi. Pertanto, puoi</p>

Parametro	Valori possibili	Descrizione
		<p>mettere in corrispondenza ciascuno dei seguenti formati:</p> <ul style="list-style-type: none">• Uno, alcuni o tutti gli spazi tabella delle tabelle• Uno, alcuni o tutti gli spazi tabella degli indici

Parametro	Valori possibili	Descrizione
<code>rule-action</code>	<code>add-column</code> , <code>include-column</code> , <code>remove-column</code> <code>rename</code> <code>convert-lowercase</code> , <code>convert-upper</code> <code>uppercase</code> <code>add-prefix</code> , <code>remove-prefix</code> , <code>replace-prefix</code> <code>add-suffix</code> , <code>remove-suffix</code> , <code>replace-suffix</code> <code>define-primary-key</code> <code>change-data-type</code> <code>add-before-image-columns</code>	<p>La trasformazione che desideri applicare all'oggetto. Tutte le operazioni delle regole di trasformazione prevedono una distinzione tra lettere maiuscole e minuscole.</p> <p>Il valore <code>add-column</code> del parametro <code>rule-action</code> aggiunge una colonna a una tabella. Tuttavia, non è possibile aggiungere una nuova colonna con lo stesso nome di una colonna esistente della stessa tabella.</p> <p>Se utilizzato con i parametri <code>expression</code> e <code>data-type</code> , <code>add-column</code> specifica il valore dei nuovi dati di colonna.</p> <p>Il valore <code>change-data-type</code> per <code>rule-action</code> è disponibile solo per le destinazioni della regola <code>column</code>.</p> <p>Il valore <code>include-column</code> del parametro <code>rule-action</code> modifica la modalità della tabella in modo da eliminare tutte le colonne per impostazione predefinita e includere le colonne specificate. Nella destinazione vengono incluse più colonne richiamando più volte la regola <code>include-column</code> .</p> <p>Non puoi usare una regola <code>define-primary-key</code> quando include</p>

Parametro	Valori possibili	Descrizione
		<p>un carattere jolly (%) in un nome di schema o di tabella.</p> <p>Per un'attività esistente, le azioni delle regole di trasformazione che alterano lo schema della tabella di destinazione, ad esempio <code>remove-column</code>, <code>rename</code> o <code>add-prefix</code> non avranno effetto finché l'attività non viene riavviata. Se riprendi l'attività dopo aver aggiunto la regola di trasformazione, potresti notare un comportamento imprevisto o della colonna alterata, come i dati mancanti nella colonna. È necessario il riavvio dell'attività per garantire il corretto funzionamento della regola di trasformazione.</p>
<code>rule-target</code>	<code>schema</code> , <code>table</code> , <code>column</code> , <code>table-tablespace</code> , <code>index-tablespace</code>	<p>Il tipo di oggetto che stai trasformando.</p> <p>I valori <code>table-tablespace</code> e <code>index-tablespace</code> sono disponibili solo per un endpoint di destinazione Oracle.</p> <p>Assicurarsi di specificare un valore per il parametro specificato come parte del <code>object-locator</code>: il nome <code>table-tablespace-name</code> o <code>index-tablespace-name</code>.</p>
<code>value</code>	Un valore alfanumerico che segue le regole di denominazione per il tipo di destinazione.	Il nuovo valore per operazioni che richiedono input, ad esempio <code>rename</code> .

Parametro	Valori possibili	Descrizione
<code>old-value</code>	Un valore alfanumerico che segue le regole di denominazione per il tipo di destinazione.	Il vecchio valore per operazioni che richiedono la sostituzione, ad esempio <code>replace-prefix</code> .

Parametro	Valori possibili	Descrizione
data-type	<p>type: il tipo di dati da utilizzare se rule-action è add-column o il tipo di dati sostitutivo se rule-action è change-data-type .</p> <p>In alternativa, il nome del tipo di dati sostitutivo quando rule-action è change-data-type , il valore di column-name è "%" e un parametro data-type aggiuntivo per identificare il tipo di dati esistente è incluso in object-locator .</p> <p>AWS DMS supporta le trasformazioni dei tipi di dati delle colonne per i seguenti tipi di dati DMS: "bytes", "date", "time", "datetime", "int1", "int2", "int4", "int8", "numeric", "real4", "real8", "string", "uint1", "uint2", "uint4", "uint8", "wstring", "blob", "nclob", "clob", "boolean", "set", "list", "map", "tuple"</p> <p>precision : se la colonna aggiunta o il tipo di dati di sostituzione ha una precisione, un valore intero per specificare la precisione.</p> <p>scale: se la colonna aggiunta o il tipo di dati di sostituzione ha una scala, un valore intero o un valore di data e ora per specificare la scala.</p>	<p>Di seguito è riportato un esempio di un parametro data-type per specificare il tipo di dati esistente da sostituire.</p> <pre> { "rules": [{ "rule-type": "selection", "rule-id": "1", "rule-name": "1", "object-locator": { "schema-name": "%", "table-name": "%" }, "rule-action": "include" }, { "rule-type": "transformation", "rule-id": "2", "rule-name": "2", "rule-target": "column", "object-locator": { "schema-name": "test", "table-name": "table_t" }, "column-name": "col10", "rule-action": "change-data-type", "data-type": { "type": "string", "length": "4092", "scale": "" } }] } </pre>

Parametro	Valori possibili	Descrizione
	<code>length</code> : la lunghezza dei dati della nuova colonna (se utilizzata con <code>add-column</code>).	Qui, la colonna <code>col10</code> della tabella <code>table_t</code> viene modificata in base al tipo di dati <code>string</code> .

Parametro	Valori possibili	Descrizione
expression	Valore alfanumerico che segue la sintassi SQLite.	<p>Se utilizzato con <code>rule-action</code> impostato su <code>rename-schema</code>, il parametro <code>expression</code> specifica un nuovo schema. Se utilizzato con il <code>rule-action</code> impostato su <code>rename-table</code>, <code>expression</code> specifica una nuova tabella. Se utilizzato con <code>rule-action</code> impostato su <code>rename-column</code>, <code>expression</code> specifica un nuovo valore del nome di colonna.</p> <p>Se utilizzato con <code>rule-action</code> impostato su <code>add-column</code>, <code>expression</code> specifica i dati che costituiscono una nuova colonna.</p> <p>Tieni presente che per questo parametro sono supportate solo le espressioni. Gli operatori e i comandi non sono supportati.</p> <p>Per ulteriori informazioni sull'utilizzo delle espressioni per le regole di trasformazione, consulta Utilizzo delle espressioni delle regole di trasformazione per definire il contenuto delle colonne.</p> <p>Per ulteriori informazioni sulle espressioni SQLite, consulta Utilizzo delle funzioni SQLite per creare espressioni.</p>

Parametro	Valori possibili	Descrizione
<code>primary-key-def</code>	<p>Un oggetto con i seguenti parametri:</p> <ul style="list-style-type: none">• <code>name</code>: il nome di una nuova chiave primaria o di un indice univoco per la tabella o la vista.• (Facoltativo) <code>origin</code>: il tipo di chiave univoca per definire <code>primary-key</code> (l'impostazione predefinita) oppure <code>unique-index</code>.• <code>columns</code>: una matrice di stringhe che elenca i nomi delle colonne nell'ordine in cui vengono visualizzati nella chiave primaria o nell'indice univoco.	<p>Questo parametro può definire il nome, il tipo e il contenuto di una chiave univoca sulla tabella o sulla vista trasformata. Lo fa quando <code>rule-action</code> è impostato su <code>define-primary-key</code> e <code>rule-target</code> su <code>table</code>. Per impostazione predefinita, la chiave univoca viene definita come chiave primaria.</p>

Parametro	Valori possibili	Descrizione
<code>before-image-def</code>	<p>Un oggetto con i seguenti parametri:</p> <ul style="list-style-type: none"> <code>column-prefix</code> : valore anteposto al nome di una colonna. Il valore predefinito è <code>BI_</code>. <code>column-suffix</code> : valore aggiunto al nome della colonna. L'impostazione predefinita è vuota. <code>column-filter</code> : richiede uno dei seguenti valori: <code>pk-only</code> (predefinito), <code>non-lob</code> (facoltativo) e <code>all</code> (facoltativo). 	<p>Questo parametro definisce una convenzione di denominazione per identificare le colonne immagine precedente e specifica un filtro per identificare quali colonne di origine possono avere colonne immagine precedente create per esse sulla destinazione. È possibile specificare questo parametro quando <code>rule-action</code> è impostato su <code>add-before-image-columns</code> e <code>rule-target</code> su <code>column</code>.</p> <p>Non impostare sia <code>column-prefix</code> sia <code>column-suffix</code> sull'opzione per svuotare le stringhe.</p> <p>Per <code>column-filter</code>, selezionare:</p> <ul style="list-style-type: none"> <code>pk-only</code>: per aggiungere solo colonne che fanno parte delle chiavi primarie della tabella. <code>non-lob</code>: per aggiungere solo colonne non di tipo LOB. <code>all</code>: per aggiungere qualsiasi colonna con un valore dell'immagine precedente. <p>Per ulteriori informazioni sul supporto dell'immagine precedente per gli endpoint di destinazione AWS DMS, consulta:</p> <ul style="list-style-type: none"> Utilizzo di un'immagine precedente e per visualizzare i valori originali

Parametro	Valori possibili	Descrizione
		<p>delle righe CDC per un flusso di dati Kinesis come destinazione</p> <ul style="list-style-type: none">• Utilizzo di un'immagine precedent e per visualizzare i valori originali delle righe CDC per Apache Kafka come destinazione

Esempi

Example Assegnazione di un nuovo nome a uno schema

Nell'esempio seguente viene rinominato uno schema da Test nell'origine a Test1 nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-action": "rename",
      "rule-target": "schema",
      "object-locator": {
        "schema-name": "Test"
      },
      "value": "Test1"
    }
  ]
}
```

```
}
```

Example Rinominare una tabella

Nell'esempio seguente viene rinominata una tabella da Actor nell'origine a Actor1 nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-action": "rename",
      "rule-target": "table",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "Actor"
      },
      "value": "Actor1"
    }
  ]
}
```

Example Ridenominazione di una colonna

Nell'esempio seguente viene rinominata una colonna nella tabella Actor da first_name nell'origine a fname nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
```



```

    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "transformation",
    "rule-id": "4",
    "rule-name": "4",
    "rule-action": "rename",
    "rule-target": "column",
    "object-locator": {
      "schema-name": "test",
      "table-name": "Actor",
      "column-name": "first_name"
    },
    "value": "fname"
  }
]
}

```

Example Rinominare uno spazio tabella di tabella Oracle

L'esempio seguente rinomina lo spazio tabella di tabella denominato SetSpace per una tabella denominata Actor nell'origine Oracle in SceneTblSpace nell'endpoint Oracle di destinazione.

```

{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Play",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",

```

```

    "rule-id": "2",
    "rule-name": "2",
    "rule-action": "rename",
    "rule-target": "table-tablespace",
    "object-locator": {
      "schema-name": "Play",
      "table-name": "Actor",
      "table-tablespace-name": "SetSpace"
    },
    "value": "SceneTblSpace"
  }
]
}

```

Example Rinominare uno spazio tabella di indice Oracle

L'esempio seguente rinomina lo spazio tabella di indice denominato SetISpace per una tabella denominata Actor nell'origine Oracle in SceneIdxSpace nell'endpoint Oracle di destinazione.

```

{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Play",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-action": "rename",
      "rule-target": "table-tablespace",
      "object-locator": {
        "schema-name": "Play",
        "table-name": "Actor",
        "table-tablespace-name": "SetISpace"
      },
      "value": "SceneIdxSpace"
    }
  ]
}

```

```
    }  
  ]  
}
```

Example Aggiungere una colonna

Nell'esempio seguente viene aggiunta una colonna `datetime` alla tabella `Actor` nello schema `test`.

```
{  
  "rules": [  
    {  
      "rule-type": "selection",  
      "rule-id": "1",  
      "rule-name": "1",  
      "object-locator": {  
        "schema-name": "test",  
        "table-name": "%"  
      },  
      "rule-action": "include"  
    },  
    {  
      "rule-type": "transformation",  
      "rule-id": "2",  
      "rule-name": "2",  
      "rule-action": "add-column",  
      "rule-target": "column",  
      "object-locator": {  
        "schema-name": "test",  
        "table-name": "actor"  
      },  
      "value": "last_updated",  
      "data-type": {  
        "type": "datetime",  
        "precision": 6  
      }  
    }  
  ]  
}
```

Example Rimozione di una colonna

Nell'esempio seguente viene trasformata la tabella denominata `Actor` nell'origine per rimuovere da essa tutte le colonne che iniziano con i caratteri `col` nella destinazione.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "rule-action": "include"
  }, {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",
    "rule-action": "remove-column",
    "rule-target": "column",
    "object-locator": {
      "schema-name": "test",
      "table-name": "Actor",
      "column-name": "col%"
    }
  }
]
```

Example Conversione in minuscolo

Nell'esempio seguente viene convertito un nome di tabella da `ACTOR` nell'origine a `actor` nella destinazione.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    }
  },
```

```
"rule-action": "include"
}, {
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "convert-lowercase",
  "rule-target": "table",
  "object-locator": {
    "schema-name": "test",
    "table-name": "ACTOR"
  }
}]
}
```

Example Conversione in caratteri maiuscoli

Nell'esempio seguente vengono convertite tutte le colonne in tutte le tabelle e tutti gli schemi da caratteri minuscoli nell'origine a caratteri maiuscoli nella destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-action": "convert-uppercase",
      "rule-target": "column",
      "object-locator": {
        "schema-name": "%",
        "table-name": "%",
        "column-name": "%"
      }
    }
  ]
}
```

```

]
}

```

Example Aggiunta di un prefisso

Nell'esempio seguente tutte le tabelle nell'origine vengono trasformate con l'aggiunta del prefisso DMS_ nella destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "rule-action": "include"
  }, {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",
    "rule-action": "add-prefix",
    "rule-target": "table",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "value": "DMS_"
  }
]}

```

Example Sostituzione di un prefisso

Nell'esempio seguente tutte le colonne contenenti il prefisso Pre_ nell'origine vengono trasformate mediante la sostituzione del prefisso con NewPre_ nella destinazione.

```

{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",

```

```

        "rule-name": "1",
        "object-locator": {
            "schema-name": "test",
            "table-name": "%"
        },
        "rule-action": "include"
    },
    {
        "rule-type": "transformation",
        "rule-id": "2",
        "rule-name": "2",
        "rule-action": "replace-prefix",
        "rule-target": "column",
        "object-locator": {
            "schema-name": "%",
            "table-name": "%",
            "column-name": "%"
        },
        "value": "NewPre_",
        "old-value": "Pre_"
    }
]
}

```

Example Rimozione di un suffisso

Nell'esempio seguente tutte le tabelle nell'origine vengono trasformate con la rimozione del suffisso `_DMS` nella destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "%"
    },
    "rule-action": "include"
  }, {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",

```

```

"rule-action": "remove-suffix",
"rule-target": "table",
"object-locator": {
  "schema-name": "test",
  "table-name": "%"
},
"value": "_DMS"
}]
}

```

Example Definire una chiave primaria

L'esempio seguente definisce una chiave primaria denominata ITEM-primary-key su tre colonne della tabella ITEM migrata nell'endpoint di destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "inventory",
      "table-name": "%"
    },
    "rule-action": "include"
  }, {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",
    "rule-action": "define-primary-key",
    "rule-target": "table",
    "object-locator": {
      "schema-name": "inventory",
      "table-name": "ITEM"
    },
    "primary-key-def": {
      "name": "ITEM-primary-key",
      "columns": [
        "ITEM-NAME",
        "BOM-MODEL-NUM",
        "BOM-PART-NUM"
      ]
    }
  }
]
}

```



```
  ]]  
}
```

Example Definire un indice univoco

L'esempio seguente definisce un indice univoco denominato `ITEM-unique-idx` su tre colonne della tabella `ITEM` migrata verso l'endpoint di destinazione.

```
{  
  "rules": [{  
    "rule-type": "selection",  
    "rule-id": "1",  
    "rule-name": "1",  
    "object-locator": {  
      "schema-name": "inventory",  
      "table-name": "%"  
    },  
    "rule-action": "include"  
  }, {  
    "rule-type": "transformation",  
    "rule-id": "2",  
    "rule-name": "2",  
    "rule-action": "define-primary-key",  
    "rule-target": "table",  
    "object-locator": {  
      "schema-name": "inventory",  
      "table-name": "ITEM"  
    },  
    "primary-key-def": {  
      "name": "ITEM-unique-idx",  
      "origin": "unique-index",  
      "columns": [  
        "ITEM-NAME",  
        "BOM-MODEL-NUM",  
        "BOM-PART-NUM"  
      ]  
    }  
  }  
}]  
}
```

Example Modifica del tipo di dati della colonna di destinazione

Nell'esempio seguente viene modificato il tipo di dati di una colonna di destinazione denominata SALE_AMOUNT da un tipo di dati esistente su int8.

```
{
  "rule-type": "transformation",
  "rule-id": "1",
  "rule-name": "RuleName 1",
  "rule-action": "change-data-type",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "dbo",
    "table-name": "dms",
    "column-name": "SALE_AMOUNT"
  },
  "data-type": {
    "type": "int8"
  }
}
```

Example Aggiungere una colonna dell'immagine precedente

Per una colonna di origine denominata emp_no, la regola di trasformazione nell'esempio seguente aggiunge una nuova colonna denominata BI_emp_no nella destinazione.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "transformation",
    "rule-id": "2",
    "rule-name": "2",
    "rule-target": "column",
    "object-locator": {
```

```
"schema-name": "%",
"table-name": "employees"
},
"rule-action": "add-before-image-columns",
"before-image-def": {
  "column-prefix": "BI_",
  "column-suffix": "",
  "column-filter": "pk-only"
}
}
]
}
```

Qui, l'istruzione seguente popola una colonna BI_emp_no nella riga corrispondente con 1.

```
UPDATE employees SET emp_no = 3 WHERE BI_emp_no = 1;
```

Quando si scrivono aggiornamenti CDC su AWS DMS destinazioni supportate, la BI_emp_no colonna consente di indicare quali righe hanno valori aggiornati nella colonna. emp_no

Utilizzo delle espressioni delle regole di trasformazione per definire il contenuto delle colonne

Per definire il contenuto per colonne nuove ed esistenti, è possibile utilizzare un'espressione all'interno di una regola di trasformazione. Ad esempio, utilizzando le espressioni è possibile aggiungere una colonna o replicare intestazioni di tabella di origine a una destinazione. È inoltre possibile utilizzare le espressioni per contrassegnare i record nelle tabelle di destinazione come inseriti, aggiornati o eliminati nell'origine.

Argomenti

- [Aggiunta di una colonna mediante un'espressione](#)
- [Contrassegno dei record di destinazione mediante un'espressione](#)
- [Replica delle intestazioni della tabella di origine mediante espressioni](#)
- [Utilizzo delle funzioni SQLite per creare espressioni](#)
- [Aggiunta di metadati a una tabella di destinazione utilizzando espressioni](#)

Aggiunta di una colonna mediante un'espressione

Per aggiungere colonne alle tabelle utilizzando un'espressione in una regola di trasformazione, utilizzare un'azione della regola `add-column` e una destinazione della regola `column`.

Nell'esempio seguente viene aggiunta una nuova colonna alla tabella `ITEM`. Imposta il nome della nuova colonna su `FULL_NAME`, con un tipo di dati di `string`, lungo 50 caratteri. L'espressione concatena i valori di due colonne esistenti `FIRST_NAME` e `LAST_NAME`, da valutare per `FULL_NAME`. `schema-name`, `table-name` e i parametri di espressione si riferiscono agli oggetti nella tabella del database di origine. `value` e il blocco `data-type` si riferiscono agli oggetti nella tabella del database di destinazione.

```
{
  "rules": [
    {
      "rule-type": "selection",
      "rule-id": "1",
      "rule-name": "1",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "%"
      },
      "rule-action": "include"
    },
    {
      "rule-type": "transformation",
      "rule-id": "2",
      "rule-name": "2",
      "rule-action": "add-column",
      "rule-target": "column",
      "object-locator": {
        "schema-name": "Test",
        "table-name": "ITEM"
      },
      "value": "FULL_NAME",
      "expression": "$FIRST_NAME||'_'||$LAST_NAME",
      "data-type": {
        "type": "string",
        "length": 50
      }
    }
  ]
}
```

```
}
```

Contrassegno dei record di destinazione mediante un'espressione

Per contrassegnare i record nelle tabelle di destinazione come inseriti, aggiornati o eliminati nella tabella di origine, utilizzare un'espressione in una regola di trasformazione. L'espressione utilizza una funzione `operation_indicator` per contrassegnare i record. I record eliminati dall'origine non vengono eliminati dalla destinazione. Al contrario, il record di destinazione viene contrassegnato con un valore fornito dall'utente per indicare che è stato eliminato dall'origine.

Note

La funzione `operation_indicator` funziona solo su tabelle che hanno una chiave primaria sul database di origine e di destinazione.

Ad esempio, la regola di trasformazione seguente aggiunge prima una nuova colonna `Operation` a una tabella di destinazione. Quindi aggiorna la colonna con il valore `D` ogni volta che un record viene eliminato da una tabella di origine.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "%",
    "table-name": "%"
  },
  "rule-action": "add-column",
  "value": "Operation",
  "expression": "operation_indicator('D', 'U', 'I')",
  "data-type": {
    "type": "string",
    "length": 50
  }
}
```

Replica delle intestazioni della tabella di origine mediante espressioni

Per impostazione predefinita, le intestazioni per le tabelle di origine non vengono replicate nella destinazione. Per indicare le intestazioni da replicare, utilizzare una regola di trasformazione con un'espressione che include l'intestazione di colonna della tabella.

Nelle espressioni è possibile utilizzare le intestazioni di colonna seguenti.

Header	Valore nella replica in corso	Valore a pieno carico	Tipo di dati
AR_H_STRE AM_POSITION	Il valore della posizione del flusso dall'origine. Questo valore potrebbe essere il numero SCN (System Change Number) o il numero di sequenza di log (LSN), a seconda dell'endpoint di origine.	Una stringa vuota.	STRING
AR_H_TIMESTAMP	Indicatore orario che indica l'ora della modifica.	Un timestamp che indica la data e l'ora correnti in cui i dati arrivano alla destinazione.	DATETIME (scale=7)
AR_H_COMMIT_TIMESTAMP	Un timestamp che indica l'ora del commit.	Indicatore orario che indica l'ora corrente.	DATETIME (scale=7)
AR_H_OPERATION	INSERT, UPDATE o DELETE	INSERT	STRING
AR_H_USER	Nome utente, ID o qualsiasi altra informazione fornita	La trasformazione che desideri applicare all'oggetto. Tutte	STRING

Header	Valore nella replica in corso	Valore a pieno carico	Tipo di dati
	<p>dall'origine sull'utente che ha apportato la modifica.</p> <p>Questa intestazione è supportata solo sugli endpoint di origine SQL Server e Oracle (versione 11.2.0.3 e successive).</p>	<p>le operazioni delle regole di trasformazione prevedono una distinzione tra lettere maiuscole e minuscole.</p>	
AR_H_CHANNEL_SEQ	<p>Un numero incrementale univoco del database di origine costituito da un timestamp e un numero a incremento automatico. Il valore dipende dal sistema del database di origine.</p>	<p>Una stringa vuota.</p>	<p>STRING</p>

Nell'esempio seguente viene aggiunta una nuova colonna alla destinazione utilizzando il valore della posizione del flusso dall'origine. Per SQL Server, il valore della posizione del flusso è il LSN dell'endpoint di origine. Per Oracle, il valore della posizione del flusso è il SCN dell'endpoint di origine.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "%",
    "table-name": "%"
  }
}
```

```

    },
    "rule-action": "add-column",
    "value": "transact_id",
    "expression": "$AR_H_STREAM_POSITION",
    "data-type": {
      "type": "string",
      "length": 50
    }
  }
}

```

L'esempio seguente aggiunge una nuova colonna alla destinazione con un numero incrementale univoco dell'origine. Questo valore rappresenta un numero univoco di 35 cifre a livello di attività. Le prime 16 cifre fanno parte del timestamp e le ultime 19 cifre sono il numero record_id incrementato dal DBMS.

```

{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "%",
    "table-name": "%"
  },
  "rule-action": "add-column",
  "value": "transact_id",
  "expression": "$AR_H_CHANGE_SEQ",
  "data-type": {
    "type": "string",
    "length": 50
  }
}

```

Utilizzo delle funzioni SQLite per creare espressioni

Puoi utilizzare le impostazioni di tabella per specificare le impostazioni che desideri applicare alla tabella o alla vista selezionata per una determinata operazione. Le regole a livello di impostazioni di tabella sono facoltative.

Note

Invece di tabelle e viste, i database MongoDB e DocumentDB archiviano i record di dati come documenti che vengono archiviati in raccolte. Quindi, quando esegui la migrazione da una origine MongoDB o DocumentDB, considera il tipo di segmentazione dell'intervallo delle impostazioni di caricamento parallelo per le raccolte selezionate anziché le tabelle e le viste.

Argomenti

- [Utilizzo di un'espressione CASE](#)
- [Esempi](#)

Di seguito sono disponibili le funzioni di stringa che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzioni stringa	Descrizione
<code>lower(x)</code>	La funzione <code>lower(x)</code> restituisce una copia della stringa <code>x</code> con tutti i caratteri convertiti in minuscolo. La funzione <code>lower</code> predefinita e integrata funziona solo per i caratteri ASCII.
<code>upper(x)</code>	La funzione <code>upper(x)</code> restituisce una copia della stringa <code>x</code> con tutti i caratteri convertiti in maiuscolo. La funzione <code>upper</code> predefinita e integrata funziona solo per i caratteri ASCII.
<code>ltrim(x,y)</code>	La funzione <code>ltrim(x,y)</code> restituisce una stringa formata rimuovendo tutti i caratteri presenti in <code>y</code> dal lato sinistro di <code>x</code> . Se non è presente alcun valore per <code>y</code> , <code>ltrim(x)</code> rimuove gli spazi dal lato sinistro di <code>x</code> .
<code>replace(x,y,z)</code>	La funzione <code>replace(x,y,z)</code> restituisce una stringa formata sostituendo la stringa <code>z</code> per ogni occorrenza della stringa <code>y</code> nella stringa <code>x</code> .
<code>rtrim(x,y)</code>	La funzione <code>rtrim(x,y)</code> restituisce una stringa formata rimuovendo tutti i caratteri presenti in <code>y</code> dal lato destro di <code>x</code> . Se

Funzioni stringa	Descrizione
	<p>non è presente alcun valore per y, <code>rtrim(x)</code> rimuove gli spazi dal lato destro di x.</p>
<code>substr(x, y, z)</code>	<p>La funzione <code>substr(x, y, z)</code> restituisce una sottostringa della stringa di input x che inizia con il carattere yth e che è lunga z caratteri.</p> <p>Se z viene omissso, <code>substr(x, y)</code> restituisce tutti i caratteri fino alla fine della stringa x che inizia con il carattere yth. Il carattere più a sinistra di x è il numero 1. Se y è negativo, il primo carattere della sottostringa viene trovato contando da destra anziché da sinistra. Se z è negativo, vengono restituiti i caratteri <code>abs(z)</code> che precedono il carattere yth. Se x è una stringa, gli indici dei caratteri si riferiscono ai caratteri UTF-8 effettivi. Se x è un BLOB, gli indici si riferiscono ai byte.</p>
<code>trim(x, y)</code>	<p>La funzione <code>trim(x, y)</code> restituisce una stringa formata rimuovendo tutti i caratteri presenti in y da entrambi i lati di x. Se non è presente alcun valore per y, <code>trim(x)</code> rimuove gli spazi da entrambi i lati di x.</p>

Di seguito sono disponibili le funzioni LOB che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzioni LOB	Descrizione
<code>hex(x)</code>	<p>La funzione <code>hex</code> riceve un BLOB come argomento e restituisce una versione in stringa esadecimale maiuscola del contenuto del BLOB.</p>
<code>randblob (N)</code>	<p>La funzione <code>randblob(N)</code> restituisce un BLOB di N byte che contiene byte pseudocasuali. Se N è minore di 1, viene restituito un BLOB casuale da 1 byte.</p>

Funzioni LOB	Descrizione
zeroblob(<i>N</i>)	La funzione zeroblob(<i>N</i>) restituisce un BLOB composto da <i>N</i> byte di 0x00.

Di seguito sono disponibili le funzioni numeriche che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzioni numeriche	Descrizione
abs(<i>x</i>)	La funzione abs(<i>x</i>) restituisce il valore assoluto dell'argomento numerico <i>x</i> . La funzione abs(<i>x</i>) restituisce NULL se <i>x</i> è NULL. La funzione abs(<i>x</i>) restituisce 0,0 se <i>x</i> è una stringa o un BLOB che non può essere convertito in un valore numerico.
random()	La funzione random restituisce un intero pseudocasuale compreso tra -9.223.372.036.854.775.808 e +9.223.372.036.854.775.807.
round (<i>x</i> , <i>y</i>)	La funzione round (<i>x</i> , <i>y</i>) restituisce un valore a virgola mobile <i>x</i> arrotondato a <i>y</i> cifre a destra del punto decimale. Se non esiste alcun valore per <i>y</i> , si presume che sia 0.
max (<i>x</i> , <i>y</i> , . . .)	<p>La funzione max multiargomento restituisce l'argomento con il valore massimo o restituisce NULL se un argomento è NULL.</p> <p>La funzione max cerca negli argomenti da sinistra a destra un argomento che definisca una funzione di confronto. Se ne viene trovato uno, utilizza la funzione delle regole di confronto per i confronti tra tutte le stringhe. Se nessuno degli argomenti per max definiscono una funzione delle regole di confronto, viene utilizzata la funzione delle regole di confronto BINARY. La funzione max è una funzione semplice quando ha due o più argomenti, ma viene usata come una funzione aggregata se ha un solo argomento.</p>

Funzioni numeriche	Descrizione
<code>min (x,y...)</code>	<p>La funzione <code>min</code> multiargomento restituisce l'argomento con il valore minimo.</p> <p>La funzione <code>min</code> cerca negli argomenti da sinistra a destra un argomento che definisca una funzione di confronto. Se ne viene trovato uno, utilizza la funzione delle regole di confronto per i confronti tra tutte le stringhe. Se nessuno degli argomenti per <code>min</code> definiscono una funzione delle regole di confronto, viene utilizzata la funzione delle regole di confronto <code>BINARY</code>. La funzione <code>min</code> è una funzione semplice quando ha due o più argomenti, ma viene usata come una funzione aggregata se ha un solo argomento.</p>

Di seguito sono disponibili le funzioni di controllo `NULL` che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzioni di controllo <code>NULL</code>	Descrizione
<code>coalesce (x,y...)</code>	La funzione <code>coalesce</code> restituisce una copia del primo argomento non <code>NULL</code> , ma restituisce <code>NULL</code> se tutti gli argomenti sono <code>NULL</code> . La funzione <code>coalesce</code> ha almeno due argomenti.
<code>ifnull(x,y)</code>	La funzione <code>ifnull</code> restituisce una copia del primo argomento non <code>NULL</code> , ma restituisce <code>NULL</code> se entrambi gli argomenti sono <code>NULL</code> . La funzione <code>ifnull</code> ha esattamente due argomenti. La funzione <code>ifnull</code> è uguale a <code>coalesce</code> con due argomenti.
<code>nullif(x,y)</code>	<p>La funzione <code>nullif(x,y)</code> restituisce una copia del primo argomento se gli argomenti sono diversi, ma restituisce <code>NULL</code> se gli argomenti sono gli stessi.</p> <p>La funzione <code>nullif(x,y)</code> cerca negli argomenti da sinistra a destra un argomento che definisca una funzione di confronto . Se ne viene trovato uno, utilizza la funzione delle regole di confronto per i confronti tra tutte le stringhe. Se nessuno degli</p>

Funzioni di controllo NULL	Descrizione
	argomenti per nullif definisce una funzione delle regole di confronto, viene utilizzata la funzione delle regole di confronto BINARY.

Di seguito sono disponibili le funzioni di data e ora che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzioni di data e ora	Descrizione
<code>date(<i>timestring</i> , <i>modifier</i>, <i>modifier</i>...)</code>	La funzione <code>date</code> restituisce la data nel formato AAAA-MM-GG.
<code>time(<i>timestring</i> , <i>modifier</i>, <i>modifier</i>...)</code>	La funzione <code>time</code> restituisce l'ora nel formato HH:MM:SS.
<code>datetime(<i>timestring</i> , <i>modifier</i>, <i>modifier</i>...)</code>	La funzione <code>datetime</code> restituisce la data e l'ora nel formato AAAA-MM-GG HH:MM:SS.
<code>julianday(<i>timestring</i> <i>g</i> , <i>modifier</i>, <i>modifier</i>...)</code>	La funzione <code>julianday</code> restituisce il numero di giorni trascorsi dal mezzogiorno di Greenwich del 24 novembre 4714 a.C.
<code>strftime(<i>format</i>, <i>timestring</i> , <i>modifier</i>, <i>modifier</i>...)</code>	La funzione <code>strftime</code> restituisce la data in base alla stringa di formato specificata come primo argomento, utilizzando una delle seguenti variabili: %d: giorno del mese %H: ora 00-24 %f: ** secondi frazionari SS.SSS %j: giorno dell'anno 001-366 %J: ** numero del giorno del calendario giuliano %m: mese 01-12

Funzioni di data e ora	Descrizione
	%M: minuti 00-59
	%s: secondi dal 1970-01-01
	%S: secondi 00-59
	%w: giorno della settimana 0-6 domenica==0
	%W: settimana dell'anno 00-53
	%Y: anno 0000-9999
	%%: %

Di seguito è disponibile una funzione hash che puoi utilizzare per creare espressioni di regole di trasformazione.

Funzione hash	Descrizione
hash_sha256(<i>x</i>)	<p>La funzione hash genera un valore hash per una colonna di input (utilizzando l'algoritmo SHA-256) e restituisce il valore esadecimale del valore hash generato.</p> <p>Per utilizzare la funzione hash in un'espressione, aggiungi hash_sha256(<i>x</i>) all'espressione e sostituisci <i>x</i> con il nome della colonna di origine.</p>

Utilizzo di un'espressione CASE

L'espressione SQLite CASE valuta un elenco di condizioni e restituisce un'espressione basata sul risultato. La sintassi viene mostrata di seguito.

```

CASE case_expression
  WHEN when_expression_1 THEN result_1
  WHEN when_expression_2 THEN result_2
  ...
  [ ELSE result_else ]

```

```

END

# Or

CASE
WHEN case_expression THEN result_1
WHEN case_expression THEN result_2
...
[ ELSE result_else ]
END

```

Esempi

Example di aggiunta di una nuova colonna di stringhe alla tabella di destinazione utilizzando una condizione case

Ad esempio, la regola di trasformazione seguente aggiunge la nuova colonna di stringhe `emp_seniority` alla tabella di destinazione `employee`. Utilizza la funzione SQLite `round` nella colonna dello stipendio, con una condizione case per verificare se lo stipendio è pari o superiore a 20.000. In tal caso, la colonna ottiene il valore `SENIOR` e ogni altra cosa ha il valore `JUNIOR`.

```

{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "add-column",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "public",
    "table-name": "employee"
  },
  "value": "emp_seniority",
  "expression": " CASE WHEN round($emp_salary)>=20000 THEN 'SENIOR' ELSE 'JUNIOR'
END",
  "data-type": {
    "type": "string",
    "length": 50
  }
}

```

Example di aggiunta di una nuova colonna di data alla tabella di destinazione

Nell'esempio seguente viene aggiunta la nuova colonna di data `createdate` alla tabella di destinazione `employee`. Quando si utilizza la funzione di data SQLite `datetime`, la data viene aggiunta alla tabella appena creata per ogni riga inserita.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "add-column",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "public",
    "table-name": "employee"
  },
  "value": "createdate",
  "expression": "datetime ()",
  "data-type": {
    "type": "datetime",
    "precision": 6
  }
}
```

Example di aggiunta di una nuova colonna numerica alla tabella di destinazione

Nell'esempio seguente viene aggiunta la nuova colonna numerica `rounded_emp_salary` alla tabella di destinazione `employee`. Utilizza la funzione SQLite `round` per aggiungere lo stipendio arrotondato.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "add-column",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "public",
    "table-name": "employee"
  },
  "value": "rounded_emp_salary",
  "expression": "round($emp_salary)",
}
```



```
"data-type": {
  "type": "int8"
}
}
```

Example di aggiunta di una nuova colonna di stringhe alla tabella di destinazione utilizzando la funzione hash

Nell'esempio seguente viene aggiunta la nuova colonna di stringhe `hashed_emp_number` alla tabella di destinazione `employee`. La funzione SQLite `hash_sha256(x)` crea valori con hash sulla destinazione per la colonna di origine `emp_number`.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "add-column",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "public",
    "table-name": "employee"
  },
  "value": "hashed_emp_number",
  "expression": "hash_sha256($emp_number)",
  "data-type": {
    "type": "string",
    "length": 64
  }
}
```

Aggiunta di metadati a una tabella di destinazione utilizzando espressioni

È possibile aggiungere le informazioni sui metadati alla tabella di destinazione utilizzando le espressioni seguenti:

- `$AR_M_SOURCE_SCHEMA`: il nome dello schema di origine.
- `$AR_M_SOURCE_TABLE_NAME`: il nome della tabella di origine.
- `$AR_M_SOURCE_COLUMN_NAME`: il nome di una colonna nella tabella di origine.
- `$AR_M_SOURCE_COLUMN_DATATYPE`: il tipo di dati di una colonna nella tabella di origine.

Example di aggiunta di una colonna per il nome dello schema utilizzando il nome dello schema dell'origine

Nell'esempio seguente viene aggiunta una nuova colonna denominata `schema_name` alla destinazione utilizzando il nome dello schema dell'origine.

```
{
  "rule-type": "transformation",
  "rule-id": "2",
  "rule-name": "2",
  "rule-action": "add-column",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "%",
    "table-name": "%"
  },
  "rule-action": "add-column",
  "value": "schema_name",
  "expression": "$AR_M_SOURCE_SCHEMA",
  "data-type": {
    "type": "string",
    "length": 50
  }
}
```

Regole e operazioni delle impostazioni di tabella e raccolta

Puoi utilizzare le impostazioni di tabella per specificare le impostazioni che desideri applicare alla tabella o alla vista selezionata per una determinata operazione. Le regole delle impostazioni di tabella sono facoltative, a seconda dell'endpoint e dei requisiti di migrazione.

Invece di tabelle e viste, i database MongoDB e Amazon DocumentDB archiviano i record di dati come documenti che vengono archiviati in raccolte. Un singolo database per un endpoint MongoDB o Amazon DocumentDB è un set specifico di raccolte identificate dal nome del database.

Quando esegui la migrazione da un'origine MongoDB o Amazon DocumentDB, le impostazioni di caricamento parallelo si utilizzano in modo leggermente diverso. In tal caso, considera il tipo di segmentazione automatica o di segmentazione degli intervalli delle impostazioni di caricamento parallelo per le raccolte selezionate anziché per le tabelle e le viste.

Argomenti

- [Utilizzo limitato dei caratteri jolly nelle impostazioni delle tabelle](#)
- [Utilizzo del caricamento parallelo per le tabelle, le viste e le raccolte selezionate](#)
- [Definizione delle impostazioni LOB per una tabella o una vista selezionata](#)
- [Esempi di impostazioni di tabella](#)

Per le regole di mappatura della tabella che utilizzano il tipo di regola di impostazione della tabella, puoi applicare i parametri riportati di seguito.

Parametro	Valori possibili	Descrizione
<code>rule-type</code>	<code>table-settings</code>	Un valore che applica la regola a una tabella, una vista o una raccolta specificata dalla regola di selezione.
<code>rule-id</code>	Un valore numerico.	Un valore numerico univoco per identificare la regola.
<code>rule-name</code>	Un valore alfanumerico.	Un nome univoco per identificare la regola.
<code>object-locator</code>	Un oggetto con i seguenti parametri: <ul style="list-style-type: none"> • <code>schema-name</code> : il nome dello schema. Per gli endpoint MongoDB e Amazon DocumentDB, questo è il nome del database che contiene un set di raccolte. • <code>table-name</code> : il nome della tabella, della vista o della raccolta. 	Il nome di uno schema e di una tabella o di una vista specifici o il nome di un database e di una raccolta specifici (senza caratteri jolly).
<code>parallel-load</code>	Un oggetto con i seguenti parametri: <ul style="list-style-type: none"> • <code>type</code>: specifica se il caricamento in parallelo è attivato. 	Specifica un'operazione di caricamento parallelo (multi-thread) sulla tabella o sulla vista identificato

Parametro	Valori possibili	Descrizione
	<p>In questo caso, il parametro specifica anche il meccanismo per identificare le partizioni delle tabelle o delle viste, le partizioni secondarie o altri segmenti da caricare in parallelo. Le partizioni sono segmenti già definiti e identificati in base al nome nella tabella o nella vista di origine.</p> <p>Per gli endpoint MongoDB e Amazon DocumentDB, le partizioni sono segmenti. AWS DMS può calcolare questi parametri di segmentazione automatica associati automaticamente. In alternativa è possibile specificarli manualmente utilizzando i parametri di segmentazione degli intervalli.</p> <p>Solo per gli endpoint Oracle, le partizioni secondarie rappresentano un ulteriore livello di segmenti già definiti e identificati in base al nome nella tabella o nella vista di origine. Puoi identificare altri segmenti nella regola <code>table-settings</code> specificando i limiti dell'intervallo di valori per una o più colonne della tabella o della vista.</p> <ul style="list-style-type: none"> • <code>partitions</code> : quando <code>type</code> è <code>partitions-list</code> , questo valore specifica tutte le partizioni da caricare in parallelo. 	<p>dall'opzione <code>object-locator</code> . In questo caso, è possibile caricare in parallelo in uno dei seguenti modi:</p> <ul style="list-style-type: none"> • Per segmenti specificati da tutte le partizioni disponibili o secondarie. • Per partizioni selezionate e partizioni secondarie. • Per segmentazione automatica o segmenti basati su intervalli specificati dall'utente. <p>Per ulteriori informazioni sul caricamento parallelo , consulta Utilizzo del caricamento parallelo per le tabelle, le viste e le raccolte selezionate.</p>

Parametro	Valori possibili	Descrizione
	<ul style="list-style-type: none">• <code>subpartitions</code> : solo per gli endpoint Oracle, quando <code>type</code> è <code>partitions-list</code> questo valore specifica tutte le partizioni secondarie da caricare in parallelo.• <code>columns</code>: quando <code>type</code> è <code>ranges</code>, questo valore specifica i nomi delle colonne utilizzate per identificare i segmenti basati su intervalli che vengono caricati in parallelo.• <code>boundaries</code> : quando <code>type</code> è <code>ranges</code>, questo valore specifica i valori di <code>columns</code> utilizzati per identificare i segmenti basati su intervalli da caricare in parallelo.	

Parametro	Valori possibili	Descrizione
type	<p>Uno dei valori seguenti di <code>parallel-load</code> :</p> <ul style="list-style-type: none"> • <code>partitions-auto</code> : tutte le partizioni della tabella o della vista vengono caricate in parallelo. Ogni partizione è allocata al proprio thread. <p>Questa è un'impostazione obbligatoria per gli endpoint di origine MongoDB e Amazon DocumentDB per utilizzare l'opzione di segmentazione automatica di un pieno carico parallelo.</p> <ul style="list-style-type: none"> • <code>subpartitions-auto</code> : (solo per endpoint Oracle) tutte le partizioni secondarie delle tabelle o delle viste vengono caricate in parallelo. Ogni partizione secondaria è allocata al proprio thread. • <code>partitions-list</code> : tutte le partizioni specificate della tabella o della vista vengono caricate in parallelo. Solo per gli endpoint Oracle, tutte le partizioni secondarie e specificate delle tabelle o delle viste vengono caricate in parallelo . Ogni partizione e partizione secondaria specificate vengono allocate al proprio thread. Puoi identificare le partizioni e le partizioni secondarie da caricare in parallelo specificando i nomi 	<p>Il meccanismo per identificare partizioni, partizioni secondarie o segmenti della tabella, della vista o della raccolta da caricare in parallelo.</p>

Parametro	Valori possibili	Descrizione
	<p>delle partizioni (<code>partitions</code>) e i nomi delle partizioni secondarie (<code>subpartitions</code>).</p> <ul style="list-style-type: none"> • <code>ranges</code>: tutti i segmenti della tabella, della vista o della raccolta specificati dall'intervallo vengono caricati in parallelo. Ogni segmento della tabella, della vista o della raccolta identificato è allocato al proprio thread. Puoi specificare questi segmenti per i nomi delle colonne (<code>columns</code>) e i valori delle colonne (<code>boundaries</code>). <p>Gli endpoint PostgreSQL supportano solo questo tipo di caricamento parallelo. MongoDB e Amazon DocumentDB come endpoint di origine supportano sia questo tipo di segmentazione dell'intervallo che il tipo di segmentazione automatica di un pieno carico parallelo (<code>partitions-auto</code>).</p> <ul style="list-style-type: none"> • <code>none</code>: la tabella, la vista o la raccolta viene caricata in un'unica operazione a thread singolo (impostazione predefinita), indipendentemente dalle sue partizioni o dalle partizioni secondarie. Per ulteriori informazioni, consulta Creazione di un'attività. 	

Parametro	Valori possibili	Descrizione
<code>number-of-partitions</code>	(Facoltativo) Quando <code>type</code> è <code>partitions-auto</code> per raccolte specifiche di un endpoint MongoDB o Amazon DocumentDB, questo parametro specifica il numero totale di partizioni (segmenti) utilizzate per la migrazione. Il valore predefinito è 16.	Specifica il numero esatto di partizioni da caricare in parallelo.
<code>collection-count-from-metadata</code>	(Facoltativo) <code>type</code> When <code>partitions-auto</code> si riferisce a raccolte specifiche di un endpoint MongoDB o Amazon DocumentDB e questo parametro è impostato su <code>AWS DMS</code> , utilizza un conteggio stimato delle raccolte <code>true</code> per determinare il numero di partizioni. Se questo parametro è impostato su <code>false</code> , <code>AWS DMS</code> utilizza il conteggio effettivo delle raccolte. Il valore predefinito è <code>true</code> .	Specifica se utilizzare un numero stimato di raccolte o il numero effettivo di raccolte per calcolare il numero di partizioni da caricare in parallelo.

Parametro	Valori possibili	Descrizione
<code>max-records-skip-per-page</code>	(Facoltativo) Quando <code>type</code> è <code>partitions-auto</code> per raccolte specifiche di un endpoint MongoDB o Amazon DocumentDB, questo è numero di record da ignorare contemporaneamente quando si determinano i limiti di ogni partizione. AWS DMS utilizza un approccio per ignorare con paginazione per determinare il limite minimo di una partizione. Il valore predefinito è 10.000.	Specifica il numero di record da ignorare contemporaneamente quando si determinano i limiti di ogni partizione. L'impostazione di un valore relativamente elevato rispetto a quello predefinito potrebbe causare timeout del cursore e errori delle attività. L'impostazione di un valore relativamente basso rispetto a quello predefinito comporta un numero maggiore di operazioni per pagina e un pieno carico più lento.
<code>batch-size</code>	(Facoltativo) Quando <code>type</code> è <code>partitions-auto</code> per raccolte specifiche di un endpoint MongoDB o Amazon DocumentDB, questo valore intero limita il numero di documenti restituiti in un batch di andata e ritorno. Se la dimensione del batch è zero (0), il cursore utilizza la dimensione massima del batch definita dal server. Il valore predefinito è 0.	Specifica il numero massimo di documenti restituiti in un batch. Ogni batch richiede un round trip al server.
<code>partitions</code>	Quando <code>type</code> è impostato su <code>partitions-list</code> , questo è un vettore di stringhe che specifica i nomi delle partizioni che vengono caricate in parallelo.	I nomi di partizioni da caricare in parallelo.

Parametro	Valori possibili	Descrizione
<code>subpartitions</code>	(Solo per endpoint Oracle) Quando <code>type</code> è impostato su <code>partitions-list</code> , questo è un vettore di stringhe che specifica i nomi delle partizioni secondarie da caricare in parallelo.	I nomi delle partizioni secondarie da caricare in parallelo.
<code>columns</code>	Quando <code>type</code> è <code>ranges</code> , questa è una matrice di stringhe che specifica i nomi delle colonne utilizzate per identificare i segmenti delle tabelle, delle viste o delle raccolte basati su intervalli da caricare in parallelo.	I nomi delle colonne utilizzate per identificare i segmenti delle tabelle, delle viste o delle raccolte basati su intervalli da caricare in parallelo.
<code>boundaries</code>	Quando <code>type</code> è impostato su <code>ranges</code> , questo è un vettore di vettori di valori di colonna. Ogni vettore di valori di colonna contiene valori di colonna nella quantità e nell'ordine specificati da <code>columns</code> . Una matrice di valori di colonna specifica il limite superiore di un segmento delle tabelle, delle viste o delle raccolte. Ogni matrice di valori di colonna aggiuntiva aggiunge un limite superiore per definire un ulteriore segmento delle tabelle, delle viste o delle raccolte. Tutti questi segmenti delle tabelle, delle viste o delle raccolte basati su intervalli vengono caricati in parallelo.	I valori della colonna che identificano le partizioni delle tabelle, delle viste o delle raccolte basate su intervalli da caricare in parallelo.

Parametro	Valori possibili	Descrizione
<code>lob-settings</code>	<p>Un oggetto con i seguenti parametri:</p> <ul style="list-style-type: none">• <code>mode</code>: specifica la modalità di gestione della migrazione per i LOB.• <code>bulk-max-size</code> : specifica le dimensioni massime dei LOB, in base all'impostazione <code>mode</code>.	<p>Un valore che specifica la gestione LOB per la tabella o la vista identificata dall'opzione <code>object-locator</code> . Il LOB specificato sostituisce tutte le attività di gestione delle impostazioni LOB solo per questa tabella o questa vista. Per ulteriori informazioni sull'utilizzo dei parametri delle impostazioni dei LOB, consulta Definizione delle impostazioni LOB per una tabella o una vista selezionata.</p>

Parametro	Valori possibili	Descrizione
mode	<p>Specifica la gestione della migrazione e per i LOB nella tabella o nella vista selezionata utilizzando i seguenti valori:</p> <ul style="list-style-type: none">• <code>limited</code>: (impostazione predefinita) questo valore imposta la migrazione nella modalità LOB limitata, con tutti i LOB migrati inline insieme a tutti gli altri tipi di dati di colonna nella tabella o nella vista. Utilizzare questo valore quando si replicano i LOB più piccoli (100 MB o meno). Inoltre, specifica un valore <code>bulk-max-size</code> (zero non è valido). Tutti i LOB migrati superiori a <code>bulk-max-size</code> vengono troncati alle dimensioni che hai impostato.• <code>unlimited</code> questo valore imposta la migrazione nella modalità LOB completa. Utilizza questo valore quando tutti o la maggior parte dei LOB che desideri replicare sono di dimensioni superiori a 1 GB. Se si specifica un valore <code>bulk-max-size</code> di zero, tutti i LOB vengono migrati in modalità LOBstandard completa. In questa modalità <code>unlimited</code>, viene eseguita separatamente la migrazione di tutti i LOB da altri tipi di dati di colonna utilizzando una ricerca	Il meccanismo utilizzato per migrare i LOB.

Parametro	Valori possibili	Descrizione
	<p>dalla tabella o dalla vista di origine. Se si specifica un valore <code>bulk-max-size</code> superiore a zero, tutti i LOB vengono migrati in modalità LOB completa in combinazione. In questa modalità <code>unlimited</code>, viene eseguita la migrazione dei LOB superiori a <code>bulk-max-size</code> utilizzando una ricerca della tabella o della vista di origine, in modo analogo alla modalità LOB standard completa. Al contrario, i LOB fino a questa dimensione e vengono migrati inline, in modo analogo a quanto accade per la modalità LOB limitati. Nessun LOB viene mai troncato in modalità <code>unlimited</code>, indipendentemente dalla forma utilizzata.</p> <ul style="list-style-type: none">• <code>none</code>: viene eseguita la migrazione di tutti i LOB della tabella o della vista in base alle impostazioni per i LOB delle attività. <p>Per ulteriori informazioni sulle impostazioni per i LOB delle attività, consulta Impostazioni delle attività dei metadati di destinazione.</p> <p>Per ulteriori informazioni su come migrare i LOB e su come specificare le impostazioni per i LOB delle attività, consulta Impostazione del</p>	

Parametro	Valori possibili	Descrizione
	supporto LOB per i database di origine in un task AWS DMS.	
<code>bulk-max-size</code>	L'effetto di questo valore dipende dall'impostazione del parametro <code>mode</code> .	Specifica le dimensioni massime dei LOB in incrementi di kilobyte. Specifica questa opzione solo se hai bisogno di replicare LOB di piccole dimensioni o se l'endpoint di destinazione non supporta LOB di dimensioni illimitate.

Utilizzo limitato dei caratteri jolly nelle impostazioni delle tabelle

L'utilizzo del carattere jolly percentuale ("%") nelle regole "table-settings" non è supportato per i database di origine, come illustrato di seguito.

```
{
  "rule-type": "table-settings",
  "rule-id": "8",
  "rule-name": "8",
  "object-locator": {
    "schema-name": "ipeline-prod",
    "table-name": "%"
  },
  "parallel-load": {
    "type": "partitions-auto",
    "number-of-partitions": 16,
    "collection-count-from-metadata": "true",
    "max-records-skip-per-page": 1000000,
    "batch-size": 50000
  }
}
```

Se si utilizza "%" nelle "table-settings" regole come mostrato, AWS DMS restituisce l'eccezione seguente.

```
Error in mapping rules. Rule with ruleId = x failed validation. Exact schema and table name required when using table settings rule.
```

Inoltre, si AWS consiglia di non caricare un gran numero di raccolte di grandi dimensioni utilizzando un'unica operazione `conparallel-load`. AWS DMS limita il conflitto di risorse e il numero di segmenti caricati in parallelo in base al valore del parametro delle impostazioni delle attività `MaxFullLoadSubTasks`, con un valore massimo di 49.

Specifica tutte le raccolte più grandi per il database di origine definendo singolarmente "schema-name" e "table-name". Inoltre, aumenta correttamente la migrazione. Ad esempio, esegui più attività su un numero sufficiente di istanze di replica per gestire un elevato numero di raccolte di grandi dimensioni nel database.

Utilizzo del caricamento parallelo per le tabelle, le viste e le raccolte selezionate

Per velocizzare la migrazione e renderla più efficiente, puoi usare la funzione di caricamento parallelo per le tabelle relazionali, le viste e le raccolte selezionate. In altre parole, puoi eseguire la migrazione di una singola tabella, vista o raccolta segmentata utilizzando diversi thread in parallelo. A tale scopo, AWS DMS suddivide un'attività a caricamento completo in thread, con ogni segmento di tabella assegnato al relativo thread.

Utilizzando questo processo di caricamento in parallelo, puoi innanzitutto avere più thread che scaricano più tabelle, viste e raccolte in parallelo dall'endpoint di origine. Successivamente, puoi avere più thread che eseguono la migrazione e caricano le stesse tabelle, viste e raccolte in parallelo per l'endpoint di destinazione. Per alcuni motori di database, puoi segmentare le tabelle e le viste utilizzando le partizioni o le partizioni secondarie esistenti. Per altri motori di database, è possibile segmentare AWS DMS automaticamente le raccolte in base a parametri specifici (segmentazione automatica). In caso contrario, puoi segmentare qualsiasi tabella, vista o raccolta in base a intervalli di valori delle colonne specificati dall'utente.

Il caricamento parallelo è supportata per i seguenti endpoint di origine:

- Oracle
- Microsoft SQL Server
- MySQL

- PostgreSQL
- IBM Db2 LUW
- SAP Adaptive Server Enterprise (ASE)
- MongoDB (supporta solo le opzioni di segmentazione automatica e segmentazione degli intervalli di un pieno carico parallelo)
- Amazon DocumentDB (supporta solo le opzioni di segmentazione automatica e segmentazione degli intervalli di un pieno carico parallelo)

Per gli endpoint MongoDB e Amazon DocumentDB AWS DMS , supporta i seguenti tipi di dati per le colonne che sono chiavi di partizione per l'opzione di segmentazione dell'intervallo di un carico completo parallelo.


- Doppio
- Stringa
- ObjectId
- Intero a 32 bit
- Intero a 64 bit

Il caricamento parallelo per l'utilizzo con le regole di impostazione delle tabelle è supportato per i seguenti endpoint di destinazione:

- Oracle
- Microsoft SQL Server
- MySQL
- PostgreSQL
- Amazon S3
- SAP Adaptive Server Enterprise (ASE)
- Amazon Redshift
- MongoDB (supporta solo le opzioni di segmentazione automatica e segmentazione degli intervalli di un pieno carico parallelo)
- Amazon DocumentDB (supporta solo le opzioni di segmentazione automatica e segmentazione degli intervalli di un pieno carico parallelo)
- Db2 LUW

Per specificare il numero massimo di tabelle e viste da caricare in parallelo, utilizza l'impostazione dell'attività `MaxFullLoadSubTasks`.

Per specificare il numero massimo di thread per tabella o vista per le destinazioni supportate di un'attività di caricamento parallelo, definisci più segmenti utilizzando i limiti dei valori delle colonne.

 Important

`MaxFullLoadSubTasks` controlla il numero di tabelle o segmenti di tabella da caricare in parallelo. `ParallelLoadThreads` controlla il numero di thread utilizzati da un'attività di migrazione per eseguire i carichi in parallelo. Queste impostazioni sono moltiplicative. Pertanto, il numero totale di thread utilizzati durante un'operazione di pieno carico è approssimativamente il risultato del valore di `ParallelLoadThreads` moltiplicato per il valore di `MaxFullLoadSubTasks` ($\text{ParallelLoadThreads} * \text{MaxFullLoadSubTasks}$). Se si creano attività con un numero elevato di attività secondarie di pieno carico e un numero elevato di thread di caricamento parallelo, l'attività può consumare troppa memoria e non riuscire.

Per specificare il numero massimo di thread per tabella per le destinazioni Amazon DynamoDB, Flusso di dati Amazon Kinesis, Apache Kafka o Amazon Elasticsearch Service, utilizza l'impostazione dell'attività dei metadati di destinazione `ParallelLoadThreads`.

Per specificare le dimensioni del buffer per un'attività di caricamento parallelo quando si usa `ParallelLoadThreads`, utilizza l'impostazione dell'attività dei metadati di destinazione `ParallelLoadBufferSize`.

La disponibilità e le impostazioni di `ParallelLoadThreads` e `ParallelLoadBufferSize` dipendono dall'endpoint di destinazione.

Per ulteriori informazioni sulle impostazioni `ParallelLoadThreads` e `ParallelLoadBufferSize`, consulta [Impostazioni delle attività dei metadati di destinazione](#). Per ulteriori informazioni sull'impostazione `MaxFullLoadSubTasks`, consulta [Impostazioni delle attività di caricamento completo](#). Per informazioni specifiche per gli endpoint di destinazione, vedere gli argomenti correlati.

Per utilizzare il caricamento in parallelo, crea una regola di mappatura della tabella di tipo `table-settings` con l'opzione `parallel-load`. All'interno della regola `table-settings`, puoi

specificare i criteri di segmentazione per una singola tabella, vista o raccolta che desideri caricare in parallelo. Per farlo, impostare il parametro `type` dell'opzione `parallel-load` per una delle diverse opzioni.

Come eseguire questa operazione dipende dal modo in cui desideri segmentare la tabella, la vista o la raccolta per il caricamento in parallelo:

- Per partizioni (o segmenti): carica tutte le partizioni (o i segmenti) delle tabelle o delle viste esistenti utilizzando il tipo `partitions-auto`. In alternativa, carica solo le partizioni selezionate utilizzando il tipo `partitions-list` con una matrice di partizioni specificata.

Solo per gli endpoint MongoDB e Amazon DocumentDB, carica tutte le raccolte o quelle specificate per segmenti, AWS DMS che vengono calcolate automaticamente anche utilizzando il tipo e i parametri opzionali aggiuntivi. `partitions-auto table-settings`

- (Solo gli endpoint Oracle) Per partizioni secondarie: carica tutte le partizioni secondarie delle tabelle o delle viste esistenti utilizzando il tipo `subpartitions-auto`. Oppure caricare solo le partizioni secondarie selezionate utilizzando il tipo `partitions-list` con una matrice `subpartitions` specificata.
- Per segmenti definiti: carica i segmenti delle tabelle, delle viste o delle raccolte definiti utilizzando limiti di valori per colonna. Per farlo, utilizzare il tipo `ranges` con matrice specificate `columns` e `boundaries`.

Note

Gli endpoint PostgreSQL supportano solo questo tipo di caricamento parallelo. MongoDB e Amazon DocumentDB come endpoint di origine supportano sia questo tipo di segmentazione dell'intervallo che il tipo di segmentazione automatica di un pieno carico parallelo (`partitions-auto`).

Per identificare le tabelle, le viste o le raccolte aggiuntive da caricare in parallelo, specifica ulteriori oggetti `table-settings` con opzioni `parallel-load`.

Nelle seguenti procedure puoi scoprire come creare il codice JSON per ciascun tipo di caricamento parallelo, dai casi più semplici a quelli più complessi.

Per specificare tutte le partizioni delle tabelle, delle viste o delle raccolte o tutte le partizioni secondarie delle tabelle o delle viste

- Specifica `parallel-load` con il tipo `partitions-auto` o il tipo `subpartitions-auto` (ma non entrambi).


Ogni partizione (segmento) o partizione secondaria della tabella, della vista o della raccolta viene automaticamente allocata al proprio thread.

Per alcuni endpoint, il caricamento parallelo include partizioni o partizioni secondarie solo se sono già definite per la tabella o la vista. Per gli endpoint di origine MongoDB e Amazon DocumentDB, puoi calcolare automaticamente le partizioni (o AWS DMS segmenti) in base a parametri aggiuntivi opzionali. Tra queste vi sono `number-of-partitions`, `collection-count-from-metadata`, `max-records-skip-per-page` e `batch-size`.

Per specificare partizioni o partizioni secondarie di una tabella o una vista selezionata o entrambe

1. Specifica `parallel-load` con il tipo `partitions-list`.
2. (Facoltativo) Includi le partizioni specificando una vasta gamma di nomi di partizione come valore di `partitions`.

Ogni partizione specificata viene quindi allocata al proprio thread.

 Important

Per gli endpoint Oracle, assicurati che le partizioni e le partizioni secondarie non si sovrappongano quando le scegli per il caricamento parallelo. Se si utilizzano partizioni e partizioni secondarie sovrapposte per caricare i dati in parallelo, le voci vengono duplicate o l'operazione non riesce a causa di una violazione del duplicato della chiave primaria.

3. (Facoltativo) Solo per gli endpoint Oracle includi le partizioni secondarie specificando una serie di nomi di partizioni secondarie come valore di `subpartitions`.

Ogni partizione secondaria specificata viene quindi allocata al proprio thread.

Note

Il caricamento in parallelo include partizioni o partizioni secondarie solo se sono già definite per la tabella o la vista.

Puoi specificare i segmenti delle tabelle o delle viste come intervalli di valori delle colonne. In questo caso, è necessario ricordare le caratteristiche di queste colonne:

- L'utilizzo di colonne indicizzate migliora in modo significativo le prestazioni.
- È possibile specificare fino a 10 colonne.
- Non puoi utilizzare le colonne per definire i confini dei segmenti con i seguenti tipi di AWS DMS dati: DOUBLE, FLOAT, BLOB, CLOB e NCLOB
- I record con valori nulli non vengono replicati.

Per specificare i segmenti delle tabelle, delle viste o delle raccolte come intervalli di valori delle colonne

1. Specifica `parallel-load` con il tipo `ranges`.
2. Definire un limite tra i segmenti delle tabelle o delle viste specificando una matrice di nomi di colonne come valore di `columns`. Eseguire questa operazione per ogni colonna per cui si desidera definire un limite tra i segmenti delle tabelle o delle viste.

L'ordine delle colonne è significativo. La prima colonna è la più significativa e l'ultima colonna è la meno significativa nella definizione di ogni limite, come descritto nei seguenti passaggi.

3. Definire gli intervalli di dati per tutti i segmenti delle tabelle o delle viste attribuendo a una matrice di delimitatori il valore `boundaries`. Un vettore di delimitatori è un vettore di vettori colonna-valore. A tale scopo, procedere come indicato di seguito.
 - a. Specifica ciascun elemento di una matrice colonna-valore come valore che corrisponde a ogni colonna. Una matrice di valori di colonna rappresenta il limite superiore di ciascun segmento della tabella o della vista da definire. Specifica ogni colonna nello stesso ordine specificato per tale colonna nella matrice `columns`.

Inserisci i valori per le colonne di tipo DATE nel formato supportato dall'origine.

- b. Specificate ogni array di valori di colonna come limite superiore, nell'ordine, di ogni segmento dalla parte inferiore al segmento della tabella o della vista. next-to-top Se esistono delle righe che vanno oltre il massimo limite superiore specificato, queste righe costituiranno l'ultimo segmento della tabella o della vista. Di conseguenza, il numero di segmenti basati su intervalli è potenzialmente uno più del numero di delimitazioni di segmento contenute nel vettore delle delimitazioni. Ognuno di questi segmenti basati su intervalli è allocato al proprio thread.

Tutti i dati non nulli della tabella vengono replicati, anche se non si definiscono intervalli di dati per tutte le colonne della tabella o della vista.

Ad esempio, supponi di definire tre vettori colonna-valore per le colonne COL1, COL2 e COL3 come segue.

COL1	COL2	COL3
10	30	105
20	20	120
100	12	99

Hai definito tre delimitazioni di segmenti per un totale di quattro potenziali segmenti.

Per identificare gli intervalli di righe da replicare per ogni segmento, l'istanza di replica applica una ricerca su queste tre colonne per ciascuno dei quattro segmenti. La ricerca è simile alla seguente:

Segmento 1

Replicare tutte le righe in cui si verificano le seguenti condizioni: i primi valori di due colonne sono inferiori o uguali ai valori di limite superiore del Segmento 1 corrispondenti. Inoltre, i valori della terza colonna sono inferiori al valore di limite superiore del Segmento 1.

Segmento 2

Replica tutte le righe (eccetto le righe Segmento 1) in cui si verificano le seguenti condizioni: i valori delle prime due colonne sono inferiori o uguali ai valori di limite superiore del

Segmento 2 corrispondente. Inoltre, i valori della terza colonna sono inferiori al relativo valore di limite superiore del Segmento 2 .

Segmento 3

Replicare tutte le righe (eccetto le righe del Segmento 2) in cui si verificano le seguenti condizioni: i valori delle prime due colonne sono inferiori o uguali ai valori di limite superiore del Segmento 3 corrispondente. Inoltre, i valori della terza colonna sono inferiori al relativo valore del limite superiore del Segmento 3 .

Segmento 4

Replica tutte le righe rimanenti (escluse quelle appartenenti ai Segmenti 1, 2 e 3).

In questo caso, l'istanza di replica crea una clausola WHERE per caricare ogni segmento come segue:

Segmento 1

```
((COL1 < 10) OR ((COL1 = 10) AND (COL2 < 30)) OR ((COL1 = 10) AND (COL2 = 30) AND (COL3 < 105)))
```

Segmento 2

```
NOT ((COL1 < 10) OR ((COL1 = 10) AND (COL2 < 30)) OR ((COL1 = 10) AND (COL2 = 30) AND (COL3 < 105))) AND ((COL1 < 20) OR ((COL1 = 20) AND (COL2 < 20)) OR ((COL1 = 20) AND (COL2 = 20) AND (COL3 < 120)))
```

Segmento 3

```
NOT ((COL1 < 20) OR ((COL1 = 20) AND (COL2 < 20)) OR ((COL1 = 20) AND (COL2 = 20) AND (COL3 < 120))) AND ((COL1 < 100) OR ((COL1 = 100) AND (COL2 < 12)) OR ((COL1 = 100) AND (COL2 = 12) AND (COL3 < 99)))
```

Segmento 4

```
NOT ((COL1 < 100) OR ((COL1 = 100) AND (COL2 < 12)) OR ((COL1 = 100) AND (COL2 = 12) AND (COL3 < 99)))
```

Definizione delle impostazioni LOB per una tabella o una vista selezionata

Puoi impostare le impostazioni LOB dell'attività per una o più tabelle mediante la creazione di una regola di mappatura della tabella di tipo `table-settings` con l'opzione `lob-settings` per uno o più oggetti `table-settings`.

La definizione delle impostazioni LOB per le tabelle o le viste selezionate è supportata per i seguenti endpoint origine:

- Oracle
- Microsoft SQL Server
- MySQL
- PostgreSQL
- IBM Db2, a seconda delle impostazioni `mode` e `bulk-max-size`, descritte di seguito
- SAP Adaptive Server Enterprise (ASE), a seconda delle impostazioni `mode` e `bulk-max-size`, come descritto di seguito

La definizione delle impostazioni LOB per le tabelle o le viste selezionate è supportata per i seguenti endpoint di destinazione:

- Oracle
- Microsoft SQL Server
- MySQL
- PostgreSQL
- SAP ASE, a seconda delle impostazioni `mode` e `bulk-max-size`, come descritto di seguito

Note

Puoi utilizzare i tipi di dati LOB solo con le tabelle e le viste che includono una chiave primaria.

Per usare le impostazioni per i LOB per una tabella o una vista selezionata, devi creare una regola di mappatura della tabella di tipo `table-settings` con l'opzione `lob-settings`. Questa azione specifica la modalità di gestione dei LOB per la tabella o la vista identificata dall'opzione `object-`

locator. All'interno della regola table-settings è possibile specificare un oggetto lob-settings con i parametri seguenti:

- **mode**: specifica il meccanismo di gestione della migrazione dei LOB per la tabella o la vista selezionata come segue:
 - **limited**: questa modalità LOB limitata predefinita è la modalità più veloce ed efficiente. Utilizzare questa modalità solo se tutti i LOB sono piccoli (100 MB al massimo) o l'endpoint di destinazione non supporta un numero illimitato di dimensioni LOB. Anche se utilizzi limited, tutti i LOB devono essere entro le dimensioni impostate per bulk-max-size.

In questa modalità per un'attività di caricamento completo, l'istanza di replica esegue la migrazione di tutti i LOB inline insieme ad altri tipi di dati delle colonne come parte dello storage della tabella o della vista principale. Tuttavia, l'istanza tronca tutti i LOB migrati di dimensioni maggiori rispetto al valore bulk-max-size riducendoli alla dimensione specificata. In caso di caricamento per acquisizione delle modifiche dei dati (Change Data Capture, CDC), l'istanza migra tutti i LOB utilizzando un'operazione di ricerca sulla tabella di origine, in modo analogo a quanto accade per la modalità standard LOB completi (vedi quanto segue).

Note

Puoi eseguire la migrazione delle viste solo per le attività di caricamento completo.

- **unlimited**: il meccanismo di migrazione per questa modalità LOB completa varia in base al valore impostato per bulk-max-size come segue:
 - **Modalità standard LOB completa**: quando imposti bulk-max-size su zero, l'istanza di replica migra tutti i LOB utilizzando la modalità LOB completa standard. Questa modalità richiede un'operazione di ricerca nella tabella o nella vista di origine per eseguire la migrazione di ogni LOB, indipendentemente dalle dimensioni. In genere ciò porta a una migrazione molto più lenta rispetto a quelle in modalità LOB limitate. Utilizza questa modalità solo se tutti o la maggior parte dei tuoi LOB sono di grandi dimensioni (1 GB o superiore).
 - **Modalità combinazione LOB completa**: quando imposti bulk-max-size su un valore diverso da zero, la modalità LOB completa utilizza una combinazione di modalità LOB limitata e modalità LOB completa standard. Ciò è valido per un'attività di caricamento completo, se la dimensione del LOB rientra all'interno del valore bulk-max-size, l'istanza migra il LOB inline come accade nella modalità LOB limitata. Se la dimensione del LOB è superiore a tale valore, l'istanza esegue la migrazione del LOB utilizzando un'operazione di ricerca nella tabella o nella vista di origine come accade nella modalità standard LOB completa. In caso di caricamento

per acquisizione delle modifiche dei dati (Change Data Capture, CDC), l'istanza migra tutti i LOB utilizzando un'operazione di ricerca sulla tabella di origine, in modo analogo a quanto accade per la modalità standard LOB completi (vedi quanto segue). Opera in questo modo, indipendentemente dalle dimensioni LOB.

Note

Puoi eseguire la migrazione delle viste solo per le attività di caricamento completo.

In questo modo si ottiene una velocità di migrazione che è un compromesso tra la più veloce modalità LOB limitati e la più lenta modalità standard LOB completi. Utilizza questa modalità solo quando agisci su una combinazione di LOB di piccole e grandi dimensioni e la maggior parte dei LOB sono di piccole dimensioni.

Questa modalità LOB completa in combinazione è disponibile solo per i seguenti endpoint:

- IBM Db2 come origine
- SAP ASE come origine o destinazione

Indipendentemente da come viene specificato il meccanismo per la modalità `unlimited`, l'istanza migra tutti i LOB in modo completo, senza troncamento.

- `none`: l'istanza di replica consente di eseguire la migrazione dei LOB nella tabella o nella vista selezionata utilizzando le impostazioni dei LOB dell'attività. Puoi utilizzare questa opzione per confrontare i risultati della migrazione con e senza le impostazioni per LOB specifici per la tabella o la vista selezionata.

Se la tabella o la vista specificata ha LOB inclusi nella replica, puoi impostare l'attività `BatchApplyEnabled` su `true` solo quando si usa la modalità `limited` LOB.

In alcuni casi, è possibile impostare `BatchApplyEnabled` su `true` e `BatchApplyPreserveTransaction` su `false`. In questi casi, l'istanza imposta `BatchApplyPreserveTransaction` su `true` se la tabella o la vista ha LOB e gli endpoint di origine e di destinazione sono Oracle.

- `bulk-max-size`: imposta questo valore su zero o un valore diverso da zero in kilobyte, a seconda dell'impostazione di `mode` come descritto per i precedenti elementi. In modalità `limited`, è necessario impostare un valore diverso da zero per il parametro.

L'istanza converte i LOB in formato binario. Pertanto, per indicare il LOB di dimensione massima da replicare, moltiplica le sue dimensioni per tre. Ad esempio, se il tuo LOB è di maggiori dimensioni di 2MB, imposta `bulk-max-size` su 6.000 (6 MB).

Esempi di impostazioni di tabella

In seguito, puoi trovare alcuni esempi che illustrano l'utilizzo delle impostazioni di tabella.

Example Carica una tabella segmentata per partizioni

L'esempio seguente carica una tabella SALES presente nell'origine in modo più efficiente eseguendo il caricamento in parallelo sulla base di tutte le sue partizioni.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "HR",
      "table-name": "SALES"
    },
    "parallel-load": {
      "type": "partitions-auto"
    }
  }
  ]
}
```

Example Carica una tabella segmentata per partizioni secondarie

L'esempio seguente carica una tabella SALES presente nell'origine in modo più efficiente eseguendo il caricamento in parallelo sulla base di tutte le sue partizioni secondarie.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "HR",
      "table-name": "SALES"
    },
    "parallel-load": {
      "type": "subpartitions-auto"
    }
  }
  ]
}
```

Example Caricare una tabella segmentata tramite un elenco di partizioni

L'esempio seguente carica una tabella SALES presente nell'origine eseguendo il caricamento in parallelo sulla base di uno specifico elenco di partizioni. In questo caso, le partizioni specificate vengono denominate con valori che iniziano con porzioni dell'alfabeto inglese, ad esempio ABCD, EFGH e così via.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
```



```

        "object-locator": {
            "schema-name": "%",
            "table-name": "%"
        },
        "rule-action": "include"
    },
    {
        "rule-type": "table-settings",
        "rule-id": "2",
        "rule-name": "2",
        "object-locator": {
            "schema-name": "HR",
            "table-name": "SALES"
        },
        "parallel-load": {
            "type": "partitions-list",
            "partitions": [
                "ABCD",
                "EFGH",
                "IJKL",
                "MNOP",
                "QRST",
                "UVWXYZ"
            ],
            "subpartitions": [
                "01234",
                "56789"
            ]
        }
    }
]
}

```

Example Caricare una tabella segmentata per intervalli di valori di colonna

L'esempio seguente carica una tabella SALES presente sull'origine caricandola in parallelo per segmenti specificati da intervalli di valori delle colonne SALES_NO e REGION.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",

```

```

    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "HR",
      "table-name": "SALES"
    },
    "parallel-load": {
      "type": "ranges",
      "columns": [
        "SALES_NO",
        "REGION"
      ],
      "boundaries": [
        [
          "1000",
          "NORTH"
        ],
        [
          "3000",
          "WEST"
        ]
      ]
    }
  }
]
}

```

In questo caso, per gli intervalli dei segmenti sono specificate due colonne denominate SALES_NO e REGION. Sono indicati due delimitazioni con due gruppi di valori di colonna (["1000", "NORTH"] e ["3000", "WEST"]).

Queste due delimitazioni identificano perciò i seguenti tre segmenti di tabella da caricare in parallelo:

Segmento 1

Righe con SALES_NO minore o uguale a 1.000 e REGION inferiore a "NORTH". In altre parole, i totali di vendita fino a 1.000 nella regione EAST.

Segmento 2

Righe non incluse nel Segmento 1 con SALES_NO minore o uguale a 3.000 e REGION inferiore a "WEST". In altre parole, i totali di vendita maggiori di 1.000 e fino a 3.000 nelle regioni NORTH e SOUTH.

Segmento 3

Tutte le righe rimanenti non incluse nel Segmento 1 e nel Segmento 2. In altre parole, i totali di vendita maggiori di 3.000 nella regione "WEST".

Example Caricamento di due tabelle: una segmentata per intervalli e l'altra segmentata tramite partizioni

L'esempio seguente consente di caricare una tabella SALES in parallelo per limiti di segmenti che hai identificato. Inoltre, consente di caricare una tabella ORDERS in parallelo da tutte le partizioni, come con esempi precedenti.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "HR",
      "table-name": "SALES"
    }
  },
```

```

    "parallel-load": {
      "type": "ranges",
      "columns": [
        "SALES_NO",
        "REGION"
      ],
      "boundaries": [
        [
          "1000",
          "NORTH"
        ],
        [
          "3000",
          "WEST"
        ]
      ]
    }
  },
  {
    "rule-type": "table-settings",
    "rule-id": "3",
    "rule-name": "3",
    "object-locator": {
      "schema-name": "HR",
      "table-name": "ORDERS"
    },
    "parallel-load": {
      "type": "partitions-auto"
    }
  }
]
}

```

Example Caricare una tabella con LOB utilizzando la modalità LOB limitati

L'esempio seguente carica una tabella ITEMS che include i LOB presenti sull'origine utilizzando la modalità LOB limitata (quella predefinita) con una dimensione massima non troncata di 100 MB. Qualsiasi LOB di dimensioni superiori a questa viene troncato a 100 MB. Tutti i LOB vengono caricati in linea assieme a tutti gli altri tipi di dati di colonna.

```

{
  "rules": [{
    "rule-type": "selection",

```



```

    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "INV",
      "table-name": "ITEMS"
    },
    "lob-settings": {
      "bulk-max-size": "100000"
    }
  }
]
}

```

Example Caricare una tabella con LOB utilizzando la modalità standard LOB completi

L'esempio seguente carica una tabella ITEMS presente sull'origine, compresi tutti i suoi LOB, senza troncamento utilizzando la modalità LOB completi. Tutti i LOB, indipendentemente dalle dimensioni, vengono caricati separatamente da altri tipi di dati utilizzando un'operazione di ricerca sulla tabella di origine per ogni LOB.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",

```

```

        "rule-id": "2",
        "rule-name": "2",
        "object-locator": {
            "schema-name": "INV",
            "table-name": "ITEMS"
        },
        "lob-settings": {
            "mode": "unlimited",
            "bulk-max-size": "0"
        }
    }
]
}

```

Example Caricare una tabella con LOB utilizzando la modalità combinazione LOB completi

L'esempio seguente carica una tabella ITEMS presente sull'origine, compresi tutti i suoi LOB, senza troncamento utilizzando la modalità combinazione LOB completi. Tutti i LOB di dimensione inferiore ai 100 MB vengono caricati inline insieme ad altri tipi di dati, come accade nella modalità LOB limitati. Tutti i LOB di dimensioni superiori a 100 MB vengono caricati separatamente dagli altri tipi di dati. Questo carico separato utilizza una ricerca per ciascun LOB di questo tipo nella tabella di origine, come nella modalità LOB completa standard.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "INV",
      "table-name": "ITEMS"
    },
    "lob-settings": {

```

```

        "mode": "unlimited",
        "bulk-max-size": "100000"
    }
}
]
}

```

Example Caricare una tabella con i LOB utilizzando le impostazioni per i LOB dell'attività

L'esempio seguente carica una tabella ITEMS presente sull'origine, compresi tutti i suoi LOB, utilizzando le impostazioni per i LOB dell'attività. L'impostazione a 100 MB di `bulk-max-size` viene ignorata e lasciata solo per un più rapido ripristino delle modalità `limited` o `unlimited`.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "%",
      "table-name": "%"
    },
    "rule-action": "include"
  },
  {
    "rule-type": "table-settings",
    "rule-id": "2",
    "rule-name": "2",
    "object-locator": {
      "schema-name": "INV",
      "table-name": "ITEMS"
    },
    "lob-settings": {
      "mode": "none",
      "bulk-max-size": "100000"
    }
  }
]
}

```

Utilizzo di filtri di origine

Puoi utilizzare i filtri di origine per limitare il numero e il tipo di record trasferiti dall'origine alla destinazione. Ad esempio, puoi specificare che solo i dipendenti con un'ubicazione di sede vengano spostati al database di destinazione. I filtri fanno parte di una regola di selezione. I filtri vengono applicati su una colonna di dati.

I filtri di origine devono seguire questi vincoli:

- Una regola di selezione può avere uno o più filtri o nessun filtro.
- Ogni filtro può avere una o più condizioni di filtro.
- Se viene utilizzato più di un filtro, l'elenco di filtri viene combinato come se venisse utilizzato un operatore AND tra i filtri.
- Se più di una condizione di filtro viene utilizzata all'interno di un singolo filtro, l'elenco delle condizioni di filtro viene combinato come se venisse utilizzato un operatore OR tra le condizioni di filtro.
- I filtri vengono applicati solo quando `rule-action = 'include'`.
- I filtri richiedono un nome di colonna e un elenco di condizioni di filtro. Le condizioni di filtro devono avere un operatore associato a un valore, due valori o nessun valore, a seconda dell'operatore.
- I nomi delle colonne, i nomi delle tabelle e i nomi delle viste prevedono una distinzione tra lettere maiuscole e minuscole. Oracle e Db2 devono sempre utilizzare lettere MAIUSCOLE.
- I filtri supportano solo tabelle con nomi esatti. I filtri non supportano i caratteri jolly.

Le seguenti limitazioni si applicano all'utilizzo dei filtri di origine:

- I filtri non calcolano le colonne delle right-to-left lingue.
- Non applicare filtri alle colonne LOB.
- Applicare filtri solo alle colonne immutabili, che dopo la creazione non vengono aggiornate. Se i filtri di origine vengono applicati alle colonne mutabili, che possono essere aggiornate dopo la creazione, è possibile che si verifichi un comportamento indesiderato.

Ad esempio, un filtro per escludere o includere righe specifiche in una colonna esclude o include sempre le righe specificate, anche se queste vengono modificate in un secondo momento. Supponi di escludere o includere le righe da 1 a 10 nella colonna A e di modificarle in seguito affinché diventino le righe da 11 a 20. In questo caso, le righe continuano ad essere escluse o incluse anche quando i dati non sono più gli stessi.

Analogamente, supponiamo che una riga al di fuori dell'ambito del filtro venga successivamente aggiornata (o aggiornata ed eliminata) e che venga esclusa o inclusa in base a quanto definito dal filtro. In tal caso, viene replicata sulla destinazione.

Le seguenti preoccupazioni aggiuntive si applicano all'utilizzo dei filtri di origine:

- Si consiglia di creare un indice utilizzando le colonne incluse nella definizione del filtro e la chiave primaria.

Creazione di regole di filtro di origine in formato JSON

È possibile creare filtri di origine utilizzando il parametro JSON `filters` di una regola di selezione. Il parametro `filters` specifica una matrice di uno o più oggetti JSON. Ogni oggetto dispone di parametri che specificano il tipo di filtro di origine, il nome delle colonne e condizioni di filtro. Queste condizioni di filtro includono uno o più operatori filtro e i relativi valori.

La tabella seguente mostra i parametri utilizzati per specificare il filtro sull'origine in un oggetto `filters`.

Parametro	Valore
<code>filter-type</code>	<code>source</code>
<code>column-name</code>	Un parametro con il nome della colonna di origine a cui si desidera applicare il filtro. Per il nome è prevista una distinzione tra maiuscole e minuscole.
<code>filter-conditions</code>	Una matrice di uno o più oggetti che contengono un parametro <code>filter-operator</code> e zero o più parametri associati, a seconda del valore <code>filter-operator</code> .
<code>filter-operator</code>	Un parametro con uno dei seguenti valori: <ul style="list-style-type: none"> • <code>lte</code>: minore o uguale a un valore • <code>ste</code>: minore o uguale a un valore (alias <code>lte</code>) • <code>gte</code>: maggiore o uguale a un valore • <code>eq</code>: uguale a un valore

Parametro	Valore
	<ul style="list-style-type: none"> • <code>noteq</code>: non uguale a un valore • <code>between</code>: uguale o compreso tra due valori • <code>notbetween</code> : non uguale o compreso tra due valori • <code>null</code>: valori NULL • <code>notnull</code>: valori non NULL
<code>value</code> o	Zero o più parametri associati a <code>filter-operator</code> :
<code>start-value</code> e <code>end-value</code> o	<ul style="list-style-type: none"> • Se <code>filter-operator</code> è <code>lte</code>, <code>ste</code>, <code>gte</code>, <code>eq</code> o <code>noteq</code>, si usa <code>value</code> per specificare un parametro.
nessun valore	<ul style="list-style-type: none"> • Se <code>filter-operator</code> è <code>between</code> o <code>notbetween</code> , si usa <code>start-value</code> e <code>end-value</code> per specificare due parametri. • Se <code>filter-operator</code> è <code>null</code> o <code>notnull</code>, non si specifica alcun parametro.

I seguenti esempi mostrano alcune delle modalità più comuni per l'utilizzo di filtri sull'origine.

Example Filtro singolo

Il filtro seguente replica tutti i dipendenti con `empid >= 100` sul database di destinazione.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empid",
      "filter-conditions": [{
        "filter-operator": "gte",
        "value": "50"
      }
    ]
  }
  ]
}
```

```

    },{
      "filter-operator": "noteq",
      "value": "100"
    }
  ]
}

```

Example Più operatori di filtro

Il filtro seguente applica più operatori di filtro a una singola colonna di dati. Il filtro replica tutti i dipendenti con (empid <= 10) O (empid is between 50 and 75) O (empid >= 100) sul database di destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empid",
      "filter-conditions": [{
        "filter-operator": "lte",
        "value": "10"
      }],
      "filter-operator": "between",
      "start-value": "50",
      "end-value": "75"
    }, {
      "filter-operator": "gte",
      "value": "100"
    }
  ]
}

```

Example Più filtri

I seguenti filtri applicano più filtri a due colonne in una tabella. Il filtro replica tutti i dipendenti con (empid <= 100) E (dept = tech) sul database di destinazione.

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empid",
      "filter-conditions": [{
        "filter-operator": "lte",
        "value": "100"
      }]
    }, {
      "filter-type": "source",
      "column-name": "dept",
      "filter-conditions": [{
        "filter-operator": "eq",
        "value": "tech"
      }]
    }
  ]
}]
}
```

Example Filtro dei valori NULL

Il seguente filtro mostra come filtrare i valori vuoti. Replica tutti i dipendenti con dept = NULL sul database di destinazione.

```
{
  "rules": [{
```



```

    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "dept",
      "filter-conditions": [{
        "filter-operator": "null"
      }]
    }]
  }]
}

```

Example Filtro utilizzando gli operatori NOT

Alcuni operatori possono essere utilizzati in forma negativa. Il filtro seguente replica tutti i dipendenti con (empid is < 50) OR (empid is > 75) sul database di destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empid",
      "filter-conditions": [{
        "filter-operator": "notbetween",
        "start-value": "50",
        "end-value": "75"
      }]
    }]
  }]
}

```

```

    ]]
  ]]
}

```

Example Utilizzo di operatori di filtro misti

A partire dalla AWS DMS versione 3.5.0, puoi combinare operatori inclusivi e operatori negativi.

Il filtro seguente replica tutti i dipendenti con (empid != 50) AND (dept is not NULL) sul database di destinazione.

```

{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empid",
      "filter-conditions": [{
        "filter-operator": "noteq",
        "value": "50"
      }]
    }, {
      "filter-type": "source",
      "column-name": "dept",
      "filter-conditions": [{
        "filter-operator": "notnull"
      }]
    }]
  }]
}

```

Tieni presente quanto segue quando utilizzi null con altri operatori di filtro:

- L'utilizzo combinato di condizioni di filtro inclusive, negative e null all'interno dello stesso filtro non replica i record con valori NULL.
- L'utilizzo combinato di condizioni di filtro negative e null senza condizioni di filtro inclusive all'interno dello stesso filtro non replica i dati.
- L'utilizzo di condizioni di filtro negative senza una condizione di filtro null impostata in modo esplicito non replica i record con valori NULL.

Applicazione di filtri in base a ora e data

Quando si selezionano i dati da importare, è possibile specificare una data o un'ora come parte dei criteri di filtro. AWS DMS utilizza il formato della data YYYY-MM-GG e il formato dell'ora YYYY-MM-DD HH:MM:SS per il filtraggio. AWS DMS Le funzioni di confronto seguono le convenzioni SQLite. Per ulteriori informazioni sui tipi di dati SQLite e sui confronti tra date, consulta la sezione relativa ai [tipi di dati in SQLite versione 3](#) nella documentazione di SQLite.

Il seguente filtro mostra come filtrare una data. Replica tutti i dipendenti con `empstartdate >= January 1, 2002` sul database di destinazione.

Example Filtro per data singola

```
{
  "rules": [{
    "rule-type": "selection",
    "rule-id": "1",
    "rule-name": "1",
    "object-locator": {
      "schema-name": "test",
      "table-name": "employee"
    },
    "rule-action": "include",
    "filters": [{
      "filter-type": "source",
      "column-name": "empstartdate",
      "filter-conditions": [{
        "filter-operator": "gte",
        "value": "2002-01-01"
      }]
    }]
  }]
}
```

}

Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività

Una valutazione di pre-migrazione analizza i componenti specifici di un'attività di migrazione del database per identificare eventuali problemi che potrebbero impedire l'esecuzione dell'attività di migrazione come previsto. Questa valutazione consente di identificare e risolvere i problemi prima di eseguire un'attività nuova o modificata. Ciò consente di evitare ritardi legati agli errori delle attività causati dalla mancanza di requisiti o da limitazioni note.

AWS DMS fornisce l'accesso a due diverse opzioni per le valutazioni preliminari alla migrazione:

- Valutazione del tipo di dati: un rapporto precedente che fornisce un ambito limitato di valutazioni.
- Esecuzione della valutazione prima della migrazione: contiene vari tipi di valutazioni individuali, inclusi i risultati della valutazione del tipo di dati.

Note

Se si sceglie un'esecuzione di valutazione prima della migrazione, non è necessario scegliere separatamente una valutazione del tipo di dati.

Queste opzioni sono descritte nei seguenti argomenti:

- [Specifica, avvio e visualizzazione delle esecuzioni della valutazione di pre-migrazione:](#) un'esecuzione di valutazione prima della migrazione (consigliata) specifica una o più valutazioni individuali da eseguire in base a una configurazione dell'attività di migrazione nuova o esistente. Ogni singola valutazione valuta un elemento specifico di un database di origine e/o di destinazione supportato dal punto di vista di criteri quali il tipo di migrazione, gli oggetti supportati, la configurazione dell'indice e altre impostazioni delle attività, come le mappature delle tabelle che identificano gli schemi e le tabelle da migrare.

Ad esempio, una valutazione individuale potrebbe valutare quali tipi di dati di origine o formati di chiave primaria possono o non possono essere migrati, possibilmente in base alla versione del motore. AWS DMS Puoi avviare e visualizzare i risultati dell'ultima valutazione eseguita e visualizzare i risultati di tutte le esecuzioni di valutazione precedenti per un'attività utilizzando la

Console di AWS DMS gestione o utilizzando gli SDK AWS CLI e per accedere all' AWS DMS API. Puoi anche visualizzare i risultati delle precedenti esecuzioni di valutazione per un'attività in un bucket Amazon S3 per cui hai selezionato per AWS DMS archiviare questi risultati.

Note

Il numero e i tipi di valutazioni individuali disponibili possono aumentare nel tempo. Per ulteriori informazioni sugli aggiornamenti periodici, consulta [Specifiche delle valutazioni individuali](#).

- [Avvio e visualizzazione delle valutazioni dei tipi di dati \(Legacy\)](#): una valutazione del tipo di dati (legacy) restituisce i risultati di un singolo tipo di valutazione di premigrazione in un'unica struttura JSON: i tipi di dati che potrebbero non essere migrati correttamente in un'istanza di database di origine relazionale supportata. Questo report restituisce i risultati per tutti i tipi di dati problematici presenti in ogni schema e tabella del database di origine selezionato per la migrazione.

Creazione di prerequisiti per le valutazioni preliminari alla migrazione

Questa sezione descrive le risorse Amazon S3 e IAM necessarie per creare una valutazione di premigrazione.

Creare un bucket S3

AWS DMS archivia i report di valutazione della premigrazione in un bucket S3. Per creare il bucket S3, procedi come segue:

1. [Accedi AWS Management Console e apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3/](https://console.aws.amazon.com/s3/).
2. Seleziona Crea bucket.
3. *Nella pagina **Crea bucket**, inserisci un nome univoco globale che includa il nome di accesso per il bucket, ad esempio dms-bucket- yoursignin.*
4. Regione AWS Scegli l'opzione per l'attività di migrazione DMS.
5. Lascia le impostazioni rimanenti così come sono e scegli Crea bucket.

Creazione di risorse IAM

DMS utilizza un ruolo e una policy IAM per accedere al bucket S3 e archiviare i risultati della valutazione pre-migrazione.

Per creare la policy IAM, procedi come segue:

1. Accedi AWS Management Console e apri la console IAM all'[indirizzo https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. Nel pannello di navigazione, selezionare Policies (Policy).
3. Scegli Create Policy (Crea policy).
4. Nella pagina Crea policy seleziona la scheda JSON.
5. Incolla il seguente codice JSON nell'editor per sostituire il codice di esempio. Sostituisci *my-bucket* con il nome del bucket Amazon S3 che hai creato nella sezione precedente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObject",
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::my-bucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::my-bucket"
      ]
    }
  ]
}
```

```
}
```

6. Scegli Avanti: tag, quindi scegli e Avanti: revisione.
7. Per Nome* immetti **DMSPremigrationAssessmentS3Policy**, quindi scegli Crea policy.

Per creare il ruolo IAM, procedi come segue:

1. Nella console IAM, nel riquadro di navigazione, scegli Ruoli.
2. Scegli Crea ruolo.
3. Nella pagina Seleziona un'entità attendibile scegli Servizio AWS per Tipo di entità attendibile. Per i casi d'uso per altri AWS servizi, scegli DMS.
4. Seleziona la casella di controllo DMS, quindi scegli Avanti.
5. Nella pagina Aggiungi autorizzazioni, scegli PremigrationAssessmentDMS S3Policy. Seleziona Successivo.
6. Nella pagina Nomina, verifica e crea immetti **DMSPremigrationAssessmentS3Role** per Nome ruolo e scegli Crea ruolo.
7. Nella pagina Ruoli immetti **DMSPremigrationAssessmentS3Role** per Nome ruolo. Scegli DMS S3Role. PremigrationAssessment
8. Nella pagina DMS PremigrationAssessment S3Role, scegli la scheda Relazioni di fiducia. Seleziona Modifica policy di attendibilità.
9. Nella pagina Modifica policy di attendibilità incolla il seguente codice JSON nell'editor, sostituendo il testo esistente.

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

Questa policy concede a DMS l'`sts:AssumeRole` autorizzazione a inserire i risultati della valutazione pre-migrazione nel bucket S3.

10. Scegli **Aggiorna policy**.

Specifica, avvio e visualizzazione delle esecuzioni della valutazione di pre-migrazione

Una valutazione pre-migrazione specifica una o più valutazioni individuali da eseguire in base a una configurazione di attività di migrazione nuova o esistente. Ogni singola valutazione valuta un elemento specifico del database di origine o di destinazione in base a considerazioni quali il tipo di migrazione, gli oggetti supportati, la configurazione dell'indice e altre impostazioni delle attività, come le mappature delle tabelle che identificano gli schemi e le tabelle da migrare. Ad esempio, una valutazione individuale potrebbe valutare quali tipi di dati di origine o formati di chiave primaria possono e non possono essere migrati.

Specifica delle valutazioni individuali

Quando si crea una nuova esecuzione di valutazione, è possibile scegliere di eseguire alcune o tutte le valutazioni individuali applicabili alla configurazione dell'attività.

AWS DMS supporta le esecuzioni di valutazione prima della migrazione per i seguenti motori di database relazionali di origine e destinazione:

- [Valutazioni Oracle](#)
- [Valutazioni di Sql Server](#)
- [Valutazioni MySQL](#) (include l'edizione compatibile con Mariadb e Amazon Aurora MySQL)
- [Valutazioni PostgreSQL](#) (include l'edizione compatibile con Amazon Aurora PostgreSQL)

Avvio e visualizzazione delle esecuzioni della valutazione di pre-migrazione

Puoi avviare un'esecuzione di valutazione pre-migrazione per un'attività di migrazione nuova o esistente utilizzando la Console di AWS DMS gestione, l'API. AWS CLI AWS DMS

Per avviare l'esecuzione di una valutazione di pre-migrazione per un'attività nuova o esistente

1. Dalla pagina **Attività di migrazione del database** nella console di gestione AWS DMS effettua una delle seguenti operazioni:

- Per creare una nuova attività e valutarla, scegli Crea attività. Viene visualizzata la pagina Crea attività di migrazione del database.
 1. Immetti le impostazioni necessarie per creare l'attività, inclusa la mappatura delle tabelle.
 2. Nella sezione Valutazione preliminare, la casella di controllo Esegui la valutazione preliminare è selezionata. Questa pagina contiene le opzioni per specificare un'esecuzione di valutazione per la nuova attività.

Note

Quando si crea una nuova attività, l'abilitazione di un'esecuzione della valutazione di pre-migrazione disattiva l'opzione di avvio automatico dell'attività al momento della creazione dell'attività. È possibile avviare l'attività manualmente al termine dell'esecuzione della valutazione.

- Per valutare un'attività esistente, scegli l'identificatore per un'attività esistente nella pagina Attività di migrazione del database. Viene visualizzata la pagina dell'attività esistente scelta:
 1. Scegli Operazioni e seleziona Crea una valutazione di pre-migrazione. Viene visualizzata una pagina Crea una valutazione di pre-migrazione con le opzioni per specificare l'esecuzione della valutazione per l'attività esistente.
 2. Inserisci un nome univoco per l'esecuzione della valutazione o lascia il valore predefinito.
 3. Seleziona le valutazioni individuali disponibili che desideri includere in questa esecuzione della valutazione. È possibile selezionare solo le valutazioni individuali disponibili in base alle impostazioni correnti delle attività. Per impostazione predefinita, tutte le valutazioni individuali disponibili sono abilitate e selezionate.
 4. Cerca e scegli una cartella e un bucket Amazon S3 nel tuo account per archiviare il report dei risultati della valutazione. Per informazioni sulla configurazione delle risorse per le esecuzioni di valutazione, consulta [Creazione di prerequisiti per le valutazioni preliminari alla migrazione](#).
 5. Seleziona o inserisci un ruolo IAM con accesso completo dell'account al bucket e alla cartella Amazon S3 scelti. Per informazioni sulla configurazione delle risorse per le esecuzioni di valutazione, vedere [Creazione di prerequisiti per le valutazioni preliminari alla migrazione](#).
 6. Facoltativamente, è possibile scegliere un'impostazione per crittografare il report dei risultati della valutazione nel bucket Amazon S3. Per informazioni sulla crittografia dei bucket S3, consulta [Impostazione del comportamento di crittografia lato server predefinito per i bucket Amazon S3](#).

7. Scegli Crea attività per una nuova attività o scegli Crea per un'attività esistente.

Viene visualizzata la pagina Attività di migrazione del database che elenca l'attività nuova o modificata con lo Stato di Creazione in corso... e un messaggio nel banner che indica che l'esecuzione della valutazione di pre-migrazione avrà inizio una volta creata l'attività.

AWS DMS fornisce l'accesso alle più recenti e a tutte le precedenti valutazioni di premigrazione utilizzando la Console di AWS DMS gestione, l'API o l'AWS CLI.

Per visualizzare i risultati dell'esecuzione della valutazione

1. Dalla console di AWS DMS gestione, scegli l'identificatore per l'attività esistente nella pagina Attività di migrazione del database. Viene visualizzata la pagina delle attività esistenti.
2. Scegli la scheda Valutazioni di pre-migrazione nella pagina delle attività esistenti. In quella pagina viene aperta una sezione sulle valutazioni preliminari alla migrazione che mostra i risultati delle esecuzioni di valutazione, elencati per nome, in ordine cronologico inverso. Il risultato più recente viene visualizzato in cima all'elenco. Scegliete il nome dell'esecuzione di valutazione di cui desiderate visualizzare i risultati.

I risultati di queste esecuzioni della valutazione iniziano con il nome dell'ultima esecuzione della valutazione e una panoramica dello stato seguita da un elenco delle valutazioni individuali specificate e del relativo stato. È quindi possibile esplorare i dettagli dello stato di ogni singola valutazione scegliendone il nome nell'elenco, con i risultati disponibili fino al livello delle colonne della tabella.

Sia la panoramica dello stato di un'esecuzione della valutazione sia ogni valutazione individuale mostrano il valore Stato. Questo valore indica lo stato generale dell'esecuzione della valutazione e uno stato simile per ogni valutazione individuale. Di seguito è riportato un elenco dei valori di Stato per l'esecuzione della valutazione:

- "cancelling": l'esecuzione della valutazione è stata annullata.
- "deleting": l'esecuzione della valutazione è stata eliminata.
- "failed": almeno una valutazione individuale è stata completata con lo stato failed.
- "error-provisioning": si è verificato un errore interno durante il provisioning delle risorse (con stato provisioning).
- "error-executing": si è verificato un errore interno durante l'esecuzione delle valutazioni individuali (con stato running).

- "invalid state": l'esecuzione della valutazione si trova in uno stato sconosciuto.
- "passed": tutte le valutazioni individuali sono state completate e nessuna ha lo stato failed.
- "provisioning": le risorse necessarie per eseguire le valutazioni individuali sono in fase di provisioning.
- "running": le valutazioni individuali sono in esecuzione.
- "starting": l'esecuzione della valutazione è iniziata, ma non è ancora stato eseguito il provisioning delle risorse per le valutazioni individuali.
- "warning": almeno una valutazione individuale è stata completata con lo stato warning.

Di seguito è riportato un elenco dei valori di Stato per ogni valutazione individuale dell'esecuzione della valutazione:

- "cancelled": la valutazione individuale è stata annullata come parte dell'annullamento dell'esecuzione della valutazione.
- "error": la valutazione individuale non è stata completata.
- "failed": la valutazione individuale è stata completata con un risultato di convalida negativo. Visualizza i dettagli del risultato per ulteriori informazioni.
- "invalid state": la valutazione individuale è in uno stato sconosciuto.
- "passed": la valutazione individuale è stata completata con un risultato di convalida positivo.
- "pending": la valutazione individuale è in attesa di essere eseguita.
- "running": la valutazione individuale è in esecuzione.
- "warning": la valutazione individuale è stata completata con un risultato di convalida di avviso. Visualizza i dettagli del risultato per ulteriori informazioni.

Puoi anche visualizzare i file JSON per i risultati dell'esecuzione della valutazione su Amazon S3.

Per visualizzare i file JSON per l'esecuzione della valutazione su Amazon S3

1. Dalla console di AWS DMS gestione, scegli il link del bucket Amazon S3 mostrato nella panoramica dello stato dell'esecuzione della valutazione. Viene visualizzato un elenco di cartelle e altri oggetti Amazon S3 memorizzati nel bucket. Se i risultati sono archiviati in una cartella del bucket, apri la cartella.
2. I risultati dell'esecuzione della valutazione sono disponibili in diversi file JSON. Un file `summary.json` contiene i risultati complessivi dell'esecuzione della valutazione. I file rimanenti

sono denominati ciascuno in base a una valutazione individuale specificata per l'esecuzione, ad esempio `unsupported-data-types-in-source.json`. Questi file contengono ciascuno i risultati della valutazione individuale corrispondente dell'esecuzione della valutazione scelta.

Per avviare e visualizzare i risultati delle esecuzioni di valutazione pre-migrazione per un'attività di migrazione esistente, puoi eseguire i seguenti comandi CLI AWS DMS e operazioni API:

- CLI: [describe-applicable-individual-assessments](#), API: [DescribeApplicableIndividualAssessments](#): fornisce un elenco di valutazioni individuali che è possibile specificare per una nuova esecuzione della valutazione di pre-migrazione, in base a uno o più parametri di configurazione dell'attività.
- CLI: [start-replication-task-assessment-run](#), API: [StartReplicationTaskAssessmentRun](#): avvia una nuova esecuzione della valutazione di pre-migrazione per una o più valutazioni individuali di un'attività di migrazione esistente.
- CLI: [describe-replication-task-assessment-runs](#), API: [DescribeReplicationTaskAssessmentRuns](#): restituisce un elenco impaginato di esecuzioni della valutazione di pre-migrazione in base alle impostazioni di filtro.
- CLI: [describe-replication-task-individual-assessments](#), API: [DescribeReplicationTaskIndividualAssessments](#): restituisce un elenco impaginato di valutazioni individuali in base alle impostazioni di filtro.
- CLI: [cancel-replication-task-assessment-run](#), API: [CancelReplicationTaskAssessmentRun](#): annulla, ma non elimina, una singola esecuzione della valutazione di pre-migrazione.
- CLI: [delete-replication-task-assessment-run](#), API: [DeleteReplicationTaskAssessmentRun](#): elimina il record di una singola esecuzione della valutazione di pre-migrazione.

Valutazioni individuali

Questa sezione descrive le valutazioni individuali di premigrazione.

Per creare una valutazione pre-migrazione individuale utilizzando l' AWS DMS API, utilizza la chiave API elencata per il `IncludeOnly` parametro dell'azione. [StartReplicationTaskAssessmentRun](#)

Argomenti

- [Valutazioni per tutti i tipi di endpoint](#)

- [Valutazioni Oracle](#)
- [Valutazioni di Sql Server](#)
- [Valutazioni MySQL](#)
- [Valutazioni Mariadb](#)
- [Valutazioni PostgreSQL](#)

Valutazioni per tutti i tipi di endpoint

Questa sezione descrive le valutazioni individuali di pre-migrazione per tutti i tipi di endpoint.

Argomenti

- [Tipi di dati supportati](#)
- [Vengono utilizzati oggetti di grandi dimensioni \(LOB\), ma le colonne LOB di destinazione non possono essere annullate](#)
- [Tabella di origine con oggetti di grandi dimensioni \(LOB\) ma senza chiavi primarie o vincoli univoci](#)
- [Tabella di origine senza chiave primaria solo per attività CDC o a pieno carico e CDC](#)
- [Tabella di destinazione senza chiavi primarie solo per le attività CDC](#)
- [Tipi di chiavi primarie di origine non supportati: chiavi primarie composite](#)

Tipi di dati supportati

Chiave API: `unsupported-data-types-in-source`

Verifica i tipi di dati nell'endpoint di origine che DMS non supporta. Non tutti i tipi di dati possono essere migrati tra i motori.

Vengono utilizzati oggetti di grandi dimensioni (LOB), ma le colonne LOB di destinazione non possono essere annullate

Chiave API: `full-lob-not-nullable-at-target`

Verifica l'annullabilità di una colonna LOB nella destinazione quando la replica utilizza la modalità LOB completa o la modalità LOB in linea. DMS richiede che una colonna LOB sia nulla quando si utilizzano queste modalità LOB. Questa valutazione richiede che i database di origine e di destinazione siano relazionali.

Tabella di origine con oggetti di grandi dimensioni (LOB) ma senza chiavi primarie o vincoli univoci

Chiave API: `table-with-lob-but-without-primary-key-or-unique-constraint`

Verifica la presenza di tabelle di origine con LOB ma senza una chiave primaria o una chiave univoca. Una tabella deve avere una chiave primaria o una chiave unica per consentire a DMS di migrare i LOB. Questa valutazione richiede che il database di origine sia relazionale.

Tabella di origine senza chiave primaria solo per attività CDC o a pieno carico e CDC

Chiave API: `table-with-no-primary-key-or-unique-constraint`

Verifica la presenza di una chiave primaria o di una chiave univoca nelle tabelle di origine per una migrazione CDC (FullLoad and Change Data Capture) o una migrazione solo CDC. La mancanza di una chiave primaria o di una chiave unica può causare problemi di prestazioni durante la migrazione al CDC. Questa valutazione richiede che il database di origine sia relazionale e che il tipo di migrazione includa CDC.

Tabella di destinazione senza chiavi primarie solo per le attività CDC

Chiave API: `target-table-has-unique-key-or-primary-key-for-cdc`

Verifica la presenza di una chiave primaria o di una chiave univoca nelle tabelle di destinazione già create per una migrazione sola CDC. La mancanza di una chiave primaria o di una chiave univoca può causare scansioni complete della tabella nella destinazione quando DMS applica aggiornamenti ed eliminazioni. Ciò può causare problemi di prestazioni durante la migrazione al CDC. Questa valutazione richiede che il database di destinazione sia relazionale e che il tipo di migrazione includa CDC.

Tipi di chiavi primarie di origine non supportati: chiavi primarie composite

Chiave API: `unsupported-source-pk-type-for-elasticsearch-target`

Verifica la presenza di chiavi primarie composite nelle tabelle di origine durante la migrazione ad Amazon OpenSearch Service. La chiave primaria della tabella di origine deve essere costituita da un'unica colonna. Questa valutazione richiede che il database di origine sia relazionale e il database di destinazione sia DynamoDB.

Note

DMS supporta la migrazione di un database di origine verso un OpenSearch Service Target in cui la chiave primaria di origine è costituita da più colonne.

Valutazioni Oracle

Questa sezione descrive le valutazioni individuali di pre-migrazione per le attività di migrazione che utilizzano un endpoint di origine Oracle.

Note

Per utilizzare le valutazioni di pre-migrazione riportate in questa sezione, è necessario aggiungere le seguenti autorizzazioni a `dms_user`:

```
grant select on gv_$parameter to dms_user;
grant select on v_$instance to dms_user;
grant select on v_$version to dms_user;
grant select on gv_$ASM_DISKGROUP to dms_user;
grant select on gv_$database to dms_user;
grant select on DBA_DB_LINKS to to dms_user;
grant select on gv_$log_History to dms_user;
grant select on gv_$log to dms_user;
grant select on dba_types to dms_user;
grant select on dba_users to dms_user;
grant select on dba_directories to dms_user;
```

Per ulteriori informazioni sulle autorizzazioni quando si utilizza Oracle come origine, consulta [Privilegi dell'account utente richiesti su una fonte Oracle autogestita per AWS DMS](#).

Argomenti

- [Controllo della registrazione supplementare a livello di database](#)
- [Verifica della creazione del collegamento del database richiesto per Standby](#)
- [Convalida Oracle per il tipo di dati LOB e la configurazione del lettore binario](#)
- [Verifica del CDB per il database](#)
- [Controllo della versione del database Oracle](#)

- [Convalida del metodo CDC Oracle per DMS](#)
- [Convalida della configurazione Oracle RAC per DMS](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni sulla destinazione](#)
- [Verifica se è necessaria una registrazione supplementare per tutte le colonne](#)
- [Verifica se la registrazione supplementare è abilitata su tabelle con chiavi primarie o uniche](#)
- [Verifica se sono presenti LOB e l'attività è configurata per la modalità Full SecureFile LOB](#)
- [Verifica se gli indici basati sulle funzioni vengono utilizzati nelle tabelle incluse nell'ambito dell'attività.](#)
- [Verifica se le tabelle temporanee globali vengono utilizzate nelle tabelle incluse nell'ambito dell'attività.](#)
- [Verifica se le tabelle organizzate a indice con un segmento di overflow vengono utilizzate nelle tabelle incluse nell'ambito dell'attività.](#)
- [Verifica se vengono utilizzate tabelle di nidificazione multilivello nelle tabelle incluse nell'ambito dell'attività.](#)
- [Verifica se vengono utilizzate colonne invisibili nelle tabelle incluse nell'ambito dell'attività.](#)
- [Verifica se nelle tabelle incluse nell'ambito dell'attività vengono utilizzate viste materializzate basate su una colonna ROWID.](#)
- [Verifica se viene utilizzata la funzione di reindirizzamento XML di Active Data Guard.](#)
- [Verifica se vengono utilizzate tabelle partizionate ibride.](#)
- [Verifica se vengono utilizzati account Oracle che utilizzano solo lo schema](#)
- [Verifica se vengono utilizzate colonne virtuali](#)
- [Verifica se i nomi delle tabelle definiti nell'ambito del task contengono apostrofi.](#)
- [Convalida se le colonne definite nell'ambito dell'attività hanno XMLTypeLong Raw tipi di dati o o e verifica la configurazione della modalità LOB nelle impostazioni dell'attività. Long](#)
- [Verifica se la versione Oracle di origine è supportata da. AWS DMS](#)
- [Verifica se la versione Oracle di destinazione è supportata da. AWS DMS](#)
- [Verifica se la versione Oracle di destinazione è supportata da. AWS DMS](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni necessarie per utilizzare la convalida dei dati.](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con Oracle ASM](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con Oracle non ASM](#)

- [Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con il metodo CopyToTempFolder](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Oracle Standby come sorgente](#)
- [Verifica se la sorgente DMS è connessa a un contenitore di applicazioni \(PDB\)](#)
- [Verifica se la tabella contiene tipi di dati XML inclusi nell'ambito dell'attività.](#)
- [Verifica se la modalità archivelog è abilitata nel database di origine.](#)
- [Convalida la conservazione dei log di archiviazione per RDS Oracle.](#)
- [Verifica se la tabella contiene tipi di dati estesi inclusi nell'ambito del task.](#)
- [Convalida la lunghezza del nome dell'oggetto incluso nell'ambito dell'attività.](#)
- [Verifica se la sorgente DMS è connessa a un PDB Oracle](#)
- [Verifica se la tabella contiene colonne spaziali incluse nell'ambito dell'attività.](#)
- [Verifica se la sorgente DMS è connessa a uno standby Oracle.](#)
- [Verifica se il tablespace del database di origine è crittografato utilizzando TDE.](#)
- [Verifica se il database di origine è Oracle ASM](#)

Controllo della registrazione supplementare a livello di database

Chiave API: `oracle-supplemental-db-level`

Questa valutazione di pre-migrazione verifica se è abilitata la registrazione supplementare minima a livello di database. È necessario abilitare la registrazione supplementare per utilizzare un database Oracle come origine per la migrazione.

Per abilitare la registrazione supplementare, esegui la query riportata di seguito:

```
ALTER DATABASE ADD SUPPLEMENTAL LOG DATA
```

Per ulteriori informazioni, consulta [Impostazione del log supplementare](#).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Verifica della creazione del collegamento del database richiesto per Standby

Chiave API: `oracle-validate-standby-dblink`

Questa valutazione preliminare alla migrazione verifica se Dblink è stato creato per l'origine del database di standby Oracle. AWSDMS_DBLINK è un prerequisito per l'utilizzo di un database in standby come origine. Quando si utilizza Oracle Standby come origine, AWS DMS per impostazione predefinita non convalida le transazioni aperte.

Per ulteriori informazioni, consulta [Utilizzo di un database Oracle autogestito come fonte per AWS DMS](#).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Convalida Oracle per il tipo di dati LOB e la configurazione del lettore binario

Chiave API: `oracle-binary-lob-source-validation`

Questa valutazione prima della migrazione verifica se Oracle LogMiner viene utilizzato per un endpoint del database Oracle versione 12c o successiva. AWS DMS non supporta Oracle LogMiner per le migrazioni di colonne LOB dalla versione 12c dei database Oracle. Questa valutazione verifica anche la presenza di colonne LOB e fornisce raccomandazioni appropriate.

Per configurare la migrazione in modo che non utilizzi Oracle LogMiner, aggiungi la seguente configurazione all'endpoint di origine:

```
useLogMinerReader=N;useBfile=Y;
```

Per ulteriori informazioni, consulta [Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC](#).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Verifica del CDB per il database

Chiave API: `oracle-validate-cdb`

Questa valutazione di pre-migrazione verifica se il database è un database container. AWS DMS non supporta il database root container multi-tenant (CDB\$ROOT).

Note

Questa valutazione è richiesta solo per Oracle 12.1.0.1 o versioni successive. Questa valutazione non è applicabile alle versioni Oracle precedenti alla 12.1.0.1.

Per ulteriori informazioni, consulta [Limitazioni all'uso di Oracle come fonte per AWS DMS](#).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Controllo della versione del database Oracle

Chiave API: `oracle-check-cdc-support-express-edition`

Questa valutazione di pre-migrazione verifica se il database di origine Oracle è Express Edition. AWS DMS non supporta CDC per Oracle Express Edition (Oracle Database XE) 18.0 e versioni successive.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Convalida del metodo CDC Oracle per DMS

Chiave API: `oracle-recommendation-cdc-method`

Questa valutazione di premigrazione convalida la generazione di redo log negli ultimi sette giorni e consiglia se utilizzare AWS DMS Binary Reader o Oracle for CDC. LogMiner

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni sulla scelta del metodo CDC da utilizzare, consulta [Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC](#).

Convalida della configurazione Oracle RAC per DMS

Chiave API: `oracle-check-rac`

Questa valutazione di pre-migrazione verifica se il database Oracle è un Real Application Cluster. I database Real Application Cluster devono essere configurati correttamente. Se il database è basato su RAC, si consiglia di utilizzare AWS DMS Binary Reader for CDC anziché Oracle. LogMiner

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC](#).

Verifica se l'utente DMS dispone delle autorizzazioni sulla destinazione

Chiave API: `oracle-validate-permissions-on-target`

Questa valutazione preliminare alla migrazione verifica se gli utenti DMS dispongono di tutte le autorizzazioni richieste sul database di destinazione.

Verifica se è necessaria una registrazione supplementare per tutte le colonne

Chiave API: `oracle-validate-supplemental-logging-all-columns`

Questa valutazione preliminare verifica, per le tabelle menzionate nell'ambito dell'attività, se è stata aggiunta una registrazione supplementare a tutte le colonne di tabelle senza una chiave primaria o unica. Senza una registrazione supplementare su tutte le colonne per una tabella priva di una chiave primaria o unica, l' `before-and-after` immagine dei dati non sarà disponibile nei redo log. DMS richiede una registrazione supplementare per le tabelle senza una chiave primaria o unica per generare istruzioni DML.

Verifica se la registrazione supplementare è abilitata su tabelle con chiavi primarie o uniche

Chiave API: `oracle-validate-supplemental-logging-for-pk`

Questa valutazione premigratoria verifica se la registrazione supplementare è abilitata per le tabelle con una chiave primaria o un indice univoco e verifica anche se `AddSupplementalLogging` è abilitata a livello di endpoint. Per garantire che DMS possa replicare le modifiche, è possibile aggiungere manualmente una registrazione supplementare a livello di tabella in base alla chiave primaria o alla chiave univoca oppure utilizzare l'impostazione dell'endpoint `AddSupplementalLogging = true` con un utente DMS con l'autorizzazione ALTER su qualsiasi tabella replicata.

Verifica se sono presenti LOB e l'attività è configurata per la modalità Full SecureFile LOB

Chiave API: `oracle-validate-securefile-lob`

Questa valutazione premigratoria verifica la presenza di SecureFile LOB nelle tabelle che rientrano nell'ambito dell'attività e ne verifica le impostazioni LOB. È importante notare che i SecureFile LOB sono attualmente supportati solo in modalità FULL LOB. Valuta la possibilità di assegnare le tabelle LOB a un'attività separata per migliorare le prestazioni, poiché l'esecuzione di attività in modalità LOB completa può comportare un rallentamento delle prestazioni.

Verifica se gli indici basati sulle funzioni vengono utilizzati nelle tabelle incluse nell'ambito dell'attività.

Chiave API: `oracle-validate-function-based-indexes`

Questa valutazione preliminare alla migrazione verifica la presenza di indici basati su funzioni nelle tabelle che rientrano nell'ambito dell'attività. Tieni presente che AWS DMS non supporta la replica di indici basati su funzioni. Prendi in considerazione la possibilità di creare gli indici dopo la migrazione sul database di destinazione.

Verifica se le tabelle temporanee globali vengono utilizzate nelle tabelle incluse nell'ambito dell'attività.

Chiave API: `oracle-validate-global-temporary-tables`

Questa valutazione preliminare verifica se le tabelle temporanee globali vengono utilizzate nell'ambito della mappatura delle tabelle delle attività. Tieni presente che AWS DMS non supporta la migrazione o la replica di tabelle temporanee globali.

Verifica se le tabelle organizzate a indice con un segmento di overflow vengono utilizzate nelle tabelle incluse nell'ambito dell'attività.

Chiave API: `oracle-validate-iot-overflow-segments`

Verifica se le tabelle organizzate a indice con un segmento di overflow vengono utilizzate nelle tabelle incluse nell'ambito dell'attività. AWS DMS non supporta CDC per le tabelle organizzate a indice con un segmento di overflow.

Verifica se vengono utilizzate tabelle di nidificazione multilivello nelle tabelle incluse nell'ambito dell'attività.

Chiave API: `oracle-validate-more-than-one-nesting-table-level`

Questa valutazione preliminare alla migrazione verifica il livello di nidificazione della tabella nidificata utilizzata nell'ambito dell'attività. AWS DMS supporta solo un livello di nidificazione delle tabelle.

Verifica se vengono utilizzate colonne invisibili nelle tabelle incluse nell'ambito dell'attività.

Chiave API: `oracle-validate-invisible-columns`

Questa valutazione preliminare verifica se le tabelle utilizzate nell'ambito dell'attività hanno colonne invisibili. AWS DMS non migra i dati dalle colonne invisibili del database di origine. Per migrare le colonne invisibili, è necessario modificarle per renderle visibili.

Verifica se nelle tabelle incluse nell'ambito dell'attività vengono utilizzate viste materializzate basate su una colonna ROWID.

Chiave API: `oracle-validate-rowid-based-materialized-views`

Questa valutazione preliminare verifica se le viste materializzate utilizzate nella migrazione vengono create in base alla colonna ROWID. AWS DMS non supporta il tipo di dati ROWID o le viste materializzate basate su una colonna ROWID.

Verifica se viene utilizzata la funzione di reindirizzamento XML di Active Data Guard.

Chiave API: `oracle-validate-adg-redirect-dml`

Questa valutazione di premigrazione verifica se viene utilizzata la funzione di reindirizzamento DML Active Data Guard. Quando si utilizza Oracle 19.0 come origine, AWS DMS non supporta la funzione Data Guard DML Redirect.

Verifica se vengono utilizzate tabelle partizionate ibride.

Chiave API: `oracle-validate-hybrid-partitioned-tables`

Questa valutazione preliminare verifica se le tabelle partizionate ibride vengono utilizzate per le tabelle definite nell'ambito dell'attività.

Verifica se vengono utilizzati account Oracle che utilizzano solo lo schema

Chiave API: `oracle-validate-schema-only-accounts`

Questa valutazione preliminare alla migrazione verifica se nell'ambito del task sono presenti account Schema-Only.

Verifica se vengono utilizzate colonne virtuali

Chiave API: `oracle-validate-virtual-columns`

Questa valutazione preliminare alla migrazione verifica se l'istanza Oracle ha colonne virtuali nelle tabelle che rientrano nell'ambito del task.

Verifica se i nomi delle tabelle definiti nell'ambito del task contengono apostrofi.

Chiave API: `oracle-validate-names-with-apostrophes`

Questa valutazione preliminare verifica se le tabelle utilizzate nell'ambito dell'attività contengono apostrofi. AWS DMS non replica tabelle con nomi contenenti apostrofi. Se identificate, prendete in

considerazione la possibilità di rinominare tali tabelle. In alternativa, potete creare una vista o una vista materializzata senza apostrofi per caricare queste tabelle.

Convalida se le colonne definite nell'ambito dell'attività hanno **XMLTypeLong Raw** tipi di dati o o e verifica la configurazione della modalità LOB nelle impostazioni dell'attività. **Long**

Chiave API: `oracle-validate-limited-lob-mode-for-longs`

Questa valutazione preliminare verifica se le tabelle definite nell'ambito dell'attività hanno i tipi di dati o XMLType LongLong Raw, e verifica se l'impostazione dell'attività è configurata per utilizzare la modalità LOB a dimensione limitata. AWS DMS non supporta la replica di questi tipi di dati utilizzando la modalità FULL LOB. Valuta la possibilità di modificare l'impostazione dell'attività per utilizzare la modalità LOB a dimensione limitata dopo aver identificato le tabelle con tali tipi di dati.

Verifica se la versione Oracle di origine è supportata da. AWS DMS

Chiave API: `oracle-validate-supported-versions-of-source`

Questa valutazione preliminare verifica se la versione dell'istanza Oracle di origine è supportata da. AWS DMS

Verifica se la versione Oracle di destinazione è supportata da. AWS DMS

Chiave API: `oracle-validate-supported-versions-of-target`

Questa valutazione preliminare verifica se la versione dell'istanza Oracle di destinazione è supportata da. AWS DMS

Verifica se la versione Oracle di destinazione è supportata da. AWS DMS

Chiave API: `oracle-validate-supported-versions-of-target`

Questa valutazione preliminare verifica se la versione dell'istanza Oracle di destinazione è supportata da. AWS DMS

Verifica se l'utente DMS dispone delle autorizzazioni necessarie per utilizzare la convalida dei dati.

Chiave API: `oracle-prerequisites-privileges-of-validation-feature`

Questa valutazione premigratoria verifica se l'utente DMS dispone dei privilegi necessari per utilizzare DMS Data Validation. È possibile ignorare l'attivazione di questa convalida se non si intende utilizzare la convalida dei dati.

Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con Oracle ASM

Chiave API: `oracle-prerequisites-privileges-of-binary-reader-asm`

Questa valutazione preliminare verifica se l'utente DMS dispone dei privilegi necessari per utilizzare Binary Reader sull'istanza Oracle ASM. È possibile ignorare l'attivazione di questa valutazione se l'origine non è un'istanza Oracle ASM o se non si utilizza Binary Reader for CDC.

Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con Oracle non ASM

Chiave API: `oracle-prerequisites-privileges-of-binary-reader-non-asm`

Questa valutazione preliminare verifica se l'utente DMS dispone dei privilegi necessari per utilizzare Binary Reader sull'istanza Oracle non ASM. Questa valutazione è valida solo se si dispone di un'istanza Oracle non ASM.

Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Binary Reader con il metodo CopyToTempFolder

Chiave API: `oracle-prerequisites-privileges-of-binary-reader-copy-to-temp-folder`

Questa valutazione preliminare verifica se l'utente DMS dispone dei privilegi necessari per utilizzare Binary Reader con il metodo 'Copy to Temp Folder'. Questa valutazione è rilevante solo se si prevede di leggere le modifiche CDC mentre si utilizza CopyToTempFolder Binary Reader e si dispone di un'istanza ASM connessa all'origine. Puoi ignorare l'attivazione di questa valutazione se non intendi utilizzare la CopyToTempFolder funzionalità.

Ti consigliamo di non utilizzare la CopyToTempFolder funzionalità perché è obsoleta.

Verifica se l'utente DMS dispone delle autorizzazioni per utilizzare Oracle Standby come sorgente

Chiave API: `oracle-prerequisites-privileges-of-standby-as-source`

Questa valutazione preliminare alla migrazione verifica se l'utente DMS dispone dei privilegi necessari per utilizzare un'istanza Oracle come origine. StandBy Puoi ignorare l'attivazione di questa valutazione se non intendi utilizzare un'istanza StandBy Oracle come origine.

Verifica se la sorgente DMS è connessa a un contenitore di applicazioni (PDB)

Chiave API: `oracle-check-app-pdb`

Questa valutazione di premigrazione verifica se la sorgente DMS è connessa a un contenitore di applicazioni PDB. DMS non supporta la replica da un contenitore di applicazioni PDB.

Verifica se la tabella contiene tipi di dati XML inclusi nell'ambito dell'attività.

Chiave API: `oracle-check-xml-columns`

Questa valutazione preliminare verifica se le tabelle utilizzate nell'ambito dell'attività hanno tipi di dati XML. Verifica inoltre se l'attività è configurata per la modalità LOB limitata quando la tabella contiene un tipo di dati XML. DMS supporta solo la modalità LOB limitata per la migrazione delle colonne Oracle XML.

Verifica se la modalità archivelog è abilitata nel database di origine.

Chiave API: `oracle-check-archivelog-mode`

Questa valutazione premigratoria verifica se la modalità archivelog è abilitata nel database di origine. L'attivazione della modalità di registro di archiviazione sul database di origine è necessaria per consentire a DMS di replicare le modifiche.

Convalida la conservazione dei log di archiviazione per RDS Oracle.

Chiave API: `oracle-check-archivelog-retention-rds`

Questa valutazione preliminare alla migrazione verifica se la conservazione dei log di archiviazione nel database RDS Oracle è configurata per almeno 24 ore.

Verifica se la tabella contiene tipi di dati estesi inclusi nell'ambito del task.

Chiave API: `oracle-check-extended-columns`

Questa valutazione preliminare verifica se le tabelle utilizzate nell'ambito dell'attività hanno tipi di dati estesi. Tieni presente che i tipi di dati estesi sono supportati solo dalla versione DMS 3.5 e successive.

Convalida la lunghezza del nome dell'oggetto incluso nell'ambito dell'attività.

Chiave API: `oracle-check-object-30-bytes-limit`

Questa valutazione di premigrazione verifica se la lunghezza del nome dell'oggetto supera i 30 byte. DMS non supporta nomi di oggetti lunghi (oltre 30 byte).

Verifica se la sorgente DMS è connessa a un PDB Oracle

Chiave API: `oracle-check-pdb-enabled`

Questa valutazione di premigrazione verifica se la sorgente DMS è connessa a un PDB. DMS supporta CDC solo quando si utilizza Binary Reader con Oracle PDB come sorgente. La valutazione valuta anche se l'attività è configurata per utilizzare il lettore binario quando DMS è connesso a Oracle PDB.

Verifica se la tabella contiene colonne spaziali incluse nell'ambito dell'attività.

Chiave API: `oracle-check-spatial-columns`

Questa valutazione preliminare verifica se la tabella contiene colonne spaziali incluse nell'ambito dell'attività. DMS supporta i tipi di dati spaziali solo utilizzando la modalità Full LOB. La valutazione valuta anche se l'attività è configurata per utilizzare la modalità Full LOB quando DMS identifica le colonne spaziali.

Verifica se la sorgente DMS è connessa a uno standby Oracle.

Chiave API: `oracle-check-standby-db`

Questa valutazione di premigrazione verifica se la sorgente è connessa a uno standby Oracle. DMS supporta CDC solo quando si utilizza il lettore binario con Oracle Standby come sorgente. La valutazione valuta anche se il task è configurato per utilizzare il lettore binario quando DMS è collegato a Oracle Standby.

Verifica se il tablespace del database di origine è crittografato utilizzando TDE.

Chiave API: `oracle-check-tde-enabled`

Questa valutazione premigratoria verifica se l'origine ha TDE Encryption abilitato sul tablespace. DMS supporta TDE solo con tablespace crittografati quando si utilizza Oracle per RDS Oracle. LogMiner

Verifica se il database di origine è Oracle ASM

Chiave API: `oracle-check-asm`

Questa valutazione di premigrazione verifica se l'origine utilizza ASM. Per migliorare le prestazioni con la configurazione ASM, prendi in considerazione l'aggiunta di `parallelASReadThreads` e `readAheadBlocks` alle impostazioni dell'endpoint di origine.

Valutazioni di Sql Server

Questa sezione descrive le valutazioni individuali di pre-migrazione per le attività di migrazione che utilizzano un endpoint di origine Microsoft SQL Server.

Argomenti

- [Verifica della semplicità del modello di ripristino per il database](#)
- [Controllo delle colonne calcolate nelle tabelle nell'ambito dell'attività](#)
- [Controlla degli indici di archiviazione delle colonne nelle tabelle nell'ambito dell'attività](#)
- [Verifica dell'appartenenza delle tabelle ottimizzate per la memoria all'ambito dell'attività](#)
- [Verifica dell'appartenenza delle tabelle temporali all'ambito dell'attività](#)
- [Verifica dell'abilitazione della durabilità ritardata a livello di database](#)
- [Verifica dell'abilitazione del ripristino accelerato dei dati a livello di database](#)
- [Verifica della presenza di più di 10.000 tabelle con chiavi primarie nella mappatura delle tabelle](#)
- [Controlla se il database di origine contiene tabelle o nomi di schemi con caratteri speciali.](#)
- [Controlla se il database di origine ha nomi di colonne con dati mascherati](#)
- [Controlla se il database di origine ha backup crittografati](#)
- [Verifica se il database di origine contiene backup archiviati in un URL o in Windows Azure.](#)
- [Controlla se il database di origine dispone di backup su più dischi](#)
- [Controlla se il database di origine ha almeno un backup completo](#)
- [Controlla se il database di origine presenta colonne sparse e una compressione della struttura colonnare.](#)
- [Verifica se l'istanza del database di origine dispone del controllo a livello di server per SQL Server 2008 o SQL Server 2008 R2](#)
- [Controlla se il database di origine ha colonne geometriche per la modalità LOB completa](#)
- [Controlla se il database di origine contiene colonne con la proprietà Identity.](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni FULL LOAD](#)
- [Verifica se l'utente DMS dispone delle autorizzazioni FULL LOAD e CDC o CDC solo](#)
- [Verifica se l'ignoreMsReplicationEnablementECA è impostata quando usi MS-CDC con database locali o EC2](#)
- [Controlla se l'utente DMS dispone dell'autorizzazione VIEW DEFINITION.](#)

- [Verifica se l'utente DMS dispone dell'autorizzazione VIEW DATABASE STATE sul database MASTER per gli utenti senza il ruolo Sysadmin.](#)
- [Controlla se l'utente DMS dispone dell'autorizzazione VIEW SERVER STATE.](#)

Verifica della semplicità del modello di ripristino per il database

Chiave API: `sqlserver-check-for-recovery-model`

Questa valutazione premigratoria convalida il modello di ripristino degli endpoint di origine. AWS DMS richiede che il modello di ripristino sia impostato su `Bulk Logged` o `Full` per la replica continua.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Prerequisiti per l'utilizzo della replica continua \(CDC\) da un'origine SQL Server.](#)

Controllo delle colonne calcolate nelle tabelle nell'ambito dell'attività

Chiave API: `sqlserver-check-for-computed-fields`

Questa valutazione preliminare alla migrazione verifica la presenza di colonne calcolate. AWS DMS non supporta la replica delle modifiche dalle colonne calcolate di SQL Server.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS.](#)

Controlla degli indici di archiviazione delle colonne nelle tabelle nell'ambito dell'attività

Chiave API: `sqlserver-check-for-columnstore-indexes`

Questa valutazione preliminare alla migrazione verifica la presenza di tabelle con indici columnstore. AWS DMS non supporta la replica delle modifiche dalle tabelle di SQL Server con indici columnstore.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS.](#)

Verifica dell'appartenenza delle tabelle ottimizzate per la memoria all'ambito dell'attività

Chiave API: `sqlserver-check-for-memory-optimized-tables`

Questa valutazione di premigrazione verifica la presenza di tabelle ottimizzate per la memoria. AWS DMS non supporta la replica delle modifiche da tabelle ottimizzate per la memoria.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica dell'appartenenza delle tabelle temporali all'ambito dell'attività

Chiave API: `sqlserver-check-for-temporal-tables`

Questa valutazione preliminare alla migrazione verifica la presenza di tabelle temporali. AWS DMS non supporta la replica delle modifiche dalle tabelle temporali.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica dell'abilitazione della durabilità ritardata a livello di database

Chiave API: `sqlserver-check-for-delayed-durability`

Questa valutazione preliminare alla migrazione verifica la presenza di un ritardo nella durabilità. AWS DMS non supporta la replica delle modifiche apportate a transazioni che utilizzano una durabilità ritardata.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica dell'abilitazione del ripristino accelerato dei dati a livello di database

Chiave API: `sqlserver-check-for-accelerated-data-recovery`

Questa valutazione pre-migrazione verifica la presenza di un ripristino accelerato dei dati. AWS DMS non supporta la replica delle modifiche dai database con ripristino accelerato dei dati.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica della presenza di più di 10.000 tabelle con chiavi primarie nella mappatura delle tabelle

Chiave API: `sqlserver-large-number-of-tables`

Questa valutazione di pre-migrazione verifica la presenza di più di 10.000 tabelle con chiavi primarie. I database configurati con MS-Replication possono subire errori nelle attività se ci sono troppe tabelle con chiavi primarie.

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni sulla configurazione di MS-Replication, consulta [Acquisizione delle modifiche ai dati per SQL Server autogestito on-premise o su Amazon EC2](#).

Controlla se il database di origine contiene tabelle o nomi di schemi con caratteri speciali.

Chiave API: `sqlserver-check-for-special-characters`

Questa valutazione di premigrazione verifica se il database di origine ha nomi di tabelle o schemi che includono un carattere del seguente set:

```
\\ -- \n \" \b \r ' \t ;
```

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine ha nomi di colonne con dati mascherati

Chiave API: `sqlserver-check-for-masked-data`

Questa valutazione premigratoria verifica se il database di origine contiene dati mascherati. AWS DMS migra i dati mascherati senza mascherarli.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine ha backup crittografati

Chiave API: `sqlserver-check-for-encrypted-backups`

Questa valutazione preliminare verifica se il database di origine dispone di backup crittografati.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se il database di origine contiene backup archiviati in un URL o in Windows Azure.

Chiave API: `sqlserver-check-for-backup-url`

Questa valutazione premigratoria verifica se il database di origine dispone di backup archiviati in un URL o in Windows Azure.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine dispone di backup su più dischi

Chiave API: `sqlserver-check-for-backup-multiple-stripes`

Questa valutazione premigratoria verifica se il database di origine dispone di backup su più dischi.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine ha almeno un backup completo

Chiave API: `sqlserver-check-for-full-backup`

Questa valutazione preliminare verifica se il database di origine dispone di almeno un backup completo. SQL Server deve essere configurato per il backup completo ed è necessario eseguire un backup prima di replicare i dati.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine presenta colonne sparse e una compressione della struttura colonnare.

Chiave API: `sqlserver-check-for-sparse-columns`

Questa valutazione di premigrazione verifica se il database di origine presenta colonne sparse e una compressione della struttura colonnare. DMS non supporta la compressione di colonne sparse e strutture colnari.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se l'istanza del database di origine dispone del controllo a livello di server per SQL Server 2008 o SQL Server 2008 R2

Chiave API: `sqlserver-check-for-audit-2008`

Questa valutazione premigratoria verifica se il database di origine ha abilitato il controllo a livello di server per SQL Server 2008 o SQL Server 2008 R2. DMS presenta un problema noto correlato con SQL Server 2008 e 2008 R2.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine ha colonne geometriche per la modalità LOB completa

Chiave API: `sqlserver-check-for-geometry-columns`

Questa valutazione di premigrazione verifica se il database di origine dispone di colonne geometriche per la modalità LOB (Large Object) completa quando si utilizza SQL Server come origine. Si consiglia di utilizzare la modalità LOB limitata o di impostare l'impostazione dell'InlineLobMaxSizeattività in modo da utilizzare la modalità LOB in linea quando il database include colonne geometriche.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se il database di origine contiene colonne con la proprietà Identity.

Chiave API: `sqlserver-check-for-identity-columns`

Questa valutazione di premigrazione verifica se il database di origine ha una colonna con la IDENTITY proprietà. DMS non migra questa proprietà nella colonna del database di destinazione corrispondente.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se l'utente DMS dispone delle autorizzazioni FULL LOAD

Chiave API: `sqlserver-check-user-permission-for-full-load-only`

Questa valutazione premigratoria verifica se l'utente dell'attività DMS dispone delle autorizzazioni per eseguire l'attività in modalità FULL LOAD.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se l'utente DMS dispone delle autorizzazioni FULL LOAD e CDC o CDC solo

Chiave API: `sqlserver-check-user-permission-for-cdc`

Questa valutazione premigratoria verifica se l'utente DMS dispone delle autorizzazioni per eseguire l'attività in o in modalità. FULL LOAD and CDC CDC only

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se l'**ignoreMsReplicationEnablementECA** è impostata quando usi MS-CDC con database locali o EC2

Chiave API: `sqlserver-check-attribute-for-enable-ms-cdc-onprem`

Verifica se l'attributo di connessione `ignoreMsReplicationEnablement` aggiuntivo (ECA) è impostato quando usi MS-CDC con database locali o EC2.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se l'utente DMS dispone dell'autorizzazione `VIEW DEFINITION`.

Chiave API: `sqlserver-check-user-permission-on-view-definition`

Questa valutazione premigratoria verifica se l'utente specificato nelle impostazioni dell'endpoint dispone dell'autorizzazione. `VIEW DEFINITION` DMS richiede l'`VIEW DEFINITION` autorizzazione per visualizzare le definizioni degli oggetti.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Verifica se l'utente DMS dispone dell'autorizzazione `VIEW DATABASE STATE` sul database `MASTER` per gli utenti senza il ruolo `Sysadmin`.

Chiave API: `sqlserver-check-user-permission-on-view-database-state`

Questa valutazione premigratoria verifica se l'utente specificato nelle impostazioni dell'endpoint dispone dell'autorizzazione. `VIEW DATABASE STATE` DMS richiede questa autorizzazione per accedere agli oggetti del database nel database `MASTER`. DMS richiede questa autorizzazione anche quando l'utente non dispone dei privilegi di amministratore di sistema. DMS richiede questa autorizzazione per creare funzioni, certificati e accessi e per concedere credenziali.

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Controlla se l'utente DMS dispone dell'autorizzazione `VIEW SERVER STATE`.

Chiave API: `sqlserver-check-user-permission-on-view-server-state`

Questa valutazione preliminare verifica se l'utente specificato negli attributi di connessione aggiuntivi (ECA) dispone dell'`VIEW SERVER STATE` autorizzazione. `VIEW SERVER STATE` è un'autorizzazione a livello di server che consente a un utente di visualizzare informazioni e stati a livello di server. Questa autorizzazione fornisce l'accesso alle viste di gestione dinamica (DMV) e alle funzioni di gestione dinamica (DMF) che espongono informazioni sull'istanza di SQL Server. Questa autorizzazione è necessaria per consentire all'utente DMS di accedere alle risorse CDC. Questa

autorizzazione è necessaria per eseguire un'attività DMS in FULL LOAD and CDC modalità o. CDC only

Per ulteriori informazioni, consulta [Limitazioni all'utilizzo di SQL Server come origine per AWS DMS](#).

Valutazioni MySQL

Questa sezione descrive le valutazioni individuali prima della migrazione per le attività di migrazione che utilizzano un endpoint di origine MySQL.

Argomenti

- [Verifica se una tabella utilizza un motore di archiviazione diverso da InnoDB](#)
- [Verifica se l'incremento automatico è abilitato su tutte le tabelle utilizzate per la migrazione](#)
- [Verifica se l'immagine binlog del database è impostata per supportare FULL DMS CDC](#)
- [Verifica se il database di origine è un MySQL Read-Replica](#)
- [Verifica se una tabella ha partizioni e consiglia le impostazioni delle attività a caricamento completo target_table_prep_mode](#)
- [Verifica se DMS supporta la versione del database](#)
- [Verifica se il database di destinazione è configurato su 1 local_infile](#)
- [Verifica se il database di destinazione contiene tabelle con chiavi esterne](#)
- [Verifica se le tabelle di origine nell'ambito dell'attività hanno vincoli a cascata](#)
- [Verifica se i valori di timeout sono appropriati per un'origine o una destinazione MySQL](#)

Verifica se una tabella utilizza un motore di archiviazione diverso da InnoDB

Chiave API: `mysql-check-table-storage-engine`

Questa valutazione di premigrazione verifica se il motore di archiviazione utilizzato per qualsiasi tabella nel database Source MySQL è un motore diverso da InnoDB. DMS crea tabelle di destinazione con il motore di archiviazione InnoDB per impostazione predefinita. Se è necessario utilizzare un motore di archiviazione diverso da InnoDB, è necessario creare manualmente la tabella sul database di destinazione e configurare l'attività DMS da utilizzare TRUNCATE_BEFORE_LOAD o DO_NOTHING come impostazione dell'attività a caricamento completo. Per ulteriori informazioni sulle impostazioni delle attività a caricamento completo, vedere. [Impostazioni delle attività di caricamento completo](#)

Per ulteriori informazioni sulle limitazioni degli endpoint MySQL, vedere. [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#)

Verifica se l'incremento automatico è abilitato su tutte le tabelle utilizzate per la migrazione

Chiave API: `mysql-check-auto-increment`

Questa valutazione preliminare verifica se le tabelle di origine utilizzate nell'attività hanno l'incremento automatico abilitato. DMS non esegue la migrazione dell'attributo `AUTO_INCREMENT` su una colonna verso un database di destinazione.

Per ulteriori informazioni sulle limitazioni degli endpoint MySQL, vedere. [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#) Per informazioni sulla gestione delle colonne di identità in MySQL, [vedere Gestire le colonne IDENTITY AWS DMS in: Parte 2](#).

Verifica se l'immagine binlog del database è impostata per supportare **FULL** DMS CDC

Chiave API: `mysql-check-binlog-image`

Questa valutazione premigratoria verifica se l'immagine binlog del database di origine è impostata su. `FULL` In MySQL, `binlog_row_image` la variabile determina come viene scritto un evento di log binario quando si utilizza il formato. `ROW` Per garantire la compatibilità con DMS e supportare CDC, imposta la variabile su. `binlog_row_image FULL` Questa impostazione garantisce che DMS riceva informazioni sufficienti per creare l'intero Data Manipulation Language (DML) per il database di destinazione durante la migrazione.

Per impostare l'immagine binlog su, procedi come `FULL` segue:

- Per Amazon RDS, questo valore è `FULL` predefinito.
- Per i database ospitati in locale o su Amazon EC2, imposta `binlog_row_image` il valore in `my.ini` (Microsoft Windows) `my.cnf` o (UNIX).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Verifica se il database di origine è un MySQL Read-Replica

Chiave API: `mysql-check-database-role`

Questa valutazione di premigrazione verifica se il database di origine è una replica di lettura. Per abilitare il supporto CDC per DMS quando si è connessi a una replica di lettura, imposta il parametro su. `log_slave_updates True` Per ulteriori informazioni sull'utilizzo di un database MySQL autogestito, vedere. [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#)

Per impostare il `log_slave_updates` valore su `True`, procedi come segue:

- Per Amazon RDS, usa il gruppo di parametri del database. Per informazioni sull'utilizzo dei gruppi di parametri del database RDS, consulta [Working with parameters groups](#) nella Amazon RDS User Guide.
- Per i database ospitati in locale o su Amazon EC2, imposta `log_slave_updates` il valore in `my.ini` (Microsoft Windows) `my.cnf` o (UNIX).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Verifica se una tabella ha partizioni e consiglia le impostazioni delle attività a caricamento completo **target_table_prep_mode**

Chiave API: `mysql-check-table-partition`

Questa valutazione premigratoria verifica la presenza di tabelle con partizioni nel database di origine. DMS crea tabelle senza partizioni sulla destinazione MySQL. Per migrare le tabelle partizionate verso una tabella partizionata sulla destinazione, è necessario effettuare le seguenti operazioni:

- Pre-crea le tabelle partizionate nel database MySQL di destinazione.
- Configura l'attività DMS per utilizzarla `TRUNCATE_BEFORE_LOAD` o come impostazione dell'attività a caricamento completo `DO_NOTHING`.

Per ulteriori informazioni sulle limitazioni degli endpoint MySQL, vedere. [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#)

Verifica se DMS supporta la versione del database

Chiave API: `mysql-check-supported-version`

Questa valutazione di premigrazione verifica se la versione del database di origine è compatibile con DMS. CDC non è supportato con le versioni 5.5 o precedenti di Amazon RDS MySQL o versioni di MySQL successive alla 8.0.x. CDC è supportato solo per le versioni MySQL 5.6, 5.7 o 8.0.

Per ulteriori informazioni sulle versioni di MySQL supportate, vedere. [Endpoint di origine per la migrazione dei dati](#)

Verifica se il database di destinazione è configurato su 1 **local_infile**

Chiave API: `mysql-check-target-localinfile-set`

Questa valutazione preliminare alla migrazione verifica se il `local_infile` parametro nel database di destinazione è impostato su 1. DMS richiede che il parametro 'local_infile' sia impostato su 1 durante il caricamento completo nel database di destinazione. Per ulteriori informazioni, consulta [Migrazione da MySQL a MySQL mediante AWS DMS](#).

Questa valutazione è valida solo per un'attività a pieno carico o a pieno carico e CDC.

Verifica se il database di destinazione contiene tabelle con chiavi esterne

Chiave API: `mysql-check-fk-target`

Questa valutazione preliminare verifica se un'attività a pieno carico o a pieno carico e CDC che migra a un database MySQL contiene tabelle con chiavi esterne. L'impostazione predefinita in DMS prevede il caricamento delle tabelle in ordine alfabetico. Le tabelle con chiavi esterne e vincoli di integrità referenziale possono causare un errore di caricamento, poiché le tabelle principale e secondaria potrebbero non essere caricate contemporaneamente.

Per ulteriori informazioni sull'integrità referenziale in DMS, vedere Utilizzo degli indici, dei trigger e dei vincoli di integrità referenziale nell'argomento. [Miglioramento delle prestazioni di una migrazione AWS DMS](#)

Verifica se le tabelle di origine nell'ambito dell'attività hanno vincoli a cascata

Chiave API: `mysql-check-cascade-constraints`

Questa valutazione di premigrazione verifica se una qualsiasi delle tabelle di origine MySQL presenta vincoli a cascata. I vincoli Cascade non vengono migrati o replicati dalle attività DMS, perché MySQL non registra le modifiche per questi eventi nel binlog. Sebbene AWS DMS non supporti questi vincoli, è possibile utilizzare soluzioni alternative per gli obiettivi dei database relazionali.

Per informazioni sul supporto dei vincoli di cascate e di altri vincoli, consultate l'argomento Risoluzione dei problemi di migrazione. [Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati](#) AWS DMS

Verifica se i valori di timeout sono appropriati per un'origine o una destinazione MySQL

Chiave API: `mysql-check-network-parameter`

Questa valutazione premigratoria verifica se l'endpoint MySQL di un'attività ha `net_read_timeout` le impostazioni impostate su `net_wait_timeout` almeno `wait_timeout` 300 secondi. Ciò è necessario per evitare disconnessioni durante la migrazione.

Per ulteriori informazioni, consulta [Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività](#).

Valutazioni Mariadb

Questa sezione descrive le valutazioni individuali di pre-migrazione per le attività di migrazione che utilizzano un endpoint di origine MariaDB.

Per creare una valutazione pre-migrazione individuale utilizzando l' AWS DMS API, utilizza la chiave API elencata per il parametro dell'azione. Include [StartReplicationTaskAssessmentRun](#)

Argomenti

- [Convalida se una tabella utilizza un motore di archiviazione diverso da InnoDB](#)
- [Verifica se l'incremento automatico è abilitato su tutte le tabelle utilizzate per la migrazione](#)
- [Verifica se il formato binlog del database è impostato per supportare ROW DMS CDC](#)
- [Verifica se l'immagine binlog del database è impostata per supportare DMS CDC FULL](#)
- [Convalida se il database di origine è un MariaDB Read-Replica](#)
- [Verifica se una tabella ha partizioni e consiglia o utilizza le impostazioni delle attività a caricamento completo TRUNCATE_BEFORE_LOADDO_NOTHING](#)
- [Verifica se DMS supporta la versione del database](#)
- [Verifica se il database di destinazione è configurato su 1 local_infile](#)
- [Verifica se il database di destinazione ha tabelle con chiavi esterne](#)
- [Verifica se le tabelle di origine nell'ambito dell'attività hanno vincoli a cascata](#)
- [Verifica se le tabelle di origine nell'ambito dell'attività hanno generato colonne](#)
- [Verifica se i valori di timeout sono appropriati per una fonte MariaDB](#)
- [Verifica se i valori di timeout sono appropriati per un target MariaDB](#)

Convalida se una tabella utilizza un motore di archiviazione diverso da InnoDB

Chiave API: `mariadb-check-table-storage-engine`

Questa valutazione di premigrazione verifica se il motore di archiviazione utilizzato per qualsiasi tabella nel database Source MariaDB è un motore diverso da InnoDB. DMS crea tabelle di destinazione con il motore di archiviazione InnoDB per impostazione predefinita. Se è necessario utilizzare un motore di archiviazione diverso da InnoDB, è necessario creare manualmente la tabella

sul database di destinazione e configurare l'attività DMS da utilizzare TRUNCATE_BEFORE_LOAD o DO_NOTHING come impostazione dell'attività a caricamento completo. Per ulteriori informazioni sulle impostazioni delle attività a caricamento completo, vedere. [Impostazioni delle attività di caricamento completo](#)

Per ulteriori informazioni sulle limitazioni degli endpoint Mariadb, consulta. [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#)

Verifica se l'incremento automatico è abilitato su tutte le tabelle utilizzate per la migrazione

Chiave API: mariadb-check-auto-increment

Questa valutazione preliminare verifica se le tabelle di origine utilizzate nell'attività hanno l'incremento automatico abilitato. DMS non esegue la migrazione dell'attributo AUTO_INCREMENT su una colonna verso un database di destinazione.

Per ulteriori informazioni sulle limitazioni degli endpoint Mariadb, consulta. [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#) Per informazioni sulla gestione delle colonne di identità in Mariadb, [vedi Gestire le colonne IDENTITY AWS DMS in: Part 2](#).

Verifica se il formato binlog del database è impostato per supportare **ROW** DMS CDC

Chiave API: mariadb-check-binlog-format

Questa valutazione premigratoria verifica se il formato binlog del database di origine è impostato per supportare DMS Change Data Capture (ROWCDC).

Per impostare il formato binlog su, effettuate le seguenti operazioni: ROW

- Per Amazon RDS, usa il gruppo di parametri del database. Per informazioni sull'utilizzo di un gruppo di parametri RDS, consulta [Configurazione della registrazione binaria MySQL nella Amazon RDS User Guide](#).
- Per i database ospitati in locale o su Amazon EC2, imposta binlog_format il valore in my.ini (Microsoft Windows) my.cnf o (UNIX).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni sui server Mariadb ospitati autonomamente, consulta. [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#)

Verifica se l'immagine binlog del database è impostata per supportare DMS CDC **FULL**

Chiave API: `mariadb-check-binlog-image`

Questa valutazione premigratoria verifica se l'immagine binlog del database di origine è impostata su. FULL In Mariadb, `binlog_row_image` la variabile determina come viene scritto un evento di log binario quando si utilizza il formato. ROW Per garantire la compatibilità con DMS e supportare CDC, imposta la variabile su. `binlog_row_image FULL` Questa impostazione garantisce che DMS riceva informazioni sufficienti per creare l'intero Data Manipulation Language (DML) per il database di destinazione durante la migrazione.

Per impostare l'immagine binlog su, procedi come FULL segue:

- Per Amazon RDS, questo valore è FULL predefinito.
- Per i database ospitati in locale o su Amazon EC2, imposta `binlog_row_image` il valore in `my.ini` (Microsoft Windows) `my.cnf` o (UNIX).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Per ulteriori informazioni sui server Mariadb ospitati autonomamente, consulta. [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#)

Convalida se il database di origine è un MariaDB Read-Replica

Chiave API: `mariadb-check-database-role`

Questa valutazione di premigrazione verifica se il database di origine è una replica di lettura. Per abilitare il supporto CDC per DMS quando si è connessi a una replica di lettura, imposta il parametro su. `log_slave_updates True` Per ulteriori informazioni sull'utilizzo di un database MySQL autogestito, vedere. [Utilizzo di un database autogestito compatibile con MySQL come fonte per AWS DMS](#)

Per impostare il `log_slave_updates` valore su True, procedi come segue:

- Per Amazon RDS, usa il gruppo di parametri del database. Per informazioni sull'utilizzo dei gruppi di parametri del database RDS, consulta [Working with parameters groups](#) nella Amazon RDS User Guide.
- Per i database ospitati in locale o su Amazon EC2, imposta `log_slave_updates` il valore in `my.ini` (Microsoft Windows) `my.cnf` o (UNIX).

Questa valutazione è valida per una migrazione di pieno carico e CDC oppure una migrazione sola CDC. Questa valutazione non è valida per una migrazione solo pieno carico.

Verifica se una tabella ha partizioni e consiglia o utilizza le impostazioni delle attività a caricamento completo **TRUNCATE_BEFORE_LOADDO_NOTHING**

Chiave API: `mariadb-check-table-partition`

Questa valutazione premigratoria verifica la presenza di tabelle con partizioni nel database di origine. DMS crea tabelle senza partizioni sul target Mariadb. Per migrare le tabelle partizionate in una tabella partizionata sulla destinazione, devi fare quanto segue:

- Pre-crea le tabelle partizionate nel database MariaDB di destinazione.
- Configura l'attività DMS per utilizzarla TRUNCATE_BEFORE_LOAD o come impostazione dell'attività a caricamento completo DO_NOTHING.

Per ulteriori informazioni sulle limitazioni degli endpoint Mariadb, consulta [Limitazioni all'utilizzo di un database MySQL come fonte per AWS DMS](#)

Verifica se DMS supporta la versione del database

Chiave API: `mariadb-check-supported-version`

Questa valutazione di premigrazione verifica se la versione del database di origine è compatibile con DMS. CDC non è supportato con le versioni 10.4 o precedenti di Amazon RDS MariaDB o con le versioni di MySQL successive alla 10.11. Per ulteriori informazioni sulle versioni di Mariadb supportate, consulta [Endpoint di origine per la migrazione dei dati](#)

Verifica se il database di destinazione è configurato su 1 **local_infile**

Chiave API: `mariadb-check-target-localinfile-set`

Questa valutazione preliminare alla migrazione verifica se il `local_infile` parametro nel database di destinazione è impostato su 1. DMS richiede che il parametro 'local_infile' sia impostato su 1 durante il caricamento completo nel database di destinazione. Per ulteriori informazioni, consulta [Migrazione da MySQL a MySQL mediante AWS DMS.](#)

Questa valutazione è valida solo per un'attività a pieno carico.

Verifica se il database di destinazione ha tabelle con chiavi esterne

Chiave API: `mariadb-check-fk-target`

Questa valutazione premigratoria verifica se un'attività a pieno carico o a pieno carico e CDC che migra a un database Mariadb ha tabelle con chiavi esterne. L'impostazione predefinita in DMS prevede il caricamento delle tabelle in ordine alfabetico. Le tabelle con chiavi esterne e vincoli di integrità referenziale possono causare un errore di caricamento, poiché le tabelle principale e secondaria potrebbero non essere caricate contemporaneamente.

Per ulteriori informazioni sull'integrità referenziale in DMS, vedere Utilizzo degli indici, dei trigger e dei vincoli di integrità referenziale nell'argomento. [Miglioramento delle prestazioni di una migrazione AWS DMS](#)

Verifica se le tabelle di origine nell'ambito dell'attività hanno vincoli a cascata

Chiave API: mariadb-check-cascade-constraints

Questa valutazione premigratoria verifica se una qualsiasi delle tabelle di origine di Mariadb ha vincoli a cascata. I vincoli Cascade non vengono migrati o replicati dalle attività DMS, perché Mariadb non registra le modifiche per questi eventi nel binlog. Sebbene AWS DMS non supporti questi vincoli, puoi utilizzare soluzioni alternative per gli obiettivi dei database relazionali.

Per informazioni sul supporto dei vincoli di cascate e di altri vincoli, consultate l'argomento Risoluzione dei problemi di migrazione. [Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati](#) AWS DMS

Verifica se le tabelle di origine nell'ambito dell'attività hanno generato colonne

Chiave API: mariadb-check-generated-columns

Questa valutazione premigratoria verifica se una delle tabelle di origine di Mariadb ha generato colonne. Le attività DMS non migrano o replicano le colonne generate.

Per informazioni su come migrare le colonne generate, consulta. [???](#)

Verifica se i valori di timeout sono appropriati per una fonte MariaDB

Chiave API: mariadb-check-source-network-parameter

Questa valutazione premigratoria verifica se l'endpoint di origine Mariadb di un'attività ha net_read_timeout le net_wait_timeout impostazioni impostate su wait_timeout almeno 300 secondi. Ciò è necessario per evitare disconnessioni durante la migrazione.

Per ulteriori informazioni, consulta [Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività.](#)

Verifica se i valori di timeout sono appropriati per un target MariaDB

Chiave API: `mariadb-check-target-network-parameter`

Questa valutazione premigratoria verifica se l'endpoint di destinazione MariaDB di un'attività ha `net_read_timeout` e `net_wait_timeout` impostazioni impostate su `wait_timeout` almeno 300 secondi. Ciò è necessario per evitare disconnessioni durante la migrazione.

Per ulteriori informazioni, consulta [Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività](#).

Valutazioni PostgreSQL

Questa sezione descrive le valutazioni individuali di pre-migrazione per le attività di migrazione che utilizzano un endpoint di origine PostgreSQL.

Argomenti

- [Verifica se la versione del database di origine è supportata da DMS per la migrazione](#)
- [Convalida il `logical_decoding_work_mem` parametro nel database di origine](#)
- [Verifica se il database di origine contiene transazioni di lunga durata](#)
- [Convalida il parametro del database di origine `max_slot_wal_keep_size`](#)
- [Controlla se il parametro del database di origine `postgres-check-maxwalsenders` è impostato per supportare CDC.](#)
- [Controlla se il database di origine è configurato per PGLOGICAL](#)
- [Verifica se la chiave primaria della tabella di origine è del tipo di dati LOB](#)
- [Verifica se la tabella di origine ha una chiave primaria](#)
- [Verifica se le transazioni preparate sono presenti nel database di origine](#)
- [Convalida se `wal_sender_timeout` è impostato su un valore minimo richiesto per supportare DMS CDC](#)
- [Convalida se è impostato su logico nel database `wal_level` di origine](#)

Verifica se la versione del database di origine è supportata da DMS per la migrazione

Chiave API: `postgres-check-dbversion`

Questa valutazione premigratoria verifica se la versione del database di origine è compatibile con. AWS DMS

Convalida il **logical_decoding_work_mem** parametro nel database di origine

Chiave API: `postgres-check-for-logical-decoding-work-mem`

Questa valutazione preliminare alla migrazione consiglia di ottimizzare il `logical_decoding_work_mem` parametro sul database di origine. In un database altamente transazionale in cui potrebbero essere presenti transazioni di lunga durata o molte sottotransazioni, ciò può comportare un aumento del consumo di memoria di decodifica logica e la necessità di trasferimento su disco. Ciò si traduce in un'elevata latenza della sorgente DMS durante la replica. In tali scenari, potrebbe essere necessario eseguire l'ottimizzazione. `logical_decoding_work_mem` Questo parametro è supportato nelle versioni 13 e successive di PostgreSQL.

Verifica se il database di origine contiene transazioni di lunga durata

Chiave API: `postgres-check-longrunningtxn`

Questa valutazione preliminare verifica se il database di origine contiene transazioni di lunga durata che sono durate più di 10 minuti. L'avvio dell'attività potrebbe non riuscire, perché per impostazione predefinita, DMS verifica la presenza di eventuali transazioni aperte durante l'avvio dell'attività.

Convalida il parametro del database di origine **max_slot_wal_keep_size**

Chiave API: `postgres-check-maxslot-wal-keep-size`

Questa valutazione di premigrazione verifica il valore configurato per `max_slot_wal_keep_size`. Quando `max_slot_wal_keep_size` è impostato su un valore non predefinito, l'attività DMS potrebbe non riuscire a causa della rimozione dei file WAL richiesti.

Controlla se il parametro del database di origine **postgres-check-maxwalsenders** è impostato per supportare CDC.

Chiave API: `postgres-check-maxwalsenders`

Questa valutazione premigratoria verifica il valore configurato per il database di `max_wal_senders` origine. DMS deve essere `max_wal_senders` impostato su un valore maggiore di 1 per supportare Change Data Capture (CDC).

Controlla se il database di origine è configurato per **PGLLOGICAL**

Chiave API: `postgres-check-pglogical`

Questa valutazione premigratoria verifica se il `shared_preload_libraries` valore è impostato sul supporto `pglogical PGLLOGICAL` per CDC. Tieni presente che puoi ignorare questa valutazione se intendi utilizzare la decodifica di test per la replica logica.

Verifica se la chiave primaria della tabella di origine è del tipo di dati LOB

Chiave API: `postgres-check-pk-lob`

Questa valutazione di premigrazione verifica se la chiave primaria di una tabella è del tipo di dati Large Object (LOB). DMS non supporta la replica se la tabella di origine ha una colonna LOB come chiave primaria.

Verifica se la tabella di origine ha una chiave primaria

Chiave API: `postgres-check-pk`

Questa valutazione preliminare verifica se esistono chiavi primarie per le tabelle utilizzate nell'ambito dell'attività. DMS non supporta la replica di tabelle senza chiavi primarie, a meno che l'identità della replica non sia impostata sulla tabella di `full` origine.

Verifica se le transazioni preparate sono presenti nel database di origine

Chiave API: `postgres-check-preparedtxn`

Questa valutazione preliminare verifica se nel database di origine sono presenti transazioni preparate. La creazione dello slot di replica potrebbe smettere di rispondere se sono presenti transazioni preparate nel database di origine.

Convalida se **`wal_sender_timeout`** è impostato su un valore minimo richiesto per supportare DMS CDC

Chiave API: `postgres-check-walsenderstimeout`

Questa valutazione di premigrazione verifica se `wal_sender_timeout` è impostata su un minimo di 10000 millisecondi (10 secondi). Un'attività DMS con CDC richiede un minimo di 10000 millisecondi (10 secondi) e fallisce se il valore è inferiore a 10000.

Convalida se è impostato su logico nel database **`wal_level`** di origine

Chiave API: `postgres-check-wallevel`

Questa valutazione di premigrazione verifica se `wal_level` è impostato su logico. Affinché DMS CDC funzioni, questo parametro deve essere abilitato nel database di origine.

Avvio e visualizzazione delle valutazioni dei tipi di dati (Legacy)

Note

Questa sezione descrive i contenuti legacy. Si consiglia di utilizzare le esecuzioni di valutazione premigratoria, descritte in precedenza in [Specifica, avvio e visualizzazione delle esecuzioni della valutazione di pre-migrazione](#).

Le valutazioni dei tipi di dati non sono disponibili nella console. Puoi eseguire valutazioni dei tipi di dati solo utilizzando l'API o la CLI e puoi visualizzare i risultati di una valutazione del tipo di dati solo nel bucket S3 dell'attività.

Una valutazione del tipo di dati identifica i tipi di dati in un database di origine che potrebbero non essere migrati correttamente perché la destinazione non li supporta. Durante questa valutazione, AWS DMS legge gli schemi del database di origine per un'attività di migrazione e crea un elenco dei tipi di dati delle colonne. Quindi confronta questo elenco con un elenco predefinito di tipi di dati supportati da AWS DMS. Se l'attività di migrazione ha tipi di dati non supportati, AWS DMS crea un rapporto che puoi consultare per vedere se l'attività di migrazione contiene tipi di dati non supportati. AWS DMS non crea un rapporto se l'attività di migrazione non contiene tipi di dati non supportati.

AWS DMS supporta la creazione di report di valutazione dei tipi di dati per i seguenti database relazionali:

- Oracle
- SQL Server
- PostgreSQL
- MySQL
- MariaDB
- Amazon Aurora

Puoi avviare e visualizzare un rapporto di valutazione del tipo di dati utilizzando la CLI e gli SDK per accedere all'API: AWS DMS

- La CLI utilizza il comando [start-replication-task-assessment](#) per avviare una valutazione del tipo di dati e il comando [describe-replication-task-assessment-results](#) per visualizzare l'ultimo report di valutazione del tipo di dati in formato JSON.

- L' AWS DMS API utilizza l'[StartReplicationTaskAssessment](#) operazione per avviare una valutazione del tipo di dati e utilizza l'[DescribeReplicationTaskAssessmentResults](#) operazione per visualizzare l'ultimo report di valutazione del tipo di dati in formato JSON.

Il report di valutazione del tipo di dati è un singolo file JSON che include un riepilogo in cui sono elencati i tipi di dati non supportati e il conteggio delle colonne per ogni tipo. Include un elenco di strutture di dati per ogni tipo di dati non supportato, inclusi schemi, tabelle e colonne con il tipo di dati non supportato. Puoi utilizzare il report per modificare i tipi di dati di origine e migliorare l'esito della migrazione.

Vi sono due livelli di tipi di dati non supportati. I tipi di dati che compaiono nel report come non supportati non possono essere migrati. I tipi di dati che compaiono nel report come parzialmente supportati potrebbero essere convertiti in un altro tipo di dati ma non essere migrati come previsto.

Nell'esempio seguente viene illustrato un esempio di report di valutazione del tipo di dati che è possibile visualizzare.

```
{
  "summary":{
    "task-name":"test15",
    "not-supported":{
      "data-type": [
        "sql-variant"
      ],
      "column-count":3
    },
    "partially-supported":{
      "data-type":[
        "float8",
        "jsonb"
      ],
      "column-count":2
    }
  },
  "types":[
    {
      "data-type":"float8",
      "support-level":"partially-supported",
      "schemas":[
        {
```

```
        "schema-name":"schema1",
        "tables":[
          {
            "table-name":"table1",
            "columns":[
              "column1",
              "column2"
            ]
          },
          {
            "table-name":"table2",
            "columns":[
              "column3",
              "column4"
            ]
          }
        ]
      },
      {
        "schema-name":"schema2",
        "tables":[
          {
            "table-name":"table3",
            "columns":[
              "column5",
              "column6"
            ]
          },
          {
            "table-name":"table4",
            "columns":[
              "column7",
              "column8"
            ]
          }
        ]
      }
    ]
  },
  {
    "datatype":"int8",
    "support-level":"partially-supported",
    "schemas":[
      {
```



```

    "schema-name":"schema1",
    "tables":[
      {
        "table-name":"table1",
        "columns":[
          "column9",
          "column10"
        ]
      },
      {
        "table-name":"table2",
        "columns":[
          "column11",
          "column12"
        ]
      }
    ]
  }
]
}

```

AWS DMS archivia le valutazioni più recenti e tutte le precedenti sui tipi di dati in un bucket Amazon S3 creato AWS DMS da nel tuo account. Il nome del bucket Amazon S3 ha il seguente formato, dove *customerId* è l'ID cliente e *customerDNS* è un identificativo interno.

dms-*customerId*-*customerDNS*

Note

Per impostazione predefinita, è possibile creare fino a 100 bucket Amazon S3 in ciascun account AWS . Poiché AWS DMS crea un bucket nel tuo account, assicurati che non superi il limite del bucket. In caso contrario, la valutazione del tipo di dati non riesce.

Tutti i report di valutazione del tipo di dati per una determinata attività di migrazione vengono archiviati in una cartella del bucket denominata con l'identificativo dell'attività. Il nome del file di ogni rapporto è la data di valutazione del tipo di dati nel formato yyyy-mm-dd-hh -mm. Puoi visualizzare e confrontare i report di valutazione dell'attività precedenti dalla console di gestione Amazon S3.

AWS DMS crea anche un ruolo AWS Identity and Access Management (IAM) per consentire l'accesso al bucket S3 creato per questi report. Il nome del ruolo è `dms-access-for-tasks`. Il ruolo utilizza la policy `AmazonDMSRedshiftS3Role`. Se si verifica un `ResourceNotFoundFault` durante l'esecuzione `StartReplicationTaskAssessment`, consulta [ResourceNotFoundFault](#) la sezione Risoluzione dei problemi per informazioni sulla creazione manuale del `dms-access-for-tasks` ruolo.

La valutazione dei problemi viene eseguita

Di seguito, sono disponibili argomenti sulla risoluzione dei problemi relativi all'esecuzione dei report di valutazione con AWS Database Migration Service. Questi argomenti possono aiutarti a risolvere i problemi più comuni.

Argomenti

- [ResourceNotFoundFault durante l'esecuzione StartReplicationTaskAssessment](#)

ResourceNotFoundFault durante l'esecuzione StartReplicationTaskAssessment

È possibile che si verifichi la seguente eccezione durante l'esecuzione dell'[StartReplicationTaskAssessment](#).

```
An error occurred (ResourceNotFoundFault) when calling the
StartReplicationTaskAssessment operation: Task assessment has not been run or dms-
access-for-tasks IAM Role not configured correctly
```

Se riscontri questa eccezione, crea il `dms-access-for-tasks` ruolo effettuando le seguenti operazioni:

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel pannello di navigazione, seleziona Roles (Ruoli).
3. Selezionare Create role (Crea ruolo).
4. Nella pagina Seleziona entità attendibile, per Tipo di entità affidabile, scegli Criteri di attendibilità personalizzati.
5. Incolla il seguente codice JSON nell'editor, sostituendo il testo esistente.

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

```
        "Sid": "1",
        "Effect": "Allow",
        "Principal": {
            "Service": "dms.amazonaws.com"
        },
        "Action": "sts:AssumeRole"
    }
]
}
```

La politica precedente concede l'`sts:AssumeRole` autorizzazione a AWS DMS. Quando aggiungi la policy `AmazonDMSRedShifts3Role`, DMS può creare il bucket S3 nel tuo account e inserire i risultati della valutazione del tipo di dati in questo bucket S3.

6. Seleziona **Successivo**.
7. Nella pagina **Aggiungi autorizzazioni**, cerca e aggiungi la politica `AmazonDMSRedShifts3Role`. Seleziona **Successivo**.
8. Nella pagina **Nome, revisione e creazione**, assegna un nome al ruolo. `dms-access-for-tasks`. Scegli **Crea ruolo**.

Specifica dei dati supplementari per le impostazioni delle attività

Quando si crea o si modifica un'attività di replica per alcuni endpoint AWS DMS, l'attività potrebbe richiedere informazioni aggiuntive per eseguire la migrazione. È possibile specificare queste informazioni aggiuntive tramite un'opzione nella console DMS. Oppure è possibile specificarle utilizzando il parametro `TaskData` per l'operazione API DMS `CreateReplicationTask` o `ModifyReplicationTask`.

Se l'endpoint di destinazione è Amazon Neptune, è necessario specificare i dati della mappatura, che sono supplementari rispetto a quelli di mappatura delle tabelle. Questi dati di mappatura supplementari indicano come convertire i dati relazionali di origine in dati a grafo di destinazione utilizzabili da un database Neptune. In tal caso è possibile utilizzare uno dei due possibili formati. Per ulteriori informazioni, consulta [Specifiche delle regole di mappatura del grafo utilizzando Gremlin e R2RML per Amazon Neptune come destinazione](#).

Monitoraggio delle attività AWS DMS

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di AWS DMS e delle soluzioni AWS. È consigliabile raccogliere dati di monitoraggio da tutte le parti della soluzione AWS per eseguire più facilmente il debug di guasti in più punti nel caso si verificano. AWS fornisce diversi strumenti per il monitoraggio delle attività e delle risorse AWS DMS, nonché la risposta a potenziali incidenti.

Eventi e notifiche in AWS DMS

AWS DMS usa Amazon Simple Notification Service (Amazon SNS) per fornire le notifiche quando si verifica un evento AWS DMS, ad esempio la creazione o l'eliminazione di un'istanza di replica. AWS DMS raggruppa gli eventi in categorie a cui puoi abbonarti in modo da ricevere la notifica quando in una categoria si verifica un evento. Ad esempio, con la sottoscrizione alla categoria Creazione per una determinata istanza di replica, ricevi una notifica ogni volta che si verifica un evento relativo alla creazione che interessa l'istanza di replica. Queste notifiche possono essere utilizzate in qualsiasi formato supportato da Amazon SNS per una regione AWS, ad esempio un messaggio e-mail, un SMS o una chiamata a un endpoint HTTP. Per ulteriori informazioni, consulta [Utilizzo degli eventi e delle notifiche Amazon SNS in AWS Database Migration Service](#)

Stato dell'attività

Puoi monitorare l'avanzamento dell'attività attraverso la verifica dello stato e il monitoraggio della tabella di controllo dell'attività. Lo stato dell'attività indica la condizione di un'attività AWS DMS e le relative risorse associate. Include queste indicazioni quando l'attività è creata, avviata, in esecuzione o arrestata. Include anche lo stato corrente delle tabelle migrate dall'attività, ad esempio se il carico completo di una tabella è iniziato o è in corso e altri dettagli come il numero di inserimenti, eliminazioni e aggiornamenti eseguiti per la tabella. Per ulteriori informazioni sul monitoraggio dell'attività e della condizione della risorsa attività, consulta [Stato dell'attività e Stato delle tabelle durante le attività](#). Per ulteriori informazioni sulle tabelle di controllo, consultare [Impostazioni delle attività delle tabelle di controllo](#).

Allarmi e log Amazon CloudWatch

Con gli allarmi Amazon CloudWatch puoi osservare una o più metriche delle attività relative a un periodo di tempo specificato. Se una metrica supera una determinata soglia, viene inviata una notifica a un argomento Amazon SNS. Gli allarmi CloudWatch non richiamano le operazioni perché si trovano in uno stato particolare. È necessario invece che lo stato cambi e venga mantenuto per un determinato numero di periodi. AWS DMS utilizza CloudWatch anche per

registrare le informazioni sulle attività durante il processo di migrazione. Puoi utilizzare l'AWS CLI o l'API AWS DMS per visualizzare le informazioni sui registri attività. Per ulteriori informazioni sull'utilizzo di CloudWatch con AWS DMS, consulta [Monitoraggio delle attività di replica usando Amazon CloudWatch](#). Per ulteriori informazioni sui parametri di monitoraggio di AWS DMS, consulta [Parametri di AWS Database Migration Service](#). Per ulteriori informazioni sull'utilizzo dei log di attività AWS DMS, consulta [Visualizzazione e gestione dei log delle attività AWS DMS](#).

Log di Time Travel

Puoi utilizzare AWS DMS Time Travel per registrare ed eseguire il debug delle attività di replica. Con questo approccio usi Amazon S3 per archiviare e crittografare i log con le chiavi di crittografia. Puoi recuperare i log S3 utilizzando i filtri di data e ora, quindi puoi visualizzare, scaricare e offuscare i log in base alle esigenze. In questo modo, puoi andare indietro nel tempo per esaminare le attività del database.

Puoi usare Time Travel con gli endpoint di origine PostgreSQL supportati da DMS e gli endpoint di destinazione PostgreSQL e MySQL supportati da DMS. Puoi attivare Time Travel solo per le attività di pieno carico e CDC e le attività di sola CDC. Per attivare Time Travel o modificarne le impostazioni esistenti, assicurati che l'attività sia interrotta.

Per ulteriori informazioni sui log Time Travel, consulta [Impostazioni delle attività Time Travel](#). Per le best practice per l'utilizzo dei log Time Travel, consulta [Risoluzione dei problemi delle attività di replica con Time Travel](#).

Log AWS CloudTrail

AWS DMS è integrato con AWS CloudTrail, un servizio che offre un record delle azioni eseguite da un utente, un ruolo IAM o un servizio AWS in AWS DMS. CloudTrail acquisisce tutte le chiamate API per AWS DMS come eventi, incluse le chiamate della console AWS DMS e le chiamate del codice alle operazioni API AWS DMS. Se viene creato un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per AWS DMS. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS DMS, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli. Per ulteriori informazioni, consulta [Registrazione delle chiamate API AWS DMS con AWS CloudTrail](#).

Log di database

Puoi visualizzare, scaricare e osservare i log di database per gli endpoint di attività utilizzando la AWS Management Console, l'AWS CLI o l'API per il servizio di database AWS. Per ulteriori

informazioni, consulta la documentazione per il servizio di database in uso nella [documentazione di AWS](#).

Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

- [Stato dell'attività](#)
- [Stato delle tabelle durante le attività](#)
- [Monitoraggio delle attività di replica usando Amazon CloudWatch](#)
- [Parametri di AWS Database Migration Service](#)
- [Visualizzazione e gestione dei log delle attività AWS DMS](#)
- [Registrazione delle chiamate API AWS DMS con AWS CloudTrail](#)
- [Registrazione di log di contesto AWS DMS](#)

Stato dell'attività

Lo stato dell'attività indica la condizione dell'attività. La tabella seguente mostra i possibili stati di un'attività:

Stato dell'attività	Descrizione
Creating (Creazione in corso)	AWS DMS sta creando l'attività.
In esecuzione	L'attività sta eseguendo le operazioni di migrazione specificate.
Arrestate	L'attività è arrestata.
Stopping (In arresto)	L'attività è in fase di arresto. In genere, questa è un'indicazione dell'intervento dell'utente nell'attività.
Deleting (Eliminazione in corso)	L'attività è in fase di eliminazione, in genere da una richiesta di intervento dell'utente.
Failed (Non riuscito)	L'attività non è andata a buon fine. Per ulteriori informazioni, consulta i file di log delle attività.

Stato dell'attività	Descrizione
Errore	L'attività è stata interrotta a causa di un errore. Una breve descrizione dell'errore dell'attività è fornita nella sezione dell'ultimo messaggio di errore della scheda Panoramica.
Esecuzione in corso con errori	L'attività è in esecuzione con uno stato di errore. In genere indica che non è stato possibile migrare una o più tabelle dell'attività. L'attività continua a caricare le altre tabelle in base alle regole di selezione.
Avvio di	L'attività si collega all'istanza di replica e agli endpoint di origine e di destinazione. Viene applicato qualsiasi filtro e trasformazione.
Pronto	L'attività è pronta per l'esecuzione. Questo stato segue in genere lo stato "Creating" (Creazione in corso).
Modifying (Modifica in corso)	L'attività viene modificata, in genere a causa di un'operazione dell'utente che ha modificato le impostazioni delle attività.
Spostamento in corso	L'attività è in fase di spostamento in un'altra istanza di replica. La replica rimane in questo stato fino al completamento dello spostamento. L'eliminazione dell'attività è l'unica operazione consentita sull'attività di replica durante lo spostamento.
Spostamento non riuscito	Lo spostamento dell'attività non è riuscito per un qualsiasi motivo, ad esempio lo spazio di archiviazione insufficiente sull'istanza di replica di destinazione. Quando un'attività di replica si trova in questo stato, può essere avviata, modificata, spostata o eliminata.
Test in corso	La migrazione del database specificata per questa attività viene testata in risposta all'esecuzione dell'operazione StartReplicationTaskAssessmentRun o StartReplicationTaskAssessment .

La barra di stato dell'attività fornisce una stima dell'avanzamento dell'attività. La qualità di questa stima dipende dalla qualità delle statistiche della tabella del database di origine; migliori sono le statistiche della tabella, più accurata è la stima. Per le attività con una sola tabella che non prevede alcuna statistica delle righe stimate, non siamo in grado di fornire alcuna stima della percentuale di completamento. In questo caso, lo stato dell'attività e l'indicazione delle righe caricate può essere utilizzata per confermare che l'attività è effettivamente in esecuzione e in avanzamento.

Tieni presente che la colonna "Ultimo aggiornamento" della console DMS indica solo l'ora in cui AWS DMS ha eseguito l'ultimo aggiornamento del record delle statistiche per una tabella. Non indica l'ora dell'ultimo aggiornamento della tabella.

Oltre a utilizzare la console DMS, è possibile generare una descrizione delle attività di replica correnti comprensiva dello stato usando il comando `aws dms describe-replication-tasks` nella [AWS CLI](#), come illustrato nell'esempio seguente.

```
{
  "ReplicationTasks": [
    {
      "ReplicationTaskIdentifier": "moveit2",
      "SourceEndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:6GGI6YPWYGAYUVLKIB732KEVWA",
      "TargetEndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:E0M4SFKCZEYHZBFGAGZT3QEC5U",
      "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T30M70UB5NM2LCVZF7JPGJRNUE",
      "MigrationType": "full-load",
      "TableMappings": "...output omitted... ",
      "ReplicationTaskSettings": "...output omitted... ",
      "Status": "stopped",
      "StopReason": "Stop Reason FULL_LOAD_ONLY_FINISHED",
      "ReplicationTaskCreationDate": 1590524772.505,
      "ReplicationTaskStartDate": 1590619805.212,
      "ReplicationTaskArn": "arn:aws:dms:us-east-1:123456789012:task:K55IUCGBASJS5VHZJIINA45FII",
      "ReplicationTaskStats": {
        "FullLoadProgressPercent": 100,
        "ElapsedTimeMillis": 0,
        "TablesLoaded": 0,
        "TablesLoading": 0,
        "TablesQueued": 0,
        "TablesErrored": 0,
        "FreshStartDate": 1590619811.528,
      }
    }
  ]
}
```



```

    "StartDate": 1590619811.528,
    "StopDate": 1590619842.068
  }
}
]
}

```

Stato delle tabelle durante le attività

La console AWS DMS aggiorna le informazioni riguardanti lo stato delle tabelle durante la migrazione. La tabella seguente mostra i valori di stato possibili:

The screenshot shows the AWS DMS console interface for a migration task named 'dms-gs-task'. The 'Table statistics' tab is selected and highlighted with a red box. The status is 'Running with errors' and the type is 'Full load, ongoing replication'. Below the navigation tabs, the 'Table statistics (157)' section is visible, showing a search bar and a table with columns: Schema name, Table, Load state, and Elapsed load time. The 'Load state' column is highlighted with a red box, and the 'Table error' entry for the 'user' table is also highlighted.

Schema name	Table	Load state	Elapsed load time
mysql	user	Table error	< 1 s
mysql	server_cost	Table completed	< 1 s
mysql	tables_priv	Table completed	< 1 s
mysql	gtid_executed	Table completed	< 1 s
mysql	replication_asynchronous_connection_failover	Table completed	< 1 s

Stato	Descrizione
Table does not exist (Questa tabella non esiste)	AWS DMS non è in grado di trovare la tabella sull'endpoint di origine.
Before load (Prima del caricamento)	Il processo di caricamento completo è stato attivato, ma non ancora avviato.
Full load (Caricamento completo)	Il processo di caricamento completo è in corso.

Stato	Descrizione
Table completed (Tabella completata)	Il caricamento completo è stato eseguito.
Table cancelled (Tabella annullata)	Il caricamento della tabella è stato annullato.
Table error (Errore della tabella)	Si è verificato un errore durante il caricamento della tabella.

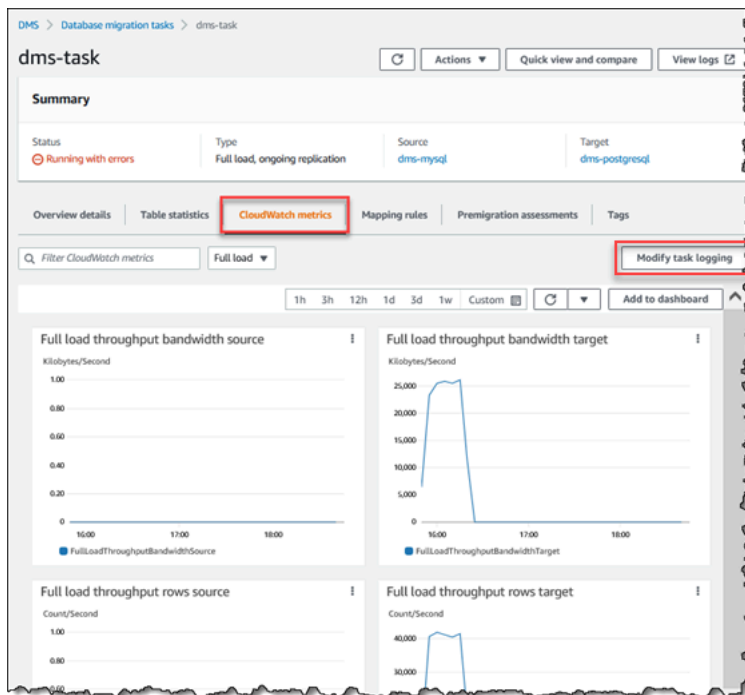
Monitoraggio delle attività di replica usando Amazon CloudWatch

Puoi usare gli allarmi o gli eventi di Amazon CloudWatch per monitorare la migrazione in maniera più efficace. Per ulteriori informazioni su Amazon CloudWatch, consulta [Che cosa sono Amazon CloudWatch, Eventi Amazon CloudWatch e File di log Amazon CloudWatch?](#) nella Guida per l'utente di Amazon CloudWatch. Tieni presente che l'utilizzo di Amazon CloudWatch comporterà un addebito.

Se l'attività di replica non crea i log CloudWatch, consulta [AWS DMS non crea registri CloudWatch](#) nella guida alla risoluzione dei problemi.

La console AWS DMS mostra le statistiche CloudWatch di base per ciascuna attività, che includono lo stato dell'attività, la percentuale di completamento, il tempo trascorso e le statistiche delle tabelle, come mostrato di seguito. Seleziona l'attività di replica, quindi scegli la scheda Parametri CloudWatch.

Per visualizzare e modificare le impostazioni del log delle attività CloudWatch scegli Modifica la registrazione delle attività. Per ulteriori informazioni, consulta [Registrazione delle impostazioni delle attività](#).

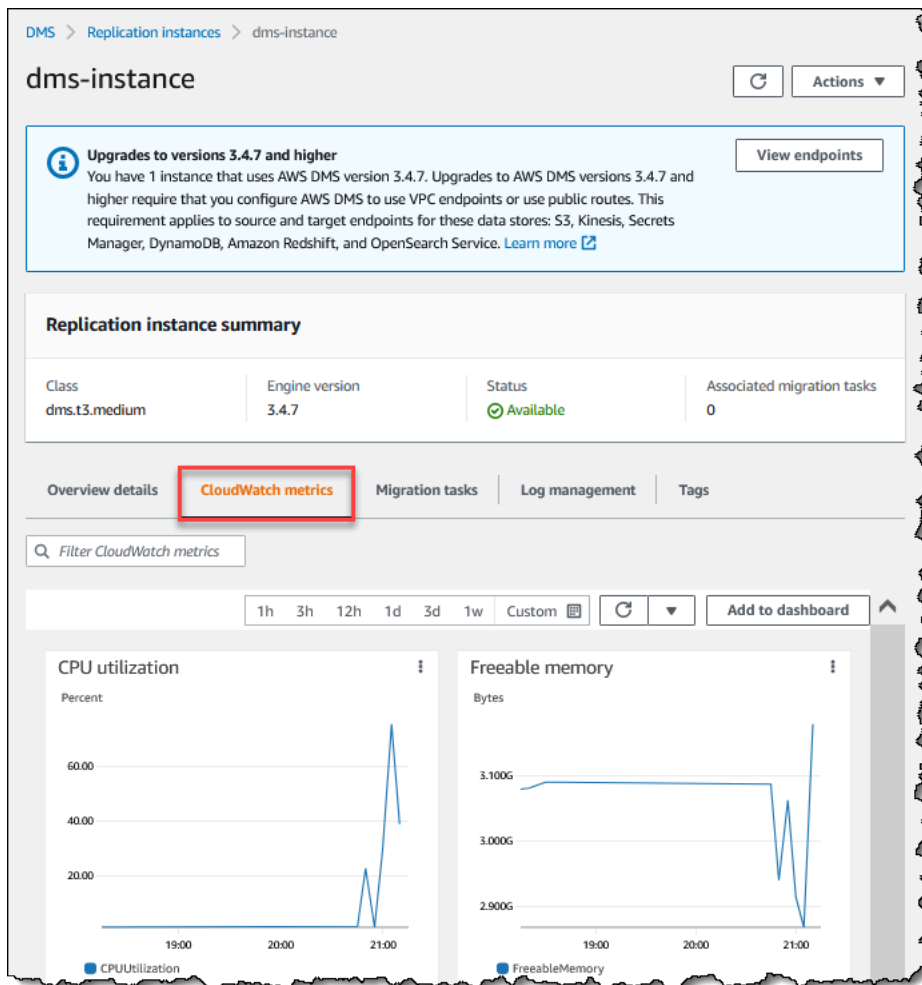


Quando si seleziona la scheda Statistiche della tabella, la console AWS DMS mostra per ogni tabella le statistiche delle prestazioni, tra cui il numero di inserimenti, eliminazioni e aggiornamenti.

The screenshot shows the 'Table statistics' page in the AWS DMS console. The 'Table statistics' tab is selected and highlighted with a red box. The page displays a table with columns for Schema name, Table, Load state, Elapsed load time, Inserts, Deletes, Updates, DDLs, and Applied inserts. The 'Inserts', 'Deletes', 'Updates', and 'DDLs' columns are highlighted with a red box. The table shows statistics for 173 tables, including 'mysql.user', 'mysql.server_cost', 'dms_sample.seat_type', and 'mysql.tables_priv'.

Schema name	Table	Load state	Elapsed load time	Inserts	Deletes	Updates	DDLs	Applied inserts
mysql	user	Table error	1 s	0	0	0	0	0
mysql	server_cost	Table completed	1 s	0	0	0	0	0
dms_sample	seat_type	Table completed	< 1 s	0	0	0	0	0
mysql	tables_priv	Table completed	1 s	0	0	0	0	0

Inoltre, se selezioni un'istanza di replica nella pagina Istanza di replica, puoi visualizzare le metriche relative alle prestazioni dell'istanza selezionando la scheda Parametri CloudWatch.



Parametri di AWS Database Migration Service

AWS DMS fornisce le statistiche per i seguenti elementi:

- Parametri host: statistiche di prestazioni e utilizzo dell'host di replica fornite da Amazon CloudWatch. Per un elenco completo dei parametri disponibili, consulta [Parametri dell' stanza di replica](#).
- Parametri dell'attività di replica: statistiche delle attività di replica, tra cui le modifiche in entrata e quelle sottoposte a commit nonché la latenza tra l'host di replica ed entrambi i database di origine e di destinazione. Per un elenco completo dei parametri disponibili, consulta [Parametri dell'attività di replica](#).
- Parametri tabella: statistiche delle tabelle in fase di migrazione, tra cui il numero di inserimenti, aggiornamenti, eliminazioni e istruzioni DDL completati.

I parametri dell'attività sono divisi in statistiche tra l'host di replica e l'endpoint di origine e statistiche tra l'host di replica e l'endpoint di destinazione. Puoi determinare le statistiche totali di un'attività unendo due statistiche correlate. Ad esempio, puoi determinare la latenza totale o il ritardo della replica di un'attività combinando i valori `CDCLatencySource` e `CDCLatencyTarget`.

I valori dei parametri dell'attività possono essere influenzati dall'attività corrente sul database di origine. Ad esempio, se una transazione è iniziata ma non è stata sottoposta al commit, il parametro `CDCLatencySource` continua a crescere finché non verrà eseguito il commit della transazione.

Per l'istanza di replica, il parametro `FreeableMemory` richiede chiarimenti. La memoria liberabile non è un'indicazione della memoria effettiva libera disponibile. È la memoria attualmente in uso che può essere liberata e utilizzata per altri scopi; è una combinazione di buffer e cache in uso sull'istanza di replica.

Sebbene il parametro `FreeableMemory` non rifletta la memoria effettiva libera disponibile, la combinazione dei parametri `FreeableMemory` e `SwapUsage` può indicare se l'istanza di replica è sovraccarica.

Monitora questi due parametri per le seguenti condizioni.

- Prossimità allo zero del parametro `FreeableMemory`.
- Aumento o oscillazione del parametro `SwapUsage`.

Se si verifica una di queste due condizioni, significa che devi considerare il passaggio a un'istanza di replica di dimensioni maggiori. Devi anche considerare di dover ridurre il numero e il tipo di attività in esecuzione nell'istanza di replica. Le attività di caricamento completo richiedono più memoria di quelle che replicano solo modifiche.

Per stimare approssimativamente i requisiti di memoria effettivi per un'attività di migrazione AWS DMS, è possibile utilizzare i seguenti parametri.

Colonne LOB

Il numero medio di colonne LOB di ogni tabella nell'ambito della migrazione.

Maximum number of tables to load in parallel (Numero massimo di tabelle da caricare in parallelo)

Il numero massimo di tabelle caricate da AWS DMS in parallelo in un'unica attività.

Il valore predefinito è 8.

Dimensione blocco LOB

La dimensione in kilobyte dei blocchi LOB utilizzati da AWS DMS per replicare i dati nel database di destinazione.

Tasso di commit durante il pieno carico

Il numero massimo di record che AWS DMS può trasferire in parallelo.

Il valore predefinito è 10,000.

Dimensione LOB

La dimensione massima in kilobyte di un singolo LOB.

Dimensione array in blocco

Il numero massimo di righe che vengono recuperate o elaborate dal driver dell'endpoint. Questo valore dipende dalle impostazioni del driver.

Il valore predefinito è 1,000.

Dopo aver determinato questi valori, puoi utilizzare uno dei seguenti metodi per stimare la quantità di memoria richiesta per l'attività di migrazione. I metodi dipendono dall'opzione scelta per Impostazioni della colonna LOB nell'attività di migrazione.

- Per Modalità LOB completa usa la formula seguente.

$$\text{Required memory} = (\text{LOB columns}) * (\text{Maximum number of tables to load in parallel}) * (\text{LOB chunk size}) * (\text{Commit rate during full load})$$

Considera un esempio in cui le tabelle di origine includono in media 2 colonne LOB e la dimensione dei blocchi LOB è di 64 KB. Se utilizzi i valori predefiniti per Maximum number of tables to load in parallel e Commit rate during full load, la quantità di memoria richiesta per l'attività è determinata come segue.

$$\text{Required memory} = 2 * 8 * 64 * 10,000 = 10,240,000 \text{ KB}$$

Note

Per ridurre il valore di Tasso di commit durante il pieno carico, apri la console AWS DMS, scegli Attività di migrazione del database e crea o modifica un'attività. Espandi Impostazioni avanzate e inserisci il valore per Tasso di commit durante il pieno carico.

- Per Modalità LOB limitata usa la formula seguente.

$$\text{Required memory} = (\text{LOB columns}) * (\text{Maximum number of tables to load in parallel}) * (\text{LOB size}) * (\text{Bulk array size})$$

Considera un esempio in cui le tabelle di origine includono in media 2 colonne LOB e la dimensione massima di un singolo LOB è di 4.096 KB. Se utilizzi i valori predefiniti per Maximum number of tables to load in parallel e Bulk array size, la quantità di memoria richiesta per l'attività è determinata come segue.

$$\text{Required memory} = 2 * 8 * 4,096 * 1,000 = 65,536,000 \text{ KB}$$

AWS DMS esegue le conversioni in modo ottimale quando la CPU è disponibile al momento delle conversioni. Il sovraccarico della CPU e la mancanza di risorse CPU sufficienti possono causare migrazioni lente. AWS DMS può richiedere un uso intensivo della CPU, soprattutto quando si eseguono migrazioni e repliche eterogenee, come la migrazione da Oracle a PostgreSQL. In questi casi, la classe di istanza di replica C4 può rappresentare una scelta adeguata. Per ulteriori informazioni, consulta [Scelta dell'istanza di replica AWS DMS giusta per la migrazione](#).

Parametri dell'istanza di replica

Il monitoraggio dell'istanza di replica include le metriche Amazon CloudWatch per le seguenti statistiche.

Parametro	Descrizione
AvailableMemory	Una stima della quantità di memoria disponibile per l'avvio di nuove applicazioni, senza swap. Per ulteriori informazioni, consulta il valore MemAvailable nella sezione /proc/memInfo di Linux man-pages .

Parametro	Descrizione
	Unità: byte
CPUAllocated	<p>La percentuale massima di CPU allocata per l'attività (0 indica nessun limite).</p> <p>AWS DMS aumenta questa metrica in relazione alle dimensioni combinate di <code>ReplicationInstanceIdentifier</code> e <code>ReplicationTaskIdentifier</code> nella console CloudWatch. Utilizza la categoria <code>ReplicationInstanceIdentifier</code>, <code>ReplicationTaskIdentifier</code> per visualizzare questa metrica.</p> <p>Unità: percentuale</p>
CPUUtilization	<p>La percentuale della vCPU (CPU virtuale) allocata attualmente in uso nell'istanza.</p> <p>Unità: percentuale</p>
DiskQueueDepth	<p>Il numero di richieste di lettura/scrittura (I/O) in sospeso che sono in attesa di accedere al disco.</p> <p>Unità: numero</p>
FreeStorageSpace	<p>La quantità di spazio di storage disponibile.</p> <p>Unità: byte</p>
FreeMemory	<p>La quantità di memoria fisica disponibile per l'uso da parte delle applicazioni, della cache delle pagine e delle strutture di dati del kernel. Per ulteriori informazioni, consulta il valore <code>MemFree</code> nella sezione <code>/proc/memInfo</code> di Linux man-pages.</p> <p>Unità: byte</p>
FreeableMemory	<p>La quantità di memoria RAM disponibile.</p> <p>Unità: byte</p>

Parametro	Descrizione
MemoryAllocated	<p>L'allocazione massima di memoria per l'attività (0 indica nessun limite).</p> <p>AWS DMS aumenta questa metrica in relazione alle dimensioni combinate di <code>ReplicationInstanceIdentifier</code> e <code>ReplicationTaskIdentifier</code> nella console CloudWatch. Utilizza la categoria <code>ReplicationInstanceIdentifier</code>, <code>ReplicationTaskIdentifier</code> per visualizzare questa metrica.</p> <p>Unità: MiB</p>
WriteIOPS	<p>Il numero medio di operazioni di I/O di scrittura su disco al secondo.</p> <p>Unità: conteggio/secondo</p>
ReadIOPS	<p>Il numero medio di operazioni di I/O di lettura del disco al secondo.</p> <p>Unità: conteggio/secondo</p>
WriteThroughput	<p>Il numero medio di byte scritti sul disco al secondo.</p> <p>Unità: byte/secondo</p>
ReadThroughput	<p>Il numero medio di byte letti dal disco al secondo.</p> <p>Unità: byte/secondo</p>
WriteLatency	<p>La quantità di tempo media che occorre per ciascuna operazione I/O (output) su disco.</p> <p>Unità: millisecondi</p>
ReadLatency	<p>La quantità di tempo media che occorre per ciascuna operazione I/O (input) su disco.</p> <p>Unità: millisecondi</p>
SwapUsage	<p>La quantità di spazio di swapping utilizzato sull'istanza di replica.</p> <p>Unità: byte</p>

Parametro	Descrizione
NetworkTransmitThroughput	<p>Il traffico di rete in uscita (trasmissione) sull'istanza di replica, inclusi il traffico del database del cliente e il traffico di AWS DMS utilizzati per le attività di monitoraggio e replica.</p> <p>Unità: byte/secondo</p>
NetworkReceiveThroughput	<p>Il traffico di rete in entrata (ricezione) sull'istanza di replica, inclusi il traffico del database del cliente e il traffico di AWS DMS utilizzati per le attività di monitoraggio e replica.</p> <p>Unità: byte/secondo</p>

Parametri dell'attività di replica

Il monitoraggio dell'attività di replica include le metriche per le seguenti statistiche.

Parametro	Descrizione
FullLoadThroughputBandwidthTarget	Dati in uscita trasmessi da un pieno carico per la destinazione in KB al secondo.
FullLoadThroughputRowsTarget	Modifiche in uscita da un pieno carico per la destinazione in righe al secondo.
CDCIncomingChanges	Numero totale di eventi di modifica in un momento specifico in attesa di essere applicati alla destinazione. Tieni presente che questo non equivale alla misura della frequenza di modifica della transazione dell'endpoint di origine. Un numero elevato per questa metrica indica in genere che AWS DMS non è in grado di applicare le modifiche acquisite in modo tempestivo, causando un'elevata latenza nella destinazione.
CDCChangeMemorySource	Quantità di righe che si accumulano in una memoria e attendono il commit dall'origine. È possibile visualizzare questa metrica insieme a CDCChangesDiskSource.

Parametro	Descrizione
CDCChange sMemoryTarget	Quantità di righe che si accumulano in una memoria e attendono il commit alla destinazione. È possibile visualizzare questa metrica insieme a CDCChangesDiskTarget.
CDCChangesDiskSource	Quantità di righe che si accumulano su disco e attendono il commit dall'origine. È possibile visualizzare questa metrica insieme a CDCChangesMemorySource.
CDCChangesDiskTarget	Quantità di righe che si accumulano su disco e attendono il commit alla destinazione. È possibile visualizzare questa metrica insieme a CDCChangesMemoryTarget.
CDCThroughputBandwidthTarget	Dati in uscita trasmessi per la destinazione in KB al secondo. CDCThroughputBandwidth registra i dati in uscita trasmessi sui punti di campionamento. Se non viene rilevato traffico di rete per l'attività, il valore è zero. CDC non emette transazioni di lunga durata, pertanto il traffico di rete potrebbe non essere registrato.
CDCThroughputRowsSource	Modifiche dell'attività in entrata dall'origine in righe al secondo.
CDCThroughputRowsTarget	Modifiche dell'attività in uscita per la destinazione in righe al secondo.

Parametro	Descrizione
CDCLatencySource	<p>Il divario, in secondi, tra l'ultimo evento acquisito dall'endpoint di origine e il timestamp di sistema corrente dell'istanza AWS DMS. CDCLatencySource rappresenta la latenza tra l'origine e l'istanza di replica. Un valore di CDCLatencySource elevato indica che il processo di acquisizione delle modifiche dall'origine è ritardato. Per identificare la latenza di una replica continua, è possibile visualizzare questa metrica insieme a CDCLatencyTarget. Se i valori di CDCLatencySource e CDCLatencyTarget sono entrambi elevati, esamina prima CDCLatencySource.</p> <p>Il valore di CDCSourceLatency può essere 0 quando non vi è alcun ritardo di replica tra l'origine e l'istanza di replica. Inoltre, il valore di CDCSourceLatency può diventare zero quando l'attività di replica tenta di leggere l'evento successivo nel log delle transazioni dell'origine e non vengono rilevati nuovi eventi rispetto all'ultima lettura dell'origine. In questo caso, l'attività reimposta CDCSourceLatency su 0.</p>
CDCLatencyTarget	<p>Il divario, in secondi, tra il primo timestamp dell'evento in attesa di commit sulla destinazione e il timestamp corrente dell'istanza AWS DMS. La latenza della destinazione è la differenza tra l'ora del server dell'istanza di replica e l'ID dell'evento non confermato meno recente inoltrato a un componente di destinazione. In altre parole, la latenza della destinazione è la differenza di timestamp tra l'istanza di replica e l'evento meno recente applicato ma non confermato dall'endpoint di destinazione (99%). Quando il valore di CDCLatencyTarget è elevato, indica che il processo di applicazione degli eventi di modifica alla destinazione è ritardato. Per identificare la latenza di una replica continua, è possibile visualizzare questa metrica insieme a CDCLatencySource. Se il valore di CDCLatencyTarget è elevato, ma non quello di CDCLatencySource, verifica se:</p> <ul style="list-style-type: none">• mancano indici o chiave primarie nella destinazione;• si verificano colli di bottiglia relativi alle risorse nella destinazione o nell'istanza di replica;• i problemi di rete risiedono tra l'istanza di replica e la destinazione.

Parametro	Descrizione
CPUUtilization	<p>La percentuale di CPU utilizzata da un'attività su più core. La semantica della metrica CPUUtilization dell'attività è leggermente diversa da quella della metrica CPUUtilization della replica. Se una vCPU è completamente utilizzata, indica il 100%, ma se sono in uso più vCPU, il valore potrebbe essere superiore al 100%.</p> <p>Unità: percentuale</p>
SwapUsage	<p>La quantità di memoria swap utilizzata dall'attività.</p> <p>Unità: byte</p>
MemoryUsage	<p>La quantità di <code>memory.usage_in_bytes</code> utilizzata da un'attività nel gruppo di controllo (cgroup). DMS usa i cgroup per controllare l'utilizzo delle risorse di sistema, come memoria e CPU. Questa metrica indica l'utilizzo in megabyte della memoria di un'attività nel relativo cgroup allocato. I limiti del cgroup si basano sulle risorse disponibili per la classe di istanza di replica DMS. Il valore di <code>memory.usage_in_bytes</code> è costituito dai componenti di memoria RSS (Resident Set Size), cache e swap. Il sistema operativo può recuperare la memoria cache se necessario. Ti consigliamo di monitorare anche la metrica dell'istanza di replica <code>AvailableMemory</code>.</p> <p>AWS DMS aumenta questa metrica in relazione alle dimensioni combinate di <code>ReplicationInstanceIdentifier</code> e <code>ReplicationTaskIdentifier</code> nella console CloudWatch. Utilizza la categoria <code>ReplicationInstanceIdentifier</code>, <code>ReplicationTaskIdentifier</code> per visualizzare questa metrica.</p>

Visualizzazione e gestione dei log delle attività AWS DMS

È possibile utilizzare Amazon CloudWatch per registrare le informazioni sulle attività durante un processo di migrazione AWS DMS. Attivare la registrazione quando si selezionano le impostazioni delle attività. Per ulteriori informazioni, consulta [Registrazione delle impostazioni delle attività](#).

Per visualizzare i registri di un'attività eseguita, attenersi alla seguente procedura:

1. Aprire la console AWS DMS e scegliere Attività di migrazione database dal riquadro di navigazione. Viene visualizzata la finestra di dialogo Attività di migrazione del database.
2. Selezionare il nome dell'attività. Viene visualizzata la finestra di dialogo Dettagli panoramica.
3. Individuare la sezione Registri attività di migrazione e scegliere Visualizza log CloudWatch.

Inoltre, è possibile utilizzare la AWS CLI o l'API AWS DMS per visualizzare le informazioni sui log delle attività. Per farlo, usa il comando `describe-replication-instance-task-logs` della AWS CLI oppure l'operazione `DescribeReplicationInstanceTaskLogs` dell'API AWS DMS.

Ad esempio, il seguente comando della AWS CLI mostra i metadati dei log delle attività in formato JSON.

```
$ aws dms describe-replication-instance-task-logs \  
  --replication-instance-arn arn:aws:dms:us-east-1:237565436:rep:CDSFSFSFFFSSUFCA Y
```

Un esempio di risposta del comando è la seguente.

```
{  
  "ReplicationInstanceTaskLogs": [  
    {  
      "ReplicationTaskArn": "arn:aws:dms:us-  
east-1:237565436:task:MY34U6Z4MSY52GRTIX304AY",  
      "ReplicationTaskName": "mysql-to-ddb",  
      "ReplicationInstanceTaskLogSize": 3726134  
    }  
  ],  
  "ReplicationInstanceArn": "arn:aws:dms:us-east-1:237565436:rep:CDSFSFSFFFSSUFCA Y"  
}
```

In questo tipo di risposta, un unico log dell'attività (`mysql-to-ddb`) è associato all'istanza di replica. La dimensione del log è 3.726.124 byte.

Puoi utilizzare le informazioni restituite da `describe-replication-instance-task-logs` per diagnosticare e risolvere eventuali problemi relativi ai log delle attività. Ad esempio, se abiliti la registrazione del log dettagliato del debug per un'attività, la dimensione del log delle attività crescerà

rapidamente, consumando potenzialmente tutto lo spazio di archiviazione disponibile sull'istanza di replica e causando la modifica dello stato dell'istanza su `storage-full`. Con la descrizione dei log delle attività, puoi determinare quelli non più necessari ed eliminarli, liberando spazio di storage.

Per eliminare i log di un'attività, configura l'impostazione `DeleteTaskLogs` su `true`. Ad esempio, il JSON seguente elimina i log delle attività quando si modifica un'attività utilizzando il comando `modify-replication-task` della AWS CLI o l'operazione `ModifyReplicationTask` dell'API AWS DMS.

```
{
  "Logging": {
    "DeleteTaskLogs":true
  }
}
```

Registrazione delle chiamate API AWS DMS con AWS CloudTrail

AWS DMS è integrato con AWS CloudTrail, un servizio che offre un record delle operazioni eseguite da un utente, un ruolo o un servizio AWS in AWS DMS. CloudTrail acquisisce tutte le chiamate API per AWS DMS come eventi, incluse le chiamate della console AWS DMS e le chiamate del codice alle operazioni API AWS DMS. Se viene creato un trail, è possibile abilitare la distribuzione continua di eventi CloudTrail in un bucket Amazon S3, inclusi gli eventi per AWS DMS. Se non si configura un trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia eventi). Le informazioni raccolte da CloudTrail consentono di determinare la richiesta effettuata ad AWS DMS, l'indirizzo IP da cui è partita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita e altri dettagli.

Per ulteriori informazioni su CloudTrail, consultare la [AWS CloudTrail Guida per l'utente di](#) .

Informazioni su AWS DMS in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività in AWS DMS, tale attività viene registrata in un evento CloudTrail insieme ad altri eventi di servizio AWS nella Cronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta [Visualizzazione di eventi mediante la cronologia eventi di CloudTrail](#).

Per una registrazione continua degli eventi nell'account AWS che includa gli eventi per AWS DMS, creare un trail. Un percorso abilita la distribuzione da parte di CloudTrail dei file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il percorso registra gli eventi da tutte le regioni AWS nella partizione AWS e distribuisce i file di log nel bucket Simple Storage Service (Amazon S3) specificato. Inoltre, è possibile configurare altri servizi AWS per analizzare con maggiore dettaglio e usare i dati evento raccolti nei log CloudTrail. Per ulteriori informazioni, consulta:

- [Panoramica della creazione di un percorso](#)
- [Servizi e integrazioni CloudTrail supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di log CloudTrail da più regioni AWS](#) e [Ricezione di file di log CloudTrail da più account](#)

Tutte le operazioni AWS DMS vengono registrate da CloudTrail e sono documentate nella [documentazione di riferimento delle API di AWS Database Migration Service](#). Ad esempio, le chiamate alle operazioni `CreateReplicationInstance`, `TestConnection` e `StartReplicationTask` generano voci nei file di log di CloudTrail.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali dell'utente IAM 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](#).

Comprensione delle voci dei file di log di AWS DMS

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. I file di log di CloudTrail possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'fonte e include informazioni sul operazione richiesta, data e ora dell'operazione, parametri richiesti e così via. I file di log di CloudTrail non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di log di CloudTrail che illustra l'operazione `RebootReplicationInstance`.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE:johndoe",
    "arn": "arn:aws:sts::123456789012:assumed-role/admin/johndoe",
    "accountId": "123456789012",
    "accessKeyId": "ASIAYFI33SINAD0JJEZW",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-01T16:42:09Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/admin",
        "accountId": "123456789012",
        "userName": "admin"
      }
    }
  },
  "eventTime": "2018-08-02T00:11:44Z",
  "eventSource": "dms.amazonaws.com",
  "eventName": "RebootReplicationInstance",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.21.198.64",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "forceFailover": false,
    "replicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:EX4MBJ2NMRDL3BMAYJ0XUGYPUE"
  },
  "responseElements": {
    "replicationInstance": {
      "replicationInstanceIdentifier": "replication-instance-1",
      "replicationInstanceStatus": "rebooting",
      "allocatedStorage": 50,
      "replicationInstancePrivateIpAddresses": [
```

```
    "172.31.20.204"
  ],
  "instanceCreateTime": "Aug 1, 2018 11:56:21 PM",
  "autoMinorVersionUpgrade": true,
  "engineVersion": "2.4.3",
  "publiclyAccessible": true,
  "replicationInstanceClass": "dms.t2.medium",
  "availabilityZone": "us-east-1b",
  "kmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/
f7bc0f8e-1a3a-4ace-9faa-e8494fa3921a",
  "replicationSubnetGroup": {
    "vpcId": "vpc-1f6a9c6a",
    "subnetGroupStatus": "Complete",
    "replicationSubnetGroupArn": "arn:aws:dms:us-
east-1:123456789012:subgrp:EDHRVRBAAAPONQAIYWP4NUW22M",
    "subnets": [
      {
        "subnetIdentifier": "subnet-cbfff283",
        "subnetAvailabilityZone": {
          "name": "us-east-1b"
        },
        "subnetStatus": "Active"
      },
      {
        "subnetIdentifier": "subnet-d7c825e8",
        "subnetAvailabilityZone": {
          "name": "us-east-1e"
        },
        "subnetStatus": "Active"
      },
      {
        "subnetIdentifier": "subnet-6746046b",
        "subnetAvailabilityZone": {
          "name": "us-east-1f"
        },
        "subnetStatus": "Active"
      },
      {
        "subnetIdentifier": "subnet-bac383e0",
        "subnetAvailabilityZone": {
          "name": "us-east-1c"
        },
        "subnetStatus": "Active"
      }
    ]
  }
},
```

```

        {
            "subnetIdentifier": "subnet-42599426",
            "subnetAvailabilityZone": {
                "name": "us-east-1d"
            },
            "subnetStatus": "Active"
        },
        {
            "subnetIdentifier": "subnet-da327bf6",
            "subnetAvailabilityZone": {
                "name": "us-east-1a"
            },
            "subnetStatus": "Active"
        }
    ],
    "replicationSubnetGroupIdentifier": "default-vpc-1f6a9c6a",
    "replicationSubnetGroupDescription": "default group created by console
for vpc id vpc-1f6a9c6a"
},
"replicationInstanceEniId": "eni-0d6db8c7137cb9844",
"vpcSecurityGroups": [
    {
        "vpcSecurityGroupId": "sg-f839b688",
        "status": "active"
    }
],
"pendingModifiedValues": {},
"replicationInstancePublicIpAddresses": [
    "18.211.48.119"
],
"replicationInstancePublicIpAddress": "18.211.48.119",
"preferredMaintenanceWindow": "fri:22:44-fri:23:14",
"replicationInstanceArn": "arn:aws:dms:us-
east-1:123456789012:rep:EX4MBJ2NMRDL3BMAYJ0XUGYPUE",
"replicationInstanceEniIds": [
    "eni-0d6db8c7137cb9844"
],
"multiAZ": false,
"replicationInstancePrivateIpAddress": "172.31.20.204",
"patchingPrecedence": 0
}
},
"requestID": "a3c83c11-95e8-11e8-9d08-4b8f2b45bfd5",
"eventID": "b3c4adb1-e34b-4744-bdeb-35528062a541",

```

```
"eventType": "AwsApiCall",  
"recipientAccountId": "123456789012"  
}
```

Registrazione di log di contesto AWS DMS

AWS DMS utilizza la registrazione di log di contesto per fornire informazioni su una migrazione in corso. La registrazione di log di contesto scrive nel log CloudWatch dell'attività informazioni come le seguenti:

- Informazioni sulla connessione dell'attività ai database di origine e di destinazione.
- Comportamento dell'attività di replica. Puoi utilizzare i log delle attività per diagnosticare i problemi di replica.
- Istruzioni SQL senza dati eseguite da AWS DMS sui database di origine e di destinazione. Puoi utilizzare i log SQL per diagnosticare i comportamenti di migrazione imprevisti.
- Dettagli sulla posizione del flusso per ogni evento CDC.

La registrazione di log di contesto è disponibile solo in AWS DMS 3.5.0 o versioni successive.

AWS DMS attiva la registrazione di log di contesto per impostazione predefinita. Per controllare la registrazione di log di contesto, configura l'impostazione dell'attività `EnableLogContext` su `true` o `false` oppure modifica l'attività nella console.

AWS DMS scrive le informazioni del log di contesto nell'attività di replica del log CloudWatch ogni tre minuti. Assicurati che l'istanza di replica disponga dello spazio sufficiente per il log dell'applicazione. Per ulteriori informazioni sulla gestione dei log delle attività, consulta [Visualizzazione e gestione dei log delle attività AWS DMS](#).

Argomenti

- [Tipi di oggetto](#)
- [Esempi di log](#)
- [Limitazioni](#)

Tipi di oggetto

AWS DMS genera la registrazione di log di contesto in CloudWatch per i seguenti tipi di oggetti.

Tipo di oggetto	Descrizione
TABLE_NAME	Queste voci di log contengono informazioni sulle tabelle che rientrano nell'ambito della regola di mappatura delle attività corrente. Puoi utilizzare queste voci per esaminare gli eventi della tabella per un periodo specifico durante la migrazione.
SCHEMA_NAME	Queste voci di log contengono informazioni sugli schemi utilizzati dalla regola di mappatura delle attività corrente. Puoi utilizzare queste voci per determinare lo schema usato da AWS DMS per un periodo specifico durante la migrazione.
TRANSACTION_ID	Queste voci contengono l'ID della transazione per ogni modifica DML/DDI acquisita dal database di origine. Puoi utilizzare queste voci di log per determinare le modifiche che sono avvenute durante una determinata transazione.
CONNECTION_ID	Queste voci contengono l'ID della connessione. Puoi utilizzare queste voci di log per determinare la connessione usata da AWS DMS per ogni fase della migrazione.
STATEMENT	Queste voci contengono il codice SQL utilizzato per recuperare, elaborare e applicare ogni modifica della migrazione.
STREAM_POSITION	Queste voci contengono la posizione nel file di log delle transazioni di ogni azione di migrazione sul database di origine. Il formato di queste voci varia a seconda del tipo di motore del database di origine. Inoltre, puoi utilizzare queste informazioni per determinare la posizione iniziale di un checkpoint di ripristino.

Tipo di oggetto	Descrizione
	o durante la configurazione della replica sola CDC.

Esempi di log

In questa sezione sono illustrati esempi di record di log che puoi utilizzare per monitorare la replica e diagnosticarne i problemi.

Esempi di log di connessione

In questa sezione sono illustrati esempi di log che includono gli ID della connessione.

```
2023-02-22T10:09:29 [SOURCE_CAPTURE ]I: Capture record 1 to internal
queue from Source {operation:START_REGULAR (43), connectionId:27598,
streamPosition:0000124A/6800A778.NOW} (streamcomponent.c:2920)

2023-02-22T10:12:30 [SOURCE_CAPTURE ]I: Capture record 0 to internal queue from
Source {operation:IDLE (51), connectionId:27598} (streamcomponent.c:2920)

2023-02-22T11:25:27 [SOURCE_CAPTURE ]I: Capture record 0 to internal queue
from Source {operation:IDLE (51), columnName:region, connectionId:27598}
(streamcomponent.c:2920)
```

Esempi di log di comportamento delle attività

In questa sezione sono illustrati esempi di log relativi al comportamento del log delle attività di replica. Puoi utilizzare queste informazioni per diagnosticare i problemi di replica, ad esempio un'attività nello stato IDLE.

I seguenti log SOURCE_CAPTURE indicano che non ci sono eventi disponibili da leggere nel file di log del database di origine e contengono record TARGET_APPLY che indicano che non ci sono eventi ricevuti dai componenti CDC AWS DMS da applicare al database di destinazione. Questi eventi contengono anche i dettagli di contesto relativi agli eventi applicati in precedenza.

```
2023-02-22T11:23:24 [SOURCE_CAPTURE ]I: No Event fetched from wal log
(postgres_endpoint_wal_engine.c:1369)
2023-02-22T11:24:29 [TARGET_APPLY ]I: No records received to load
or apply on target , waiting for data from upstream. The last context
```

```
is {operation:INSERT (1), tableName:sales_11, schemaName:public,
txnId:18662441, connectionId:17855, statement:INSERT INTO
"public"."sales_11"("sales_no","dept_name","sale_amount","sale_date","region") values
(?,?,?,?/?),
```

Esempi di log di istruzioni SQL

In questa sezione sono illustrati esempi di log relativi alle istruzioni SQL eseguite sui database di origine e di destinazione. Le istruzioni SQL presenti nei log mostrano solo l'istruzione e non i dati. Il seguente log TARGET_APPLY mostra un'istruzione INSERT eseguita sulla destinazione.

```
2023-02-22T11:26:07 [TARGET_APPLY ]I: Applied record 2193305 to
target {operation:INSERT (1), tableName:sales_111, schemaName:public,
txnId:18761543, connectionId:17855, statement:INSERT INTO
"public"."sales_111"("sales_no","dept_name","sale_amount","sale_date","region") values
(?,?,?,?/?),
```

Limitazioni

Le seguenti limitazioni si applicano alla registrazione di log di contesto AWS DMS:

- AWS DMS crea una registrazione di log minima per tutti i tipi di endpoint e la registrazione di log di contesto estesa specifica del motore è disponibile solo per i seguenti tipi di endpoint. Ti consigliamo di attivare la registrazione di log di contesto quando usi questi tipi di endpoint.
 - MySQL
 - PostgreSQL
 - Oracle
 - Microsoft SQL Server
 - MongoDB/Amazon DocumentDB
 - Amazon S3

Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service

Puoi utilizzare Amazon EventBridge per inviare le notifiche quando si verifica un evento AWS DMS, ad esempio la creazione o l'eliminazione di un'istanza di replica. EventBridge riceve la notifica di eventi e percorsi come definito dalle regole dell'evento. Puoi utilizzare le notifiche in qualsiasi formato supportato da Amazon EventBridge per una regione AWS. Per ulteriori informazioni sull'utilizzo di Amazon EventBridge, consulta [What is Amazon EventBridge?](#) nella Guida per l'utente di Amazon EventBridge.

Note

L'utilizzo degli eventi Amazon EventBridge è supportato in AWS DMS 3.4.5 e versioni successive.

EventBridge riceve un evento, l'indicatore di una modifica nell'ambiente AWS DMS e applica una regola per instradare l'evento verso un meccanismo di notifica. Le regole abbinano gli eventi ai meccanismi di notifica in base alla struttura dell'evento, chiamata modello di eventi.

AWS DMS raggruppa gli eventi in categorie a cui puoi applicare una regola evento per poter ricevere una notifica quando si verifica un evento in quella categoria. Ad esempio, supponi di applicare una regola di evento EventBridge alla categoria Creazione per una determinata istanza di replica. Riceverai una notifica ogni volta che si verifica un evento correlato alla creazione che interessa l'istanza di replica. Con l'applicazione di una regola a una categoria Modifica della configurazione per un'istanza di replica, ricevi una notifica quando la configurazione dell'istanza di replica viene modificata. Per l'elenco delle categorie di eventi fornite da AWS DMS, consulta le categorie e i messaggi di eventi AWS DMS, di seguito.

Note

Per consentire la pubblicazione da events.amazonaws.com, assicurati di aggiornare le policy di accesso degli argomenti di Amazon SNS. Per ulteriori informazioni, consulta [Using resource-based policies for Amazon EventBridge](#) nella Guida per l'utente di Amazon EventBridge.

Per ulteriori informazioni sullo spostamento delle sottoscrizioni a eventi su Amazon EventBridge, consulta [Migrate active event subscriptions from DMS to Amazon EventBridge](#).

Per ulteriori informazioni sull'utilizzo di SMS con Amazon SNS, consulta [Sending and receiving SMS notifications using Amazon SNS](#).

Utilizzo delle regole di eventi di Amazon EventBridge per AWS DMS

Amazon EventBridge invia notifiche di eventi agli indirizzi fornito al momento della creazione di una regola di evento EventBridge. È possibile creare diverse regole di eventi. Ad esempio, è possibile creare una regola che riceve tutte le notifiche degli eventi e un'altra regola che include solo gli eventi critici per le risorse DMS di produzione. Puoi anche attivare o disattivare le notifiche di eventi in EventBridge.

Per creare le regole Amazon EventBridge che reagiscono agli eventi AWS DMS

- Esegui le fasi descritte in [Creazione di regole Amazon EventBridge che reagiscono agli eventi](#) nella Guida per l'utente di Amazon EventBridge crea una regola per gli eventi AWS DMS:
 - a. Specifica un'azione di notifica da intraprendere quando EventBridge riceve un evento che corrisponde al modello di evento nella regola. Quando un evento corrisponde, EventBridge invia l'evento e richiama l'azione definita nella regola.
 - b. Per Service provider (Provider di servizi), selezionare AWS.
 - c. Per Nome del servizio scegli Database Migration Service (DMS).

Inizi a ricevere le notifiche degli eventi.

Il seguente esempio JSON mostra un modello di eventi EventBridge per un servizio AWS DMS.

```
{
  "version": "0",
  "id": "11a11b11-222b-333a-44d4-01234a5b67890",
  "detail-type": "DMS Replication Task State Change",
  "source": "aws.dms",
  "account": "0123456789012",
  "time": "1970-01-01T00:00:00Z",
  "region": "us-east-1",
  "resources": [
    "arn:aws:dms:us-east-1:012345678901:task:AAAABBBB0CCCCDDDEEEEEE1FFFF2GGG3FFFFFFF3"
  ],
}
```

```
"detail":{
  "type":"REPLICATION_TASK",
  "category":"StateChange",
  "eventType":"REPLICATION_TASK_STARTED",
  "eventId":"DMS-EVENT-0069",
  "resourceLink":"https://console.aws.amazon.com/dms/v2/home?region=us-east-1#taskDetails/taskName",
  "detailMessage":"Replication task started, with flag = fresh start"
}
```

Per un elenco delle categorie e degli eventi che possono essere notificati, consulta la sezione seguente.

Categorie di eventi AWS DMS e messaggi di evento

AWS DMS genera un numero significativo di eventi in categorie che puoi identificare. Ogni categoria si applica a un'istanza di replica o ai tipi di origine dell'attività di replica.

Argomenti

- [Messaggi dell'evento ReplicationInstance](#)
- [Messaggi dell'evento ReplicationTask](#)
- [Messaggi dell'evento Replication](#)

Messaggi dell'evento ReplicationInstance

La tabella che segue mostra le categorie e gli eventi possibili per il tipo di origine ReplicationInstance.

Categoria	ID evento	Descrizione
Creazione	DMS-EVENT-0067	Un'istanza di replica è in fase di creazione.
Eliminazione	DMS-EVENT-0066	L'istanza di replica è in fase di eliminazione.

Categoria	ID evento	Descrizione
Modifica della configurazione	DMS-EVENT-0012	La classe dell'istanza di replica è in fase di modifica.
Modifica della configurazione	DMS-EVENT-0018	Le dimensioni dell'archiviazione per l'istanza di replica sono in fase di aumento.
Modifica della configurazione	DMS-EVENT-0024	L'istanza di replica sta eseguendo la transizione a una configurazione Multi-AZ.
Modifica della configurazione	DMS-EVENT-0030	L'istanza di replica sta eseguendo la transizione a una configurazione Single-AZ.
Mantenance (Manutenzione)	DMS-EVENT-0026	La manutenzione offline dell'istanza database è in esecuzione. L'istanza di replica non è attualmente disponibile.
Creazione	DMS-EVENT-0005	Un'istanza di replica è stata creata.
Eliminazione	DMS-EVENT-0003	L'istanza di replica è stata eliminata.
Modifica della configurazione	DMS-EVENT-0014	La classe dell'istanza di replica è stata modificata.

Categoria	ID evento	Descrizione
Modifica della configurazione	DMS-EVENT-0017	Le dimensioni dell'archiviazione per l'istanza di replica sono state aumentate.
Modifica della configurazione	DMS-EVENT-0025	L'istanza di replica ha completato la transizione verso una configurazione Multi-AZ.
Modifica della configurazione	DMS-EVENT-0029	L'istanza di replica ha completato la transizione a una configurazione Single-AZ.
Maintenance (Manutenzione)	DMS-EVENT-0047	Il software di gestione sull'istanza di replica è stato aggiornato.
Maintenance (Manutenzione)	DMS-EVENT-0027	La manutenzione offline dell'istanza database è stata completata. L'istanza di replica è ora disponibile.
Maintenance (Manutenzione)	DMS-EVENT-0068	L'istanza di replica è in uno stato che non può essere aggiornato.
Failover	DMS-EVENT-0034	Se il failover viene richiesto con una frequenza eccessiva, viene generato questo evento al posto degli eventi di failover ordinari.
Errore	DMS-EVENT-0031	L'istanza di replica è nello stato %s.

Categoria	ID evento	Descrizione
Errore	DMS-EVENT-0036	L'istanza di replica ha generato un errore a causa di una rete non compatibile.
Errore	DMS-EVENT-0037	Il servizio non è in grado di accedere alla chiave KMS utilizzata per crittografare il volume di dati.
Errore		L'istanza di replica ha utilizzato parametri incompatibili
Failover		Timeout in attesa che uno stato sicuro avvii il failover richiesto dall'utente
Failover	DMS-EVENT-0013	Il failover è iniziato per un'istanza di replica Multi-AZ.
Failover	DMS-EVENT-0049	Il failover per un'istanza di replica Multi-AZ è stato completato.
Failover	DMS-EVENT-0050	L'attivazione Multi-AZ è stata avviata.
Failover	DMS-EVENT-0051	L'attivazione Multi-AZ è stata completata.
Modifica di stato		I log delle query generali e lente sono stati ruotati automaticamente come %s

Categoria	ID evento	Descrizione
Modifica di stato		AWS DMS non è in grado di accedere alla chiave di crittografia KMS per l'istanza di applicazione %s. Ciò è probabilmente dovuto al fatto che la chiave è disabilitata o AWS DMS non è in grado di accedervi. Se il problema persiste, l'applicazione verrà posta in uno stato inaccessibile. Per ulteriori dettagli, consulta la sezione relativa alla risoluzione dei problemi nella documentazione di AWS DMS.
Modifica di stato		AWS DMS ora può accedere alla chiave di crittografia KMS per l'istanza di applicazione %s.
Modifica di stato		Amazon DMS non è in grado di accedere alla chiave di crittografia KMS per l'istanza di applicazione %s. L'applicazione verrà posta in uno stato inaccessibile. Per ulteriori dettagli, consulta la sezione relativa alla risoluzione dei problemi nella documentazione di Amazon DMS.
Modifica di stato		Riavvio dell'app su HM come parte della creazione dell'istanza di replica
Modifica di stato		Chiusura dell'app su HM come parte dell'eliminazione dell'istanza di replica
Failover	DMS-EVENT-0015	Il failover di Multi-AZ in standby è stato completato.
Spazio in esaurimento	DMS-EVENT-0007	Lo spazio di storage disponibile per l'istanza di replica è ridotto.

Categoria	ID evento	Descrizione
Spazio in esaurimento		I nodi allocati sono esauriti: dimensiona lo storage per risolvere

Messaggi dell'evento ReplicationTask

La tabella che segue mostra le categorie e gli eventi possibili per il tipo di origine ReplicationTask.

Categoria	ID evento	Descrizione
Errore	DMS-EVENT-0078	Un'attività di replica non è riuscita.
Errore	DMS-EVENT-0082	Una chiamata per pulire i dati dell'attività non è riuscita.
Modifica dello stato	DMS-EVENT-0081	Un nuovo caricamento dei dettagli della tabella è stato richiesto.
Modifica dello stato		L'attività di replica è stata copiata.
Modifica dello stato		La copia dell'attività di replica non è riuscita.
Modifica dello stato		L'attività di replica è stata spostata.
Modifica dello stato		Lo spostamento del task di replica non è riuscito.
Modifica dello stato		La creazione dell'attività di destinazione non è riuscita.
Modifica dello stato		L'esecuzione della valutazione dell'attività di replica è iniziata.

Categoria	ID evento	Descrizione
Modifica dello stato		L'esecuzione della valutazione dell'attività di replica è stata completata correttamente.
Modifica dello stato		L'esecuzione della valutazione dell'attività di replica è terminata con errore.
Modifica di stato		L'esecuzione della valutazione dell'attività di replica è terminata con un avviso.
Modifica di stato		L'esecuzione della valutazione dell'attività di replica è terminata con un errore.
Modifica di stato		L'esecuzione della valutazione dell'attività di replica %s è stata annullata.
Modifica di stato		L'esecuzione della valutazione dell'attività di replica %s è stata eliminata.
Modifica di stato		L'esecuzione della valutazione dell'attività di replica non è riuscita a eseguire il provisioning delle risorse.
Modifica di stato		L'attività di replica non è riuscita.
Creazione		L'attività di replica è stata creata.
Modifica della configurazione		Un'attività di replica è stata modificata.
Errore		Un'attività di replica non è riuscita.

Categoria	ID evento	Descrizione
Modifica di stato	DMS-EVENT-0091	Lettura sospesa, limite di file di scambio raggiunto.
Modifica di stato	DMS-EVENT-0092	Lettura sospesa, limite di utilizzo del disco raggiunto.
Modifica di stato	DMS-EVENT-0093	Lettura sospesa, limite di utilizzo del disco raggiunto.
Modifica di stato	DMS-EVENT-0093	La lettura è ripresa.
Modifica di stato	DMS-EVENT-0069	L'attività di replica è iniziata con taskType: %s, startType: %s
Modifica di stato	DMS-EVENT-0079	L'attività di replica è stata interrotta.
Eliminazione	DMS-EVENT-0073	L'attività di replica è stata eliminata.

Messaggi dell'evento Replication

La tabella che segue mostra le categorie e gli eventi possibili per il tipo di origine Replication.

Categoria	Descrizione
Modifica dello stato	Evento di aumento della replica DMS.
Modifica dello stato	Evento di riduzione della replica DMS.
Modifica dello stato	Evento di dimensionamento della replica DMS completato.
Modifica dello stato	La replica DMS è stata creata.
Modifica dello stato	La replica DMS è in corso di inizializzazione.
Modifica dello stato	La replica DMS sta preparando le risorse per la raccolta dei metadati.

Categoria	Descrizione
Modifica dello stato	Le connessioni legate alla replica DMS sono in fase di test.
Modifica dello stato	La replica DMS sta recuperando i metadati.
Modifica dello stato	La replica DMS sta calcolando la capacità.
Modifica dello stato	La replica DMS sta allocando la propria capacità.
Modifica dello stato	La replica DMS è stata allocata.
Modifica dello stato	La replica DMS è iniziata.
Modifica dello stato	La replica DMS è in esecuzione.
Modifica dello stato	La replica DMS è in fase di arresto.
Modifica dello stato	La replica DMS è stata interrotta.
Modifica dello stato	La replica DMS è in fase di modifica.
Modifica dello stato	La replica DMS è in fase di eliminazione.
Modifica dello stato	La replica DMS riduce la propria capacità.
Modifica dello stato	Il provisioning della replica DMS è stato annullato.
Errore	La replica DMS non è riuscita.

Utilizzo degli eventi e delle notifiche Amazon SNS in AWS Database Migration Service

A partire da AWS DMS 3.4.5 e nelle versioni successive, ti consigliamo di utilizzare Amazon EventBridge per fornire notifiche quando si verifica un evento AWS DMS. Per ulteriori informazioni sull'utilizzo di eventi EventBridge con AWS DMS, consulta [Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service](#).

Spostamento delle sottoscrizioni a eventi su Amazon EventBridge

Puoi utilizzare il seguente comando AWS CLI per migrare le sottoscrizioni a eventi attivi da DMS ad Amazon EventBridge, fino a 10 alla volta.

```
update-subscriptions-to-event-bridge [--force-move | --no-force-move]
```

Per impostazione predefinita, AWS DMS migra le sottoscrizioni a eventi attivi solo quando l'istanza di replica è aggiornata a AWS DMS 3.4.5 e versioni successive. Per ignorare questo comportamento predefinito, utilizza l'opzione `--force-move`. Tuttavia, alcuni tipi di eventi potrebbero non essere disponibili con Amazon EventBridge se le istanze di replica non vengono aggiornate.

Per eseguire il comando CLI `update-subscriptions-to-event-bridge`, un utente AWS Identity and Access Management (IAM) deve disporre delle autorizzazioni di policy indicate di seguito.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "SNS:GetTopicAttributes",
        "SNS:SetTopicAttributes",
        "events:PutTargets",
        "events:EnableRule",
        "events:PutRule"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Per ulteriori informazioni sullo spostamento delle sottoscrizioni a EventBridge, consulta [UpdateSubscriptionsToEventBridge](#) nella Documentazione di riferimento delle API di AWS Database Migration Service.

Utilizzo degli eventi e delle notifiche Amazon SNS

AWS DMS 3.4.5 e versioni precedenti supportano l'utilizzo di eventi e notifiche come descritto di seguito.

AWS Database Migration Service (AWS DMS) può utilizzare Amazon Simple Notification Service (Amazon SNS) per fornire notifiche quando si verifica un evento AWS DMS, ad esempio la creazione o l'eliminazione di un'istanza di replica. Queste notifiche possono essere utilizzate in qualsiasi formato supportato da Amazon SNS per una regione AWS, ad esempio un messaggio e-mail, un SMS o una chiamata a un endpoint HTTP.

AWS DMS raggruppa gli eventi in categorie che puoi sottoscrivere per ricevere una notifica quando si verifica un evento di tale categoria. Ad esempio, con la sottoscrizione alla categoria Creazione per una determinata istanza di replica, ricevi una notifica ogni volta che si verifica un evento relativo alla creazione che interessa l'istanza di replica. Con la sottoscrizione a una categoria Modifica della configurazione per un'istanza di replica, ricevi una notifica quando la configurazione dell'istanza di replica viene modificata. Riceverai una notifica anche quando viene modificata la sottoscrizione a una notifica eventi. Per l'elenco delle categorie di eventi fornite da AWS DMS, consulta [Categorie di eventi e messaggi di evento AWS DMS per le notifiche SNS](#), di seguito.

AWS DMS invia le notifiche di eventi all'indirizzo da te fornito al momento della creazione della sottoscrizione a un evento. È consigliabile 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 risorse DMS di produzione. Puoi disattivare facilmente la notifica senza eliminare una sottoscrizione deselezionando l'opzione Abilitata nella console AWS DMS o impostando il parametro `Enabled` su `false` utilizzando l'API AWS DMS.

Note

Le notifiche di eventi AWS DMS tramite SMS sono attualmente disponibili per le risorse AWS DMS in tutte le regioni AWS in cui è supportato Amazon SNS. Per l'elenco delle regioni

AWS e dei paesi in cui Amazon SNS supporta i messaggi SMS, consulta [Regioni e paesi supportati](#).

Per ulteriori informazioni sull'utilizzo di SMS con SNS, consultare [Invio e ricezione di notifiche SMS tramite Amazon SNS](#).

Le notifiche di eventi AWS DMS sono diverse dagli eventi CloudTrail in CloudWatch o EventBridge. Le notifiche di eventi CloudTrail possono essere generate da qualsiasi invocazione API. DMS invia una notifica solo quando si verifica un evento DMS.

AWS DMS utilizza un identificativo per identificare ogni sottoscrizione. È possibile pubblicare più sottoscrizioni a eventi AWS sullo stesso argomento Amazon SNS. Quando utilizzi le notifiche di eventi, vengono applicati i costi di Amazon SNS. Per ulteriori sulla fatturazione di Amazon SNS, consulta [Prezzi di Amazon SNS](#).

Per effettuare la sottoscrizione a eventi AWS DMS con Amazon SNS, puoi usare la seguente procedura:

1. Creazione di un argomento Amazon SNS. Nell'argomento, devi specificare il tipo di notifica che desideri ricevere e a quale indirizzo o numero.
2. Crea una sottoscrizione alle notifiche di eventi AWS DMS tramite la AWS Management Console, la AWS CLI o l'API AWS DMS.
3. AWS DMS invia un SMS o un'e-mail di approvazione all'indirizzo da te specificato nella sottoscrizione. Per confermare la sottoscrizione, fai clic sul collegamento contenuto nel messaggio e-mail o SMS di approvazione.
4. Una volta confermata la sottoscrizione, lo stato della sottoscrizione viene aggiornato nella sezione Sottoscrizioni a eventi della console AWS DMS.
5. Inizierai quindi a ricevere le notifiche eventi.

Per un elenco delle categorie e degli eventi che possono essere notificati, consulta la sezione seguente. Per ulteriori dettagli sulla sottoscrizione a AWS DMS e sull'utilizzo delle relative sottoscrizioni a eventi, consulta [Sottoscrizione alla notifica di eventi AWS DMS tramite SNS](#).

Categorie di eventi e messaggi di evento AWS DMS per le notifiche SNS

Important

A partire da AWS DMS 3.4.5 e nelle versioni successive, ti consigliamo di utilizzare Amazon EventBridge per fornire notifiche quando si verifica un evento AWS DMS. Per ulteriori informazioni sull'utilizzo di eventi EventBridge con AWS DMS, consulta [Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service](#).

AWS DMS genera un numero significativo di eventi in categorie a cui puoi effettuare la sottoscrizione tramite la console AWS DMS o l'API AWS DMS. Ogni categoria si applica a un tipo di origine. Attualmente AWS DMS supporta i tipi di origine delle attività e delle istanze di replica.

La tabella che segue mostra le categorie e gli eventi possibili per il tipo di origine delle istanze di replica.

Categoria	ID evento DMS	Descrizione
Modifica della configurazione	DMS-EVENT-0012	La classe dell'istanza di replica è in fase di modifica.
Modifica della configurazione	DMS-EVENT-0014	La classe dell'istanza di replica è stata modificata.
Modifica della configurazione	DMS-EVENT-0018	Le dimensioni dell'archiviazione per l'istanza di replica sono in fase di aumento.
Modifica della configurazione	DMS-EVENT-0017	Le dimensioni dell'archiviazione per l'istanza di replica sono state aumentate.
Modifica della configurazione	DMS-EVENT-0024	L'istanza di replica sta eseguendo la transizione a una configurazione Multi-AZ.
Modifica della configurazione	DMS-EVENT-0025	L'istanza di replica ha completato la transizione a una configurazione Multi-AZ.

Categoria	ID evento DMS	Descrizione
Modifica della configurazione	DMS-EVENT-0030	L'istanza di replica sta eseguendo la transizione a una configurazione Single-AZ.
Modifica della configurazione	DMS-EVENT-0029	L'istanza di replica ha completato la transizione a una configurazione Single-AZ.
Creazione	DMS-EVENT-0067	Un'istanza di replica è in fase di creazione.
Creazione	DMS-EVENT-0005	L'istanza di replica è stata creata.
Eliminazione	DMS-EVENT-0066	L'istanza di replica è in fase di eliminazione.
Eliminazione	DMS-EVENT-0003	L'istanza di replica è stata eliminata.
Maintenance (Manutenzione)	DMS-EVENT-0047	Il software di gestione sull'istanza di replica è stato aggiornato.
Maintenance (Manutenzione)	DMS-EVENT-0026	La manutenzione offline dell'istanza database è in esecuzione. L'istanza di replica non è attualmente disponibile.
Maintenance (Manutenzione)	DMS-EVENT-0027	La manutenzione offline dell'istanza database è stata completata. L'istanza di replica è ora disponibile.
Maintenance (Manutenzione)	DMS-EVENT-0068	Un'istanza di replica è in uno stato che non può essere aggiornato.
Spazio in esaurimento	DMS-EVENT-0007	L'istanza di replica ha utilizzato oltre il 90% dello spazio di archiviazione allocato. Puoi monitorare lo spazio di archiviazione per un'istanza di replica usando il parametro Spazio di archiviazione libero.
Failover	DMS-EVENT-0013	Il failover è iniziato per un'istanza di replica Multi-AZ.
Failover	DMS-EVENT-0049	Il failover è stato completo per un'istanza di replica Multi-AZ.

Categoria	ID evento DMS	Descrizione
Failover	DMS-EVENT-0015	Il failover di Multi-AZ in standby è stato completato.
Failover	DMS-EVENT-0050	L'attivazione Multi-AZ è stata avviata.
Failover	DMS-EVENT-0051	L'attivazione Multi-AZ è stata completata.
Failover	DMS-EVENT-0034	Se il failover viene richiesto con una frequenza eccessiva, viene generato questo evento al posto degli eventi di failover ordinari.
Errore	DMS-EVENT-0031	L'istanza di replica ha generato un errore di archiviazione.
Errore	DMS-EVENT-0036	L'istanza di replica ha generato un errore a causa di una rete non compatibile.
Errore	DMS-EVENT-0037	Il servizio non può accedere alla chiave AWS KMS utilizzata per crittografare il volume di dati.

La tabella che segue mostra le categorie e gli eventi possibili per il tipo di origine delle attività di replica.

Categoria	ID evento DMS	Descrizione
Modifica dello stato	DMS-EVENT-0069	L'attività di replica è stata avviata.
Modifica dello stato	DMS-EVENT-0081	Un nuovo caricamento dei dettagli della tabella è stato richiesto.
Modifica dello stato	DMS-EVENT-0079	L'attività di replica è stata arrestata.
Modifica dello stato	DMS-EVENT-0091	Lettura sospesa, limite di file di scambio raggiunto.

Categoria	ID evento DMS	Descrizione
Modifica dello stato	DMS-EVENT-0092	Lettura sospesa, limite di utilizzo del disco raggiunto.
Modifica dello stato	DMS-EVENT-0093	La lettura è ripresa.
Errore	DMS-EVENT-0078	L'attività di replica non è riuscita.
Errore	DMS-EVENT-0082	Una chiamata per eliminare l'attività non è riuscita a pulire i dati dell'attività.
Modifica della configurazione	DMS-EVENT-0080	L'attività di replica è stata modificata.
Eliminazione	DMS-EVENT-0073	L'attività di replica è stata eliminata.
Creazione	DMS-EVENT-0074	L'attività di replica è stata creata.

L'esempio seguente mostra la sottoscrizione a un evento AWS DMS con la categoria Cambio stato.

```
Resources:
  DMSEvent:
    Type: AWS::DMS::EventSubscription
    Properties:
      Enabled: true
      EventCategories: State Change
      SnsTopicArn: arn:aws:sns:us-east-1:123456789:testSNS
      SourceIds: []
      SourceType: replication-task
```

Sottoscrizione alla notifica di eventi AWS DMS tramite SNS

Important

A partire da AWS DMS 3.4.5 e nelle versioni successive, ti consigliamo di utilizzare Amazon EventBridge per fornire notifiche quando si verifica un evento AWS DMS. Per ulteriori

informazioni sull'utilizzo di eventi EventBridge con AWS DMS, consulta [Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service](#).

Puoi creare una sottoscrizione alle notifiche eventi AWS DMS per ricevere una notifica quando si verifica un evento AWS DMS. Il modo più semplice di creare una sottoscrizione è utilizzare la console AWS DMS. In una sottoscrizione alle notifiche, sei tu a scegliere come e dove inviare le notifiche. Puoi specificare il tipo di origine per cui vuoi ricevere le notifiche. Attualmente AWS DMS supporta i tipi di origine delle istanze di replica e delle attività di replica. A seconda del tipo di origine selezionato, scegli le categorie di eventi e identifica le origini per cui ricevere le notifiche di eventi.

Utilizzo di AWS Management Console

Important

A partire da AWS DMS 3.4.5 e nelle versioni successive, ti consigliamo di utilizzare Amazon EventBridge per fornire notifiche quando si verifica un evento AWS DMS. Per ulteriori informazioni sull'utilizzo di eventi EventBridge con AWS DMS, consulta [Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service](#).

Per eseguire la sottoscrizione alla notifica di eventi AWS DMS con Amazon SNS mediante la console

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS.

2. Nel pannello di navigazione selezionare Event subscriptions (Sottoscrizioni di eventi).
3. Nella pagina Sottoscrizioni a eventi seleziona Crea sottoscrizione a eventi.
4. Nella pagina Crea sottoscrizione a eventi esegui queste operazioni:
 - a. Sotto Dettagli, per Nome immetti un nome per la sottoscrizione alla notifica di eventi.
 - b. Scegli Abilitato per abilitare la sottoscrizione. Per creare una sottoscrizione ma non ricevere subito le notifiche, non scegliere Abilitato.
 - c. In Destinazione scegli Argomenti esistenti, Crea nuovo argomento e-mail o Crea nuovo argomento SMS per inviare notifiche. Assicurati di disporre un argomento Amazon SNS

esistente a cui inviare avvisi o di creare l'argomento. Se scegli di creare un argomento, puoi inserire l'indirizzo e-mail a cui verranno inviate le notifiche.

- d. In Origine eventi, per Tipo di origine scegli un tipo di origine. Le uniche opzioni sono replication-instance e replication-task.
- e. A seconda del tipo di origine selezionato, scegli le categorie di eventi e le origini per cui ricevere le notifiche eventi.

Create event subscription

Details

Name

The name for your event subscription

 Enabled

Target

Send notification to

- Existing topics
- Create new email topic
- Create new SMS topic

Topic name**With these recipients**

Email addresses or phone numbers of SMS enabled devices to send the notifications to

Event source

Source type

Source Type of resource this subscription will consume events from

Event categories

- All event categories
- Select specific event categories

Replication instance

- All instances
- Select specific instances

- f. Scegli Crea sottoscrizione a eventi.

La console AWS DMS indica che è in corso la creazione della sottoscrizione.

Note

Puoi anche creare sottoscrizioni alle notifiche di eventi Amazon SNS utilizzando l'API AWS DMS e la CLI. Per ulteriori informazioni, consulta [CreateEventSubscription](#) nella Documentazione di riferimento delle API di AWS DMS e [create-event-subscription](#) nella Documentazione di riferimento della CLI di AWS DMS.

Convalida della policy di accesso dell'argomento SNS

La tua policy di accesso SNS richiede autorizzazioni che consentano ad AWS DMS di pubblicare eventi sull'argomento SNS. Puoi convalidare e aggiornare la tua policy di accesso come descritto nelle seguenti procedure.

Per convalidare la policy di accesso

1. Aprire la console Amazon SNS.
2. Dal pannello di navigazione scegli Argomenti e seleziona l'argomento per cui desideri ricevere le notifiche DMS.
3. Seleziona la scheda Policy di accesso.

Puoi aggiornare la tua policy se la policy di accesso SNS non consente ad AWS DMS di pubblicare eventi sull'argomento SNS.

Per aggiornare la policy di accesso

1. Nella sezione Dettagli della pagina dell'argomento, scegli Modifica.
2. Espandi la sezione Policy di accesso e collega la seguente policy nell'editor JSON.

```
{
  "Sid": "dms-allow-publish",
  "Effect": "Allow",
  "Principal": {
    "Service": "dms.amazonaws.com"
```

```
  },  
  "Action": "sns:Publish",  
  "Resource": "your-SNS-topic-ARN"  
}
```

Ti consigliamo di limitare ulteriormente l'accesso all'argomento SNS specificando la condizione `aws:SourceArn`, ovvero l'ARN DMS EventSubscription che pubblica gli eventi sull'argomento.

```
...  
"Resource": "your-SNS-topic-ARN"  
"Condition": {  
  "StringEquals": {  
    "aws:SourceArn": "arn:partition:dms:your-AWS-region:your-AWS-account-ID:es:your-dms-es-arn or *"  
  }  
}
```

3. Seleziona Salva modifiche.

Convalida dei dati in AWS DMS

Argomenti

- [Statistiche delle attività di replica](#)
- [Statistiche dell'attività di replica con Amazon CloudWatch](#)
- [Nuova convalida delle tabelle durante un'attività](#)
- [Utilizzo dell'editor JSON per modificare le regole di convalida](#)
- [Attività di sola convalida](#)
- [Risoluzione dei problemi](#)
- [Prestazioni di convalida di Redshift](#)
- [Limitazioni](#)
- [Convalida dei dati di destinazione Amazon S3](#)

AWS DMS fornisce supporto per la convalida dei dati per garantire che i dati siano stati migrati accuratamente dall'origine alla destinazione. Se abilitata, la convalida inizia immediatamente dopo il pieno carico di una tabella. La convalida confronta le modifiche incrementalmente di un'attività abilitata CDC man mano che si verificano.

Durante la convalida dei dati, AWS DMS confronta ogni riga nell'origine con la riga corrispondente nella destinazione e verifica che tali righe contengano gli stessi dati senza mancate corrispondente. A tale scopo, AWS DMS esegue query appropriate per recuperare i dati. Tieni presente che queste query utilizzano risorse aggiuntive all'origine e alla destinazione, nonché risorse di rete aggiuntive.

Per un'attività di sola CDC con convalida abilitata, tutti i dati preesistenti in una tabella vengono convalidati prima di iniziare la convalida di nuovi dati.

La convalida dei dati funziona con i seguenti database di origine se AWS DMS li supporta come endpoint di origine:

- Oracle
- Database compatibile con PostgreSQL (PostgreSQL, Aurora PostgreSQL o Aurora serverless per PostgreSQL)
- Database compatibile con MySQL (MySQL, MariaDB, Aurora MySQL o Aurora serverless per MySQL)
- Microsoft SQL Server

- IBM Db2 LUW

La convalida dei dati funziona con i seguenti database di destinazione se AWS DMS li supporta come endpoint di destinazione:

- Oracle
- Database compatibile con PostgreSQL (PostgreSQL, Aurora PostgreSQL o Aurora serverless per PostgreSQL)
- Database compatibile con MySQL (MySQL, MariaDB, Aurora MySQL o Aurora serverless per MySQL)
- Microsoft SQL Server
- IBM Db2 LUW
- Amazon Redshift
- Amazon S3. Per informazioni sulla convalida dei dati di destinazione di Amazon S3, consulta [Convalida dei dati di destinazione Amazon S3](#).

Per ulteriori informazioni sugli endpoint supportati, consulta [Utilizzo degli endpoint AWS DMS](#).

La convalida dei dati richiede tempo aggiuntivo rispetto alla quantità necessaria per la migrazione. Il tempo aggiuntivo necessario dipende dalla quantità di dati migrata.

Per ulteriori informazioni su queste impostazioni, consultare [Impostazioni delle attività di convalida dei dati](#).

Per un esempio di impostazioni dell'attività `ValidationSettings` in un file JSON, consulta [Esempio di impostazioni delle attività](#).

Statistiche delle attività di replica

Quando è abilitata la convalida dei dati, AWS DMS fornisce le seguenti statistiche a livello di tabella:

- `ValidationState`: lo stato di convalida della tabella. Il parametro può avere i seguenti valori:
 - Non abilitato: la convalida non è abilitata per la tabella nell'attività di migrazione.
 - Record in sospenso: alcuni record della tabella sono in attesa di convalida.
 - Record non corrispondenti: alcuni record della tabella non corrispondono tra l'origine e la destinazione. Una mancata corrispondenza può verificarsi per una serie di motivi. Per ulteriori

informazioni, consulta la tabella `awsdms_control.awsdms_validation_failures_v1` sull'endpoint di destinazione.

- Record sospesi: alcuni record della tabella non possono essere convalidati.
- Nessuna chiave primaria: la tabella non può essere convalidata perché non ha una chiave primaria.
- Errore della tabella: la tabella non è stata convalidata perché si trova in uno stato di errore e alcuni dati non sono stati migrati.
- Convalidata: tutte le righe della tabella sono state convalidate. Se la tabella viene aggiornata, lo stato può variare da `Validated` (Convalidata).
- Errore: la tabella non può essere convalidata a causa di un errore imprevisto.
- Convalida in sospeso: la tabella è in attesa di convalida.
- Preparazione della tabella: la preparazione della tabella abilitata nell'attività di migrazione per la convalida.
- Riconvalida in sospeso: tutte le righe della tabella sono in attesa di convalida dopo l'aggiornamento della tabella.
- `ValidationPending`: il numero di record che sono stati migrati nella destinazione, ma che non sono ancora stati convalidati.
- `ValidationSuspended`: il numero di record che AWS DMS non è in grado di confrontare. Ad esempio, se un record all'origine viene costantemente aggiornato, AWS DMS non può confrontare l'origine e la destinazione.
- `ValidationFailed`: il numero di record che non hanno superato la fase di convalida dei dati.

Per un esempio di impostazioni dell'attività `ValidationSettings` in un file JSON, consulta [Esempio di impostazioni delle attività](#).

Puoi visualizzare le informazioni sulla convalida dei dati tramite la console, la AWS CLI o l'API AWS DMS.

- Nella console, puoi scegliere di convalidare un'attività quando la crei o la modifichi. Per visualizzare il report di convalida dei dati utilizzando la console, scegli l'attività nella pagina `Tasks` (Attività) e scegli la scheda `Table statistics` (Statistiche tabella) nella sezione dei dettagli.
- Per avviare la convalida dei dati tramite la CLI, imposta il parametro `EnableValidation` su `true` durante la creazione o la modifica di un'attività. Nell'esempio seguente viene creata un'attività e abilitata la convalida dei dati.

```

create-replication-task
--replication-task-settings '{"ValidationSettings":{"EnableValidation":true}}'
--replication-instance-arn arn:aws:dms:us-east-1:5731014:
    rep:36KWVMB7Q
--source-endpoint-arn arn:aws:dms:us-east-1:5731014:
    endpoint:CSZAEFQURFYMM
--target-endpoint-arn arn:aws:dms:us-east-1:5731014:
    endpoint:CGPP7MF6WT4JQ
--migration-type full-load-and-cdc
--table-mappings '{"rules": [{"rule-type": "selection", "rule-id": "1",
    "rule-name": "1", "object-locator": {"schema-name": "data_types", "table-name":
"%"},
    "rule-action": "include"}]}'

```

Utilizza il comando `describe-table-statistics` per ricevere il report di convalida dei dati in formato JSON. Il comando seguente mostra il report di convalida dei dati.

```

aws dms describe-table-statistics --replication-task-arn arn:aws:dms:us-
east-1:5731014:
rep:36KWVMB7Q

```

Il report dovrebbe essere simile al seguente.

```

{
  "ReplicationTaskArn": "arn:aws:dms:us-west-2:5731014:task:VFPFTYKK2RYSI",
  "TableStatistics": [
    {
      "ValidationPendingRecords": 2,
      "Inserts": 25,
      "ValidationState": "Pending records",
      "ValidationSuspendedRecords": 0,
      "LastUpdateTime": 1510181065.349,
      "FullLoadErrorRows": 0,
      "FullLoadCondtnlChkFailedRows": 0,
      "Ddls": 0,
      "TableName": "t_binary",
      "ValidationFailedRecords": 0,
      "Updates": 0,
      "FullLoadRows": 10,
      "TableState": "Table completed",
      "SchemaName": "d_types_s_sqlserver",

```

```
    "Deletes": 0
  }
}
```

- Tramite l'API AWS DMS, crea un'attività utilizzando l'azione `CreateReplicationTask` e imposta il parametro `EnableValidation` su `true` per convalidare i dati migrati dall'attività. Utilizza l'operazione `DescribeTableStatistics` per ricevere il report della convalida dei dati in formato JSON.

Statistiche dell'attività di replica con Amazon CloudWatch

Quando Amazon CloudWatch è abilitato, AWS DMS fornisce le seguenti statistiche dell'attività di replica:

- `ValidationSucceededRecordCount`: numero di righe convalidate da AWS DMS, al minuto.
- `ValidationAttemptedRecordCount`: numero di righe in cui è stata tentata la convalida, al minuto.
- `ValidationFailedOverallCount`: numero di righe per cui la convalida non è riuscita.
- `ValidationSuspendedOverallCount`: numero di righe per cui la convalida è stata sospesa.
- `ValidationPendingOverallCount`: numero di righe per cui la convalida è ancora in sospeso.
- `ValidationBulkQuerySourceLatency`: AWS DMS può eseguire la convalida dei dati in blocco, specialmente in determinati scenari durante una replica continua o di pieno carico quando ci sono molte modifiche. Questo parametro indica la latenza necessaria per leggere una serie di dati in blocco dall'endpoint di origine.
- `ValidationBulkQueryTargetLatency`: AWS DMS può eseguire la convalida dei dati in blocco, specialmente in determinati scenari durante una replica continua o di pieno carico quando ci sono molte modifiche. Questo parametro indica la latenza necessaria per leggere una serie di dati in blocco sull'endpoint di destinazione.
- `ValidationItemQuerySourceLatency`: durante la replica continua, la convalida dei dati può identificare le modifiche in corso e convalidarle. Questo parametro indica la latenza nella lettura di tali modifiche dall'origine. La convalida è in grado di eseguire più query rispetto al necessario, in base al numero di modifiche, in caso di errori durante la convalida.
- `ValidationItemQueryTargetLatency`: durante la replica continua, la convalida dei dati può identificare le modifiche in corso e convalidarle riga per riga. Questo parametro offre la latenza nella lettura di tali modifiche dalla destinazione. La convalida è in grado di eseguire più query rispetto al necessario, in base al numero di modifiche, in caso di errori durante la convalida.

Per raccogliere informazioni sulla convalida dei dati dalle statistiche abilitate CloudWatch, seleziona **Abilita File di log CloudWatch** quando crei o modifichi un'attività utilizzando la console. Quindi, per visualizzare le informazioni sulla convalida dei dati e garantire che i dati siano stati migrati accuratamente dall'origine alla destinazione, procedi come segue.

1. Scegli l'attività nella pagina **Attività di migrazione del database**.
2. Scegli la scheda **Parametri CloudWatch**.
3. Seleziona **Convalida** dal menu a discesa.

Nuova convalida delle tabelle durante un'attività

Durante l'esecuzione di un'attività, puoi richiedere a AWS DMS di eseguire la convalida dei dati.

AWS Management Console

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.

Se hai eseguito l'accesso come utente AWS Identity and Access Management (IAM), verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per le autorizzazioni necessarie, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Scegliere **Tasks (Attività)** nel riquadro di navigazione.
3. Scegli l'attività in esecuzione che ha la tabella che desideri convalidare nuovamente.
4. Selezionare la scheda **Table Statistics (Statistiche tabella)**.
5. Scegliere la tabella da riconvalidare (è possibile scegliere fino a 10 tabelle contemporaneamente). Se l'attività non è più in esecuzione, non è possibile convalidare nuovamente la tabella.
6. Scegli **Revalidate (Convalida di nuovo)**.

Utilizzo dell'editor JSON per modificare le regole di convalida

Per aggiungere una regola di convalida a un'attività utilizzando l'editor JSON dalla console AWS DMS, procedi come segue:

1. Seleziona **Attività di migrazione del database**.

2. Seleziona l'attività dall'elenco delle attività di migrazione.
3. Se l'attività è in esecuzione, seleziona Interrompi dal menu a discesa Operazioni.
4. Una volta interrotta l'attività, seleziona Modifica dal menu a discesa Operazioni per modificarla.
5. Nella sezione Mappature delle tabelle seleziona Editor JSON e aggiungi la regola di convalida alle mappature delle tabelle.

Ad esempio, puoi aggiungere la regola di convalida seguente per eseguire una funzione di sostituzione sull'origine. In questo caso, se la regola di convalida rileva un byte nullo, lo convalida come spazio.

```
{
  "rule-type": "validation",
  "rule-id": "1",
  "rule-name": "1",
  "rule-target": "column",
  "object-locator": {
    "schema-name": "Test-Schema",
    "table-name": "Test-Table",
    "column-name": "Test-Column"
  },
  "rule-action": "override-validation-function",
  "source-function": "REPLACE(${column-name}, chr(0), chr(32))",
  "target-function": "${column-name}"
}
```

Attività di sola convalida

È possibile creare attività di sola convalida per visualizzare in anteprima e convalidare i dati senza eseguire alcuna migrazione o replica dei dati. Per creare un'attività di sola convalida, configura le impostazioni `EnableValidation` e `ValidationOnly` su `true`. Quando si abilita `ValidationOnly`, si applicano requisiti aggiuntivi. Per ulteriori informazioni, consulta [Impostazioni delle attività di convalida dei dati](#).

Per una migrazione di tipo solo pieno carico, l'attività di sola convalida viene completata molto più rapidamente dell'equivalente CDC quando vengono restituiti molti errori. Tuttavia, le modifiche all'endpoint di origine o di destinazione vengono segnalate come errori per la modalità di pieno carico, un possibile svantaggio.

Un'attività di sola convalida CDC ritarda la convalida in base alla latenza media e riprova gli errori più volte prima di segnalarli. Se la maggior parte dei confronti dei dati genera errori, un'operazione di sola convalida per la modalità CDC è molto lenta, il che rappresenta un potenziale svantaggio.

Un'attività di sola convalida deve essere impostata nella stessa direzione dell'attività di replica, in particolare per CDC. Questo perché l'attività di sola convalida CDC rileva quali righe sono state modificate e devono essere riconvalidate in base al log delle modifiche sull'origine. Se la destinazione è specificata come origine, riconosce solo le modifiche inviate alla destinazione dal DMS e non è garantito che rilevi gli errori di replica.

Sola convalida pieno carico

A partire da AWS DMS 3.4.6 e versioni successive, un'attività di sola convalida pieno carico confronta rapidamente tutte le righe delle tabelle di origine e di destinazione in un unico passaggio, segnala immediatamente eventuali errori e quindi si arresta. La convalida non viene mai sospesa a causa di errori in questa modalità ed è ottimizzata per la velocità. Tuttavia, le modifiche all'endpoint di origine o di destinazione vengono segnalate come errori.

Note

A partire da AWS DMS 3.4.6 e versioni successive, questo comportamento di convalida si applica anche alle attività di migrazione di pieno carico con la convalida abilitata.

Sola convalida CDC

Un'attività di sola convalida CDC convalida tutte le righe esistenti tra le tabelle di origine e di destinazione per un nuovo avvio. Inoltre, un'attività di sola convalida CDC viene eseguita continuamente, riconvalida le modifiche della replica continua, limita il numero di errori segnalati per ogni passaggio e riprova le righe non corrispondenti prima di restituire l'esito negativo. È ottimizzata per prevenire falsi positivi.

La convalida di una tabella (o dell'intera attività) viene sospesa in caso di violazione delle soglie `FailureMaxCount` o `TableFailureMaxCount`. Ciò vale anche per un'attività di migrazione CDC o pieno carico e CDC con la convalida abilitata. Inoltre, un'attività di CDC con la convalida abilitata ritarda la riconvalida per ogni riga modificata in base alla latenza media di origine e di destinazione.

Tuttavia un'attività di sola convalida CDC non migra i dati e non ha alcuna latenza. Per impostazione predefinita, imposta `ValidationQueryCdcDelaySeconds` su 180. Inoltre, puoi aumentare la quantità per tenere conto degli ambienti ad alta latenza e prevenire i falsi positivi.

Casi d'uso di sola convalida

I casi d'uso per suddividere la parte di convalida dei dati di un'attività di migrazione o replica in un'attività di sola convalida separata includono, a titolo esemplificativo ma non esaustivo, i seguenti:

- Controlla esattamente quando avviene la convalida: le query di convalida aggiungono un carico agli endpoint di origine e di destinazione. Quindi, può essere utile migrare o replicare prima i dati in un'attività e poi convalidare i risultati in un'altra attività.
- Riduci il carico sull'istanza di replica: suddividere la convalida dei dati per eseguirla sulla propria istanza può essere vantaggioso.
- Ottieni rapidamente quante righe non corrispondono in un determinato momento: ad esempio appena prima o durante l'interruzione della produzione di una finestra di manutenzione per un endpoint di destinazione, puoi creare un'attività di sola convalida pieno carico per ottenere una risposta alla tua domanda.
- Quando si prevedono errori di convalida per un'attività di migrazione con un componente CDC, ad esempio, se si esegue la migrazione di Oracle `varchar2` a PostgreSQL `jsonb`, la convalida CDC continua a riprovare queste righe non riuscite e limita il numero di errori segnalati ogni volta. Tuttavia, puoi creare un'attività di sola convalida pieno carico e ottenere una risposta più rapida.
- Hai sviluppato uno script/utilità per il ripristino dei dati che legge la tabella degli errori di convalida: consulta anche [Risoluzione dei problemi](#). Un'attività di sola convalida pieno carico segnala rapidamente gli errori su cui lo script di ripristino dei dati può intervenire.

Per un esempio di impostazioni dell'attività `ValidationSettings` in un file JSON, consulta [Esempio di impostazioni delle attività](#).

Risoluzione dei problemi

Durante la convalida, AWS DMS crea una nuova tabella nell'endpoint di destinazione: `awsdms_control.awsdms_validation_failures_v1`. Se uno dei record acquisisce lo stato `ValidationSuspended` o `ValidationFailed`, AWS DMS scrive informazioni di diagnostica in `awsdms_control.awsdms_validation_failures_v1`. Puoi eseguire query sulla tabella per risolvere gli errori di convalida.

Per informazioni sulla modifica dello schema predefinito in cui viene creata la tabella sulla destinazione, consulta [Impostazioni delle attività delle tabelle di controllo](#).

In seguito è riportata una descrizione della tabella
awsdms_control.awsdms_validation_failures_v1:

Nome colonna	Tipo di dati	Description
TASK_NAME	VARCHAR(128) NOT NULL	Identificatore di attività AWS DMS.
TABLE_OWNER	VARCHAR(128) NOT NULL	Schema (proprietario) della tabella.
TABLE_NAME	VARCHAR(128) NOT NULL	Nome tabella.
FAILURE_TIME	DATETIME(3) NOT NULL	Ora in cui si è verificato l'errore.
KEY_TYPE	VARCHAR(128) NOT NULL	Riservato per uso futuro (il valore è sempre "Row")
KEY	TEXT NOT NULL	Questa è la chiave primaria per il tipo di record row.
FAILURE_TYPE	VARCHAR(128) NOT NULL	Gravità dell'errore di convalida. Può essere RECORD_DIFF , MISSING_SOURCE o MISSING_TARGET .
DETAILS	VARCHAR(8000) NOT NULL	Stringa in formato JSON di tutti i valori delle colonne di origine/destinazione che non corrispondono alla chiave specificata.

La seguente query mostrerà tutti gli errori relativi a un'attività eseguendo query sulla tabella awsdms_control.awsdms_validation_failures_v1. Il nome dell'attività deve essere l'ID risorsa esterna dell'attività. L'ID risorsa esterna dell'attività è l'ultimo valore nell'ARN dell'attività. Ad esempio, per un'attività con un valore ARN di arn:aws:dms:us-west-2:5599:task:VFPFKH4FJR3FTYKK2RYSI, l'ID risorsa esterna dell'attività è VFPFKH4FJR3FTYKK2RYSI.


```
select * from awsdms_validation_failures_v1 where TASK_NAME = 'VFPFKH4FJR3FTYKK2RYSI'
```

TASK_NAME	VFPFKH4FJR3FTYKK2RYSI
TABLE_OWNER	DB2PERF
TABLE_NAME	PERFTEST
FAILURE_TIME	2020-06-11 21:58:44
KEY_TYPE	Row
KEY	{"key": ["3451491"]}
FAILURE_TYPE	RECORD_DIFF
DETAILS	[["MYREAL": '+1.10106036e-01'], {"MYREAL": '+1.10106044e-01'}],]

Puoi esaminare il campo DETAILS per determinare quali colonne non corrispondono. Dopo aver ottenuto la chiave primaria del record non riuscito, puoi eseguire query sugli endpoint di origine e di destinazione per visualizzare quale parte del record non corrisponde.

Prestazioni di convalida di Redshift

Amazon Redshift si differenzia dai database relazionali in diversi modi, tra cui l'archiviazione a colonne, la MPP, la compressione dei dati e altri fattori. Queste differenze conferiscono a Redshift un profilo prestazionale diverso rispetto ai database relazionali.

Durante la fase di replica di pieno carico, la convalida utilizza le query di intervallo, con la dimensione dei dati determinata dall'impostazione `PartitionSize`. Queste query basate su intervalli selezionano tutti i record dalla tabella di origine.

Per la replica continua, le query passano dal recupero dei record basato su intervalli a quello basato su singoli record. Il tipo di query viene determinato dinamicamente in base a più fattori, ad esempio:

- Volume di query
- Tipi di query DML sulla tabella di origine
- Latenza delle attività
- Numero totale di record
- Impostazioni di convalida come `PartitionSize`

A causa delle query di convalida, potresti riscontrare un carico aggiuntivo sul cluster Amazon Redshift. Dal momento che i fattori sopra indicati variano a seconda dei casi d'uso, è necessario esaminare le prestazioni delle query di convalida e ottimizzare il cluster e la tabella di conseguenza. Alcune opzioni per mitigare i problemi di prestazioni sono:

- Riduci le impostazioni `PartitionSize` e `ThreadCount` per diminuire il carico di lavoro durante la convalida del pieno carico. Tieni presente che in tal modo si rallenta la convalida dei dati.
- Sebbene Redshift non applichi le chiavi primarie, AWS DMS usa le chiavi primarie per identificare in modo univoco i record sulla destinazione per la convalida dei dati. Se possibile, imposta la chiave primaria in modo che rispecchi la chiave di ordinamento affinché le query di convalida del pieno carico vengano eseguite più rapidamente.

Limitazioni

- La convalida dei dati richiede che la tabella disponga di una chiave primaria o di un indice univoco.
 - Le colonne di chiave primaria non possono essere di tipo CLOB, BLOB o BYTE.
 - Per le colonne chiave primaria di tipo VARCHAR o CHAR, la lunghezza deve essere inferiore a 1024. È necessario specificare la lunghezza nel tipo di dati. Non è possibile utilizzare tipi di dati illimitati come chiave primaria per la convalida dei dati.
 - Una chiave Oracle creata con la clausola `NOVALIDATE` non è considerata una chiave primaria o un indice univoco.
 - Per una tabella Oracle senza chiave primaria e con solo una chiave univoca, le colonne con il vincolo univoco devono avere anche un vincolo `NOT NULL`.
- La convalida dei valori NULL PK/UK non è supportata.
- Se il confronto della colonna chiave primaria nell'istanza PostgreSQL di destinazione non è impostato su "C", l'ordine della chiave primaria è diverso rispetto a quello in Oracle. Se l'ordine è diverso tra PostgreSQL e Oracle, la convalida dei dati sui record ha esito negativo.
- La convalida dei dati genera ulteriori query sui database di origine e di destinazione. Devi accertarti che entrambi i database dispongano di risorse sufficienti per gestire il carico aggiuntivo. In particolare per le destinazioni Redshift. Per ulteriori informazioni, consulta la sezione seguente: [Prestazioni di convalida di Redshift](#).
- La convalida dei dati non è supportata durante il consolidamento di diversi database in uno solo.
- Per un endpoint di origine o di destinazione Oracle, AWS DMS usa `DBMS_CRYPTO` per convalidare i LOB. Se l'endpoint Oracle utilizza i LOB, devi concedere le autorizzazioni di

esecuzione su `dbms_crypto` all'account utente utilizzato per accedere all'endpoint Oracle. Puoi effettuare questa operazione eseguendo l'istruzione riportata di seguito:

```
grant execute on sys.dbms_crypto to dms_endpoint_user;
```

- Se il database di destinazione viene modificato al di fuori di AWS DMS durante la convalida, le discrepanze potrebbero non essere segnalate con precisione. Questo risultato può verificarsi se una delle applicazioni scrive dati sulla tabella di destinazione, mentre AWS DMS esegue la convalida sulla stessa tabella.
- Se una o più righe sono state modificate in modo continuo durante la convalida, AWS DMS non è in grado di convalidare tali righe.
- Se rileva più di 10.000 record non riusciti o sospesi, AWS DMS interrompe la convalida. Prima di procedere, risolvi eventuali problemi sottostanti dei dati.
- AWS DMS non supporta la convalida dei dati delle viste.
- AWS DMS non supporta la convalida dei dati quando vengono utilizzate le impostazioni delle attività di sostituzione dei caratteri.
- AWS DMS non supporta la convalida del tipo Oracle LONG.
- AWS DMS non supporta la convalida del tipo Oracle Spatial durante la migrazione eterogenea.

Per le limitazioni relative all'utilizzo della convalida della destinazione S3, consulta [Limitazioni all'utilizzo della convalida della destinazione S3](#).

Convalida dei dati di destinazione Amazon S3

AWS DMS supporta la convalida dei dati replicati nelle destinazioni Amazon S3. Poiché AWS DMS archivia i dati replicati come file flat in Amazon S3, utilizziamo le query [Amazon Athena](#) CREATE TABLE AS SELECT (CTAS) per convalidare i dati.

Le query sui dati archiviati in Amazon S3 richiedono molte risorse a livello di programmazione. Pertanto, AWS DMS esegue la convalida dei dati Amazon S3 durante l'acquisizione dei dati di modifica (CDC) solo una volta al giorno, a mezzanotte (00:00) UTC. Ogni convalida giornaliera eseguita da AWS DMS viene denominata convalida di intervallo. Durante una convalida di intervallo, AWS DMS convalida tutti i record di modifica che sono stati migrati nel bucket Amazon S3 di destinazione nelle 24 ore precedenti. Per ulteriori informazioni sulle limitazioni per la convalida di intervallo, consulta [Limitazioni all'utilizzo della convalida della destinazione S3](#).

La convalida della destinazione Amazon S3 utilizza Amazon Athena, pertanto sono previsti costi aggiuntivi. Per ulteriori informazioni, consulta [Prezzi di Amazon Athena](#).

Note

La convalida della destinazione S3 richiede AWS DMS 3.5.0 o versioni successive.

Argomenti

- [Prerequisiti per la convalida della destinazione S3](#)
- [Autorizzazioni per l'utilizzo della convalida della destinazione S3](#)
- [Limitazioni all'utilizzo della convalida della destinazione S3](#)
- [Utilizzo delle attività di sola convalida con la convalida della destinazione S3](#)

Prerequisiti per la convalida della destinazione S3

Prima di utilizzare la convalida della destinazione S3, controlla le seguenti impostazioni e autorizzazioni:

- Imposta su parquet il valore DataFormat per [S3Settings](#) dell'endpoint. Per ulteriori informazioni, consulta [Impostazioni di Parquet per S3](#).
- Assicurati che il ruolo assegnato all'account utente utilizzato per creare l'attività di migrazione disponga del set di autorizzazioni corretto. Consulta [Autorizzazioni](#) di seguito.

Per le attività che utilizzano la replica continua (CDC), controlla le seguenti impostazioni:

- Attiva il log supplementare in modo da avere i record completi nei dati CDC. Per informazioni sull'attivazione del log supplementare, consulta [Aggiunta automatica di log supplementare a un endpoint di origine Oracle](#) nella sezione [Risoluzione dei problemi e supporto diagnostico](#) della presente guida.
- Imposta il parametro TimestampColumnName per l'endpoint di destinazione. Non ci sono limitazioni al nome della colonna del timestamp. Per ulteriori informazioni, consulta [S3Settings](#).
- Imposta il partizionamento delle cartelle basato sulla data per la destinazione. Per ulteriori informazioni, consulta [Utilizzo del partizionamento delle cartelle in base alla data](#).

Autorizzazioni per l'utilizzo della convalida della destinazione S3

Per configurare l'accesso per l'uso della convalida della destinazione S3, assicurati che il ruolo assegnato all'account utente utilizzato per creare l'attività di migrazione disponga del seguente set di autorizzazioni. Sostituisci i valori di esempio con i tuoi valori.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "athena:StartQueryExecution",
        "athena:GetQueryExecution",
        "athena:CreateWorkGroup"
      ],
      "Resource": "arn:aws:athena:<endpoint_region_code>:<account_id>:workgroup/
dms_validation_workgroup_for_task_*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:CreateDatabase",
        "glue>DeleteDatabase",
        "glue:GetDatabase",
        "glue:GetTables",
        "glue:CreateTable",
        "glue>DeleteTable",
        "glue:GetTable"
      ],
      "Resource": [
        "arn:aws:glue:<endpoint_region_code>:<account_id>:catalog",
        "arn:aws:glue:<endpoint_region_code>:<account_id>:database/
aws_dms_s3_validation_*",
        "arn:aws:glue:<endpoint_region_code>:<account_id>:table/
aws_dms_s3_validation_*/**",
        "arn:aws:glue:<endpoint_region_code>:<account_id>:userDefinedFunction/
aws_dms_s3_validation_*/**"
      ]
    },
    {
      "Effect": "Allow",
```

```
    "Action": [
      "s3:GetBucketLocation",
      "s3:GetObject",
      "s3:ListBucketMultipartUploads",
      "s3:AbortMultipartUpload",
      "s3:ListMultipartUploadParts"
    ],
    "Resource": [
      "arn:aws:s3:::<bucket_name>",
      "arn:aws:s3:::<bucket_name>/*"
    ]
  }
]
```

Limitazioni all'utilizzo della convalida della destinazione S3

Esamina le seguenti limitazioni aggiuntive che si applicano quando si utilizza la convalida della destinazione S3. Per le limitazioni che si applicano a tutte le convalide, consulta [Limitazioni](#).

- Il valore `DatePartitionSequence` ha bisogno di un componente `Day`. La convalida della destinazione S3 non supporta il formato `YYYYMM`.
- Quando la convalida di intervallo è in esecuzione durante la CDC, è possibile che nella tabella `awsdms_validation_failures_v1` vengano visualizzati falsi errori di convalida. Questi errori si verificano perché AWS DMS migra le modifiche arrivate durante la convalida di intervallo nella cartella delle partizioni del giorno successivo. Normalmente, queste modifiche vengono scritte nella cartella delle partizioni del giorno corrente. Questi falsi errori rappresentano una limitazione della convalida della replica da un database di origine dinamico a una destinazione statica, come Amazon S3. Per esaminare questi falsi errori, verifica i record vicino alla fine della finestra di convalida (00:00 UTC), che è il momento in cui di solito compaiono questi errori.

Per ridurre al minimo il numero di falsi errori, assicurati che il valore di `CDCLatencySource` per l'attività sia basso. Per informazioni sul monitoraggio della latenza, consulta [Parametri dell'attività di replica](#).

- Le attività nello stato `failed` o `stopped` non convalidano le modifiche del giorno precedente. Per ridurre al minimo gli errori di convalida dovuti a malfunzionamenti imprevisti, crea attività di sola convalida separate con le stesse mappature delle tabelle e gli stessi endpoint di origine e di

destinazione. Per ulteriori informazioni sulle attività di sola convalida, consulta [Utilizzo delle attività di sola convalida con la convalida della destinazione S3](#).

- La colonna Stato di convalida nelle statistiche della tabella indica lo stato della convalida di intervallo più recente. Di conseguenza, una tabella che presenta delle discrepanze potrebbe apparire come convalidata dopo la convalida di intervallo del giorno successivo. Controlla `s3_validation_failures` folder nel bucket Amazon S3 di destinazione le mancate corrispondenze che si sono verificate più di un giorno prima.
- S3 Validation utilizza la funzionalità bucketed table di Amazon Athena. Ciò consente alla convalida S3 di creare una copia bucket dei dati della tabella di destinazione. Ciò significa che la copia dei dati della tabella è suddivisa in sottoinsiemi che corrispondono al partizionamento interno della convalida DMS. I tavoli vecchi Athena hanno un limite di 100.000 bucket. Tutte le tabelle che la convalida di S3 tenta di convalidare e che superano questo limite falliranno la convalida. Il numero di bucket che S3 Validation tenta di creare è uguale al seguente:

$$(\text{\#records in the table}) / (\text{validation partition size setting})$$

Per ovviare a questa limitazione, aumenta l'impostazione della dimensione della partizione di convalida in modo che il numero di bucket creati da S3 Validation sia inferiore a 100.000. Per ulteriori informazioni sul bucketing, consulta [Partitioning and bucketing in Athena nella Amazon Athena](#) User Guide.

Utilizzo delle attività di sola convalida con la convalida della destinazione S3

Un'attività di sola convalida esegue la convalida dei dati da migrare senza eseguire la migrazione.

Le attività di sola convalida continuano a essere eseguite, anche se l'attività di migrazione si interrompe, il che garantisce che AWS DMS non ignori la finestra di convalida di intervallo 00:00 UTC.

L'utilizzo delle attività di sola convalida con endpoint Amazon S3 presenta le seguenti limitazioni:

- La convalida Amazon S3 per le attività di pieno carico con l'impostazione Validation-Only abilitata è supportata, ma funziona in modo diverso rispetto alle attività di pieno carico con l'impostazione Validation-Only per altri endpoint. Per S3 come destinazione, un'attività di questo tipo viene convalidata solo in base ai dati di pieno carico nella destinazione S3 e non in base ai dati migrati nell'ambito di una migrazione CDC. Utilizza questa funzionalità per convalidare i dati creati da

un'attività solo pieno carico. L'utilizzo di questa modalità per convalidare i dati in una destinazione su cui è in esecuzione un'attività di CDC attiva non produce una convalida efficace.

- Le attività di sola convalida convalidano solo le modifiche avvenute dopo l'ultima finestra di convalida di intervallo (00:00 UTC). Le attività di sola convalida non convalidano i dati di pieno carico o i dati CDC dei giorni precedenti.

Assegnazione di tag alle risorse in AWS Database Migration Service

Puoi utilizzare i tag presenti in AWS Database Migration Service (AWS DMS) per aggiungere metadati alle risorse. Inoltre, puoi usare i tag con le policy AWS Identity and Access Management (IAM) per gestire l'accesso alle risorse AWS DMS e per controllare le operazioni che è possibile applicare alle risorse AWS DMS. Infine, questi tag possono essere utilizzati per monitorare i costi raggruppando le spese per risorse con tag simili.

Non a tutte le risorse AWS DMS è possibile applicare un tag:

- Certificati
- Fornitori di dati
- Migrazioni di dati
- Endpoint
- Abbonamenti a eventi
- Profili delle istanze
- Progetti di migrazione
- Istanze di replica
- Gruppi di sottoreti di replica
- Attività di replica

Un tag AWS DMS è una coppia nome-valore definita e associata a una risorsa AWS DMS. Il nome viene definito chiave. L'indicazione di un valore per la chiave è un'operazione facoltativa. È possibile usare i tag per assegnare informazioni arbitrarie a una risorsa AWS DMS. Una chiave tag potrebbe essere impiegata, ad esempio, per definire una categoria e il valore di tag potrebbe essere una voce di tale categoria. Ad esempio, puoi definire una chiave di tag "progetto" e un valore di tag "Salix", che indica che la risorsa AWS DMS viene assegnata al progetto Salix. Puoi inoltre usare i tag per designare le risorse AWS DMS usate per le attività di test o di produzione tramite una chiave, come ambiente=test o ambiente=produzione. È consigliabile utilizzare un set coerente di chiavi di tag per agevolare il monitoraggio dei metadati associati alle risorse AWS DMS.

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 la pagina sull'[utilizzo dei tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing.

Ogni risorsa AWS DMS dispone di un set di tag contenente tutti i tag assegnati a tale risorsa AWS DMS. Un set di tag può contenere fino a dieci tag ma può anche essere vuoto. Se aggiungi un tag a una risorsa AWS DMS con la stessa chiave di un tag esistente per la risorsa, il nuovo valore sovrascrive quello precedente.

AWS non applica alcun significato semantico ai tag, che vengono interpretati rigorosamente come stringhe di caratteri. AWS DMS può impostare i tag in una risorsa AWS DMS, a seconda delle impostazioni scelte al momento della creazione della risorsa.

L'elenco seguente descrive le caratteristiche di un tag AWS DMS.

- La chiave di tag corrisponde al nome obbligatorio del tag. Il valore della stringa può essere composto da 1 a 128 caratteri Unicode e non può avere il prefisso "aws:" o "dms:". La stringa può contenere solo il set Unicode di lettere, cifre, spazi vuoti, "_", ".", "/", "=", "+", "-" (espressione regolare Java: "`^[\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*`").
- Il valore di tag è un valore di stringa opzionale del tag. Il valore della stringa può essere composto da 1 a 256 caratteri Unicode e non può avere il prefisso "aws:" o "dms:". La stringa può contenere solo il set Unicode di lettere, cifre, spazi vuoti, "_", ".", "/", "=", "+", "-" (espressione regolare Java: "`^[\\p{L}\\p{Z}\\p{N}_.:/=+\\-]*`").

I valori non devono essere necessariamente univoci in un set di tag e possono essere Null. Ad esempio, può esserci una coppia chiave-valore in un set di tag project/Trinity e in cost-center/Trinity.

Puoi utilizzare la AWS CLI o l'API AWS DMS per aggiungere, elencare ed eliminare i tag nelle risorse AWS DMS. Quando si usano la AWS CLI o l'API AWS DMS, è necessario fornire il nome della risorsa Amazon (ARN) della risorsa AWS DMS che si vuole utilizzare. Per ulteriori informazioni sulla creazione di un ARN, consultare [Creazione di un Amazon Resource Name \(ARN\) per AWS DMS](#).

Tieni presente che i tag sono memorizzati nella cache a fini di autorizzazione. Questo è il motivo per il quale le aggiunte e gli aggiornamenti dei tag delle risorse AWS DMS potrebbero richiedere diversi minuti prima di diventare disponibili.

API

Puoi aggiungere, elencare o rimuovere i tag per una risorsa AWS DMS utilizzando l'API AWS DMS.

- Per aggiungere un tag a una risorsa AWS DMS, utilizza l'operazione [AddTagsToResource](#).
- Per elencare i tag assegnati a una risorsa AWS DMS, utilizza l'operazione [ListTagsForResource](#).
- Per rimuovere i tag da una risorsa AWS DMS, utilizza l'operazione [RemoveTagsFromResource](#).

Per ulteriori informazioni su come creare l'ARN necessario, consultare [Creazione di un Amazon Resource Name \(ARN\) per AWS DMS](#).

Quando utilizzi XML con l'API AWS DMS, i tag seguono questo schema:

```
<Tagging>
  <TagSet>
    <Tag>
      <Key>Project</Key>
      <Value>Trinity</Value>
    </Tag>
    <Tag>
      <Key>User</Key>
      <Value>Jones</Value>
    </Tag>
  </TagSet>
</Tagging>
```

La tabella riportata di seguito fornisce un elenco dei tag XML consentiti e le relative caratteristiche. Tieni presente che i valori relativi a chiave e valore fanno distinzione tra maiuscole e minuscole. Ad esempio, project=Trinity e PROJECT=Trinity sono due tag distinti.

Elemento del tagging	Descrizione
TagSet	<p>Un set di tag è un contenitore di tutti i tag assegnati a una risorsa Amazon RDS. Ogni risorsa può disporre di un solo set di tag. Puoi usare un elemento TagSet solo tramite l'API AWS DMS.</p>
Tag	<p>Un tag è una coppia chiave-valore definita dall'utente. Un set di tag può contenere da 1 a 10 tag.</p>
Chiave	<p>Una chiave corrisponde al nome obbligatorio del tag. Il valore della stringa può essere composto da 1 a 128 caratteri Unicode e non può avere il prefisso "dms:" o "aws:". La stringa può contenere solo il set di lettere, cifre, spazi vuoti, "_", ".", "/", "=", "+", "-" Unicode (espressione regolare Java: <code>"^([\p{L}\p{Z}\p{N}_./=+\-]*)\$"</code>).</p> <p>Le chiavi devono essere uniche per un set di tag. Ad esempio, non puoi avere una coppia di chiavi in un set di tag con la stessa chiave, ma con valori diversi, come <code>project/Trinity</code> e <code>project/Xanadu</code>.</p>
Valore	<p>Un valore è il valore opzione del tag. Il valore della stringa può essere composto da 1 a 256 caratteri Unicode e non può avere il prefisso "dms:" o "aws:". La stringa può contenere solo il set di lettere, cifre, spazi vuoti, "_", ".", "/", "=", "+", "-" Unicode (espressione regolare Java: <code>"^([\p{L}\p{Z}\p{N}_./=+\-]*)\$"</code>).</p> <p>I valori non devono essere necessariamente univoci in un set di tag e possono essere Null. Ad esempio, può esserci una coppia chiave-valore in un set di tag <code>project/Trinity</code> e in <code>cost-center/Trinity</code>.</p>

Sicurezza in AWS Database Migration Service

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformitàAWS](#). Per maggiori informazioni sui programmi di conformità applicabili AWS DMS, consulta la sezione [AWS Servizi rientranti nell'ambito del programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, nonché le leggi e le normative applicabili.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo AWS DMS. I seguenti argomenti mostrano come eseguire la configurazione AWS DMS per soddisfare gli obiettivi di sicurezza e conformità. Imparerai anche a utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere AWS DMS le tue risorse.

Puoi gestire l'accesso alle tue AWS DMS risorse e ai tuoi database (DB). Il metodo utilizzato per gestire l'accesso dipende dall'attività di replica da eseguire con: AWS DMS

- Utilizza le policy AWS Identity and Access Management (IAM) per assegnare le autorizzazioni che determinano chi è autorizzato a gestire le risorse. AWS DMS richiede che tu disponga delle autorizzazioni appropriate se accedi come utente IAM. Ad esempio, puoi utilizzare IAM per determinare chi è autorizzato a creare, descrivere, modificare ed eliminare cluster e istanze database, applicare tag alle risorse oppure modificare i gruppi di sicurezza. Per ulteriori informazioni su IAM e sul suo utilizzo con AWS DMS, consulta [Gestione delle identità e degli accessi per AWS Database Migration Service](#).
- AWS DMS utilizza Secure Sockets Layer (SSL) per le connessioni degli endpoint con Transport Layer Security (TLS). Per ulteriori informazioni sull'utilizzo di SSL/TLS con, consulta [AWS DMS Utilizzo di SSL con AWS Database Migration Service](#)

- AWS DMS utilizza le chiavi di crittografia AWS Key Management Service (AWS KMS) per crittografare lo storage utilizzato dall'istanza di replica e le relative informazioni di connessione all'endpoint. AWS DMS utilizza anche chiavi di AWS KMS crittografia per proteggere i dati di destinazione inattivi per gli endpoint di destinazione Amazon S3 e Amazon Redshift. Per ulteriori informazioni, consulta [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#).
- AWS DMS crea sempre la tua istanza di replica in un cloud privato virtuale (VPC) basato sul servizio Amazon VPC per il massimo controllo possibile degli accessi alla rete. Per le istanze database e i cluster di istanza, utilizza lo stesso VPC dell'istanza di replica o VPC aggiuntivi per corrispondere a questo livello di controllo dell'accesso. Ciascun Amazon VPC utilizzato deve essere associato a un gruppo di sicurezza che dispone di regole che consentono l'uscita di tutto il traffico su tutte le porte dal VPC. Questo approccio consente la comunicazione dall'istanza di replica agli endpoint dei database di origine e di destinazione, purché su tali endpoint sia abilitato l'ingresso corretto.

Per ulteriori informazioni sulle configurazioni di rete disponibili per, consulta. AWS DMS [Configurazione di una rete per un'istanza di replica](#) Per ulteriori informazioni sulla creazione di un'istanza database o di un cluster di istanza in un VPC, consulta la documentazione relativa alla sicurezza e alla gestione dei cluster per i database Amazon nella [Documentazione AWS](#). Per ulteriori informazioni sulle configurazioni di rete supportate da AWS DMS , consulta [Configurazione di una rete per un'istanza di replica](#).

- Per visualizzare i log di migrazione del database, sono necessarie le autorizzazioni Amazon CloudWatch Logs appropriate per il ruolo IAM che stai utilizzando. Per ulteriori informazioni sulla registrazione per AWS DMS, consulta [Monitoraggio delle attività di replica usando Amazon CloudWatch](#).

Argomenti

- [Protezione dei dati in AWS Database Migration Service](#)
- [Gestione delle identità e degli accessi per AWS Database Migration Service](#)
- [Convalida della conformità per AWS Database Migration Service](#)
- [Resilienza in AWS Database Migration Service](#)
- [Sicurezza dell'infrastruttura in AWS Database Migration Service](#)
- [Controllo granulare degli accessi tramite i nomi e i tag delle risorse](#)
- [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#)

- [Sicurezza di rete per AWS Database Migration Service](#)
- [Utilizzo di SSL con AWS Database Migration Service](#)
- [Modifica della password del database](#)

Protezione dei dati in AWS Database Migration Service

Crittografia dei dati

È possibile abilitare la crittografia per le risorse di dati degli endpoint di AWS DMS destinazione supportati. AWS DMS crittografa anche le connessioni verso AWS DMS e tra tutti gli AWS DMS endpoint di origine e di destinazione. Inoltre, è possibile gestire le chiavi utilizzate per abilitare questa AWS DMS crittografia da e dagli endpoint di destinazione supportati.

Argomenti

- [Crittografia a riposo](#)
- [Crittografia in transito](#)
- [Gestione delle chiavi](#)

Crittografia a riposo

AWS DMS supporta la crittografia a riposo, consentendoti di specificare la modalità di crittografia lato server che desideri utilizzare per inviare i dati replicati ad Amazon S3 prima che vengano copiati sugli endpoint di destinazione supportati. AWS DMS Puoi specificare questa modalità di crittografia impostando l'attributo di connessione `encryptionMode` aggiuntivo per l'endpoint. Se questa `encryptionMode` impostazione specifica la modalità di crittografia delle chiavi KMS, puoi anche creare AWS KMS chiavi personalizzate specificamente per crittografare i dati di destinazione per i seguenti endpoint di destinazione: AWS DMS

- Amazon Redshift: per ulteriori informazioni sull'impostazione di `encryptionMode`, consulta [Impostazioni degli endpoint quando si utilizza Amazon Redshift come destinazione per AWS DMS](#). Per ulteriori informazioni sulla creazione di una chiave di AWS KMS crittografia personalizzata, consulta [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#)
- Amazon S3: per ulteriori informazioni sull'impostazione di `encryptionMode`, consulta [Impostazioni degli endpoint quando si utilizza Amazon S3 come destinazione per AWS DMS](#). Per ulteriori informazioni sulla creazione di una chiave di AWS KMS crittografia personalizzata, vedere [Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3](#).

Crittografia in transito

AWS DMS supporta la crittografia in transito garantendo che i dati replicati vengano spostati in modo sicuro dall'endpoint di origine all'endpoint di destinazione. È inclusa la crittografia di un bucket S3 nell'istanza di replica utilizzata dall'attività di replica per lo storage intermedio mentre i dati si spostano attraverso la pipeline di replica. Per crittografare le connessioni delle attività agli endpoint di origine e di destinazione AWS DMS utilizza Secure Socket Layer (SSL) o Transport Layer Security (TLS). Crittografando le connessioni a entrambi gli endpoint, AWS DMS garantisce la sicurezza dei dati durante il trasferimento dall'endpoint di origine all'attività di replica e dall'attività all'endpoint di destinazione. Per ulteriori informazioni sull'utilizzo di SSL/TLS con, consulta [AWS DMS Utilizzo di SSL con AWS Database Migration Service](#)

AWS DMS supporta chiavi predefinite e personalizzate per crittografare sia lo storage di replica intermedio che le informazioni di connessione. Puoi gestire queste chiavi utilizzando AWS KMS. Per ulteriori informazioni, consulta [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#).

Gestione delle chiavi

AWS DMS supporta chiavi predefinite o personalizzate per crittografare lo storage di replica, le informazioni di connessione e l'archiviazione dei dati di destinazione per determinati endpoint di destinazione. È possibile gestire queste chiavi utilizzando AWS KMS. Per ulteriori informazioni, consulta [Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS](#).

Riservatezza del traffico Internet

Le connessioni sono dotate di protezione tra gli endpoint di origine AWS DMS e di destinazione nella stessa AWS regione, indipendentemente dal fatto che vengano eseguite in locale o come parte di un AWS servizio nel cloud. (Almeno un endpoint, di origine o di destinazione, deve essere eseguito come parte di un AWS servizio nel cloud.) Questa protezione si applica indipendentemente dal fatto che questi componenti condividano lo stesso cloud privato virtuale (VPC) o esistano in VPC separati, se i VPC si trovano tutti nella stessa regione. AWS Per ulteriori informazioni sulle configurazioni di rete supportate per, vedere [AWS DMS Configurazione di una rete per un'istanza di replica](#) Per ulteriori informazioni sulle considerazioni di protezione quando si utilizzano queste configurazioni di rete, consulta [Sicurezza di rete per AWS Database Migration Service](#).

Protezione dei dati in DMS Fleet Advisor

DMS Fleet Advisor raccoglie e analizza i metadati del database per determinare la dimensione corretta della destinazione della migrazione. DMS Fleet Advisor non accede ai dati nelle tabelle e non li trasferisce. Inoltre, DMS Fleet Advisor non tiene traccia dell'utilizzo delle funzionalità del database e non accede alle statistiche di utilizzo.

Puoi controllare l'accesso ai database quando crei gli utenti che DMS Fleet Advisor utilizza per utilizzare i database. Fornisci i privilegi richiesti agli utenti. Per utilizzare DMS Fleet Advisor, fornisci agli utenti dei database le autorizzazioni di lettura. DMS Fleet Advisor non modifica i database e non richiede autorizzazioni di scrittura. Per ulteriori informazioni, consulta [Creazione di utenti di database per AWS DMS Fleet Advisor](#).

È possibile utilizzare la crittografia dei dati nei database. AWS DMS crittografa anche le connessioni all'interno di DMS Fleet Advisor e all'interno dei suoi raccoglitori di dati.

Il raccoglitore di dati DMS utilizza l'interfaccia di programmazione delle applicazioni di protezione dei dati per crittografare, proteggere e archiviare le informazioni sull'ambiente e sulle credenziali dei database del cliente. DMS Fleet Advisor archivia questi dati crittografati in un file sul server su cui è in funzione il raccoglitore di dati DMS. DMS Fleet Advisor non trasferisce i dati dal server. Per ulteriori informazioni sull'interfaccia di programmazione delle applicazioni di protezione dei dati, vedi [How to: Use Data Protection](#).

Dopo aver installato il raccoglitore di dati DMS, puoi visualizzare tutte le query eseguite dall'applicazione per raccogliere le metriche. Puoi eseguire il raccoglitore di dati DMS in modalità offline e quindi esaminare i dati raccolti sul tuo server. Inoltre, puoi rivedere questi dati raccolti nel tuo bucket Amazon S3. Per ulteriori informazioni, consulta [Come funziona il raccoglitore di dati DMS?](#).

Gestione delle identità e degli accessi per AWS Database Migration Service

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse. AWS DMS IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come AWS Database Migration Service funziona con IAM](#)
- [AWS Database Migration Service esempi di policy basate sull'identità](#)
- [Esempi di policy basate sulle risorse per AWS KMS](#)
- [Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service](#)
- [Utilizzo di ruoli collegati ai servizi per AWS DMS](#)
- [Risoluzione dei problemi relativi AWS Database Migration Service all'identità e all'accesso](#)
- [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#)
- [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#)
- [Prevenzione del confused deputy tra servizi](#)
- [AWS politiche gestite per AWS Database Migration Service](#)

Destinatari

Il modo in cui usi AWS Identity and Access Management (IAM) varia a seconda del lavoro che AWS DMS svolgi.

Utente del servizio: se utilizzi il AWS DMS servizio per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più AWS DMS funzionalità 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 di AWS DMS, consulta [Risoluzione dei problemi relativi AWS Database Migration Service all'identità e all'accesso](#).

Amministratore del servizio: se sei responsabile delle AWS DMS risorse della tua azienda, probabilmente hai pieno accesso a AWS DMS. È tuo compito determinare a quali AWS DMS funzionalità e risorse 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 saperne di più su come la tua azienda può utilizzare IAM con AWS DMS, consulta [Come AWS Database Migration Service funziona con IAM](#).

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere policy per gestire l'accesso a AWS DMS. Per visualizzare esempi di policy AWS DMS basate sull'identità che puoi utilizzare in IAM, consulta [AWS Database Migration Service esempi di policy basate sull'identità](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS 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 Gli utenti (IAM Identity Center), 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 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 utilizzale 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 IAM.

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, se si hanno 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 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 IAMAdmins 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 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 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 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 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 conoscere la differenza tra ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta [Cross Account Resource Access in IAM nella IAM User Guide](#).
- **Accesso tra servizi:** alcuni Servizi AWS utilizzano funzionalità in 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 preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione 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 azioni. 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](#) che un servizio assume per eseguire azioni 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 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 CLI è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo 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 IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente 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 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 operazioni 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.

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'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' AWS CLI 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 IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate 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 IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata 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 funzionalità 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 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 presenti 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 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 AWS Database Migration Service funziona con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS DMS, è necessario comprendere con quali funzionalità IAM è disponibile l'uso AWS DMS. Per avere una visione di alto livello di come AWS DMS e altri AWS servizi funzionano con IAM, consulta [AWS i servizi che funzionano con IAM nella IAM User Guide](#).

Argomenti

- [Policy AWS DMS basate su identità](#)
- [Policy di AWS DMS basate sulle risorse](#)
- [Autorizzazione basata su tag AWS DMS](#)
- [Ruoli IAM per AWS DMS](#)
- [Identity and Access Management per DMS Fleet Advisor](#)

Policy AWS DMS basate su identità

Con le policy basate su identità IAM puoi specificare azioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. AWS DMS supporta azioni, risorse e chiavi di condizione specifiche. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta [Documentazione di riferimento degli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Azioni

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 `Actions` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. 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.

Le azioni politiche AWS DMS utilizzano il seguente prefisso prima dell'azione: `dms :`. Ad esempio, per concedere a qualcuno l'autorizzazione a creare un'attività di replica con l'operazione AWS DMS `CreateReplicationTask` API, includi `dms:CreateReplicationTask` azione nella sua politica. Le dichiarazioni politiche devono includere un `NotAction` elemento `Action` or. AWS DMS definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

Per specificare più operazioni in una singola istruzione, separarle con una virgola come mostrato di seguito.

```
"Action": [  
  "dms:action1",  
  "dms:action2"
```

Puoi specificare più operazioni tramite caratteri jolly (*). Ad esempio, per specificare tutte le operazioni che iniziano con la parola `Describe`, includi la seguente operazione.

```
"Action": "dms:Describe*"
```

Per visualizzare un elenco di AWS DMS azioni, consulta [Actions Defined by AWS Database Migration Service](#) nella IAM User Guide.

Risorse

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'operazione. 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": "*"
```

AWS DMS funziona con le seguenti risorse:

- Certificati
- Endpoints
- Abbonamenti a eventi
- Istanze di replica
- Gruppi di sottoreti di replica (sicurezza)
- Attività di replica

La risorsa o le risorse AWS DMS necessarie dipendono dall'azione o dalle azioni richiamate. È necessaria una policy che consenta queste azioni sulla risorsa o sulle risorse associate specificate dagli ARN.

Ad esempio, una risorsa AWS DMS endpoint ha il seguente ARN:

```
arn:${Partition}:dms:${Region}:${Account}:endpoint/${InstanceId}
```

Per ulteriori informazioni sul formato degli ARN, consulta [Amazon Resource Names \(ARNs\) e AWS service namespace](#).

Ad esempio, per specificare l'istanza dell'endpoint 1A2B3C4D5E6F7G8H9I0J1K2L3M per la regione us-east-2 nell'istruzione, utilizza il seguente ARN.

```
"Resource": "arn:aws:dms:us-east-2:987654321098:endpoint/1A2B3C4D5E6F7G8H9I0J1K2L3M"
```

Per specificare tutti gli endpoint che appartengono a un account specifico, utilizza il carattere jolly (*):

```
"Resource": "arn:aws:dms:us-east-2:987654321098:endpoint/*"
```

Alcune AWS DMS azioni, come quelle per la creazione di risorse, non possono essere eseguite su una risorsa specifica. In questi casi, è necessario utilizzare il carattere jolly (*).

```
"Resource": "*"
```

Alcune azioni AWS DMS API coinvolgono più risorse. Ad esempio, `StartReplicationTask` avvia e connette un'attività di replica a due risorse endpoint del database, un'origine e una destinazione,

pertanto un utente IAM deve disporre delle autorizzazioni per leggere l'endpoint di origine e scrivere nell'endpoint di destinazione. Per specificare più risorse in una singola istruzione, separa gli ARN con le virgole.

```
"Resource": [  
    "resource1",  
    "resource2" ]
```

Per ulteriori informazioni sul controllo dell'accesso alle AWS DMS risorse mediante le policy, consulta [Utilizzo dei nomi delle risorse per il controllo dell'accesso](#). Per un elenco di tipi di risorse di AWS DMS e i relativi ARN, consulta [Risorse definite da AWS Database Migration Service](#) nella Guida per l'utente IAM. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta [Operazioni definite da AWS Database Migration Service](#).

Chiavi di condizione

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.

AWS DMS definisce il proprio set di chiavi di condizione e supporta anche l'utilizzo di alcune chiavi di condizione globali. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le [chiavi di contesto delle condizioni AWS globali](#) nella Guida per l'utente IAM.

AWS DMS definisce un set di tag standard che puoi utilizzare nelle relative chiavi di condizione e ti consente anche di definire tag personalizzati. Per ulteriori informazioni, consulta [Utilizzo dei tag per controllare l'accesso](#).

Per visualizzare un elenco di chiavi di AWS DMS condizione, consulta [Condition Keys for AWS Database Migration Service](#) nella IAM User Guide. Per informazioni su azioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta [Operazioni definite da AWS Database Migration Service](#) e [Risorse definite da AWS Database Migration Service](#).

Esempi

Per visualizzare esempi di politiche AWS DMS basate sull'identità, consulta [AWS Database Migration Service esempi di policy basate sull'identità](#)

Policy di AWS DMS basate sulle risorse

Le politiche basate sulle risorse sono documenti di policy JSON che specificano quali azioni uno specifico principale può eseguire su una determinata risorsa e in quali condizioni. AWS DMS supporta politiche di autorizzazione basate sulle risorse per le chiavi di AWS KMS crittografia create per crittografare i dati migrati verso gli endpoint di destinazione supportati. Gli endpoint di destinazione supportati includono Amazon Redshift e Amazon S3. Utilizzando le policy basate su risorse, è possibile concedere l'autorizzazione per l'utilizzo di queste chiavi di crittografia ad altri account per ciascun endpoint di destinazione.

Per consentire l'accesso a più account, è possibile specificare un intero account o entità IAM in un altro account come [entità principale in una policy basata su 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 si trovano in AWS account diversi, è inoltre necessario concedere all'entità principale l'autorizzazione ad accedere alla risorsa. Concedi l'autorizzazione collegando una policy basata sull'identità all'entità. Tuttavia, se una policy basata su risorse concede l'accesso a un'entità 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.

Il AWS DMS servizio supporta solo un tipo di policy basata sulle risorse denominata policy chiave, che è associata a una AWS KMS chiave di crittografia. Questa policy definisce quali entità principali (account, utenti, ruoli e utenti federati) possono eseguire la crittografia dei dati migrati nell'endpoint di destinazione supportato.

Per informazioni su come collegare una policy basata su risorse a una chiave di crittografia creata per gli endpoint di destinazione supportati, consulta [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#) e [Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3](#).

Esempi

Per esempi di politiche basate sulle AWS DMS risorse, vedere. [Esempi di policy basate sulle risorse per AWS KMS](#)

Autorizzazione basata su tag AWS DMS

È possibile allegare tag alle AWS DMS risorse o passare tag in una richiesta a. AWS DMS Per controllare l'accesso in base ai tag, fornisci le informazioni sui tag nell'[elemento condition](#) di una policy utilizzando il tasto `dms:ResourceTag/key-name` `aws:RequestTag/key-name`, o `aws:TagKeys` condition. AWS DMS definisce un set di tag standard che è possibile utilizzare nelle relative chiavi di condizione e consente inoltre di definire tag personalizzati. Per ulteriori informazioni, consulta [Utilizzo dei tag per controllare l'accesso](#).

Per un esempio di policy basata su identità che limita l'accesso a una risorsa in base ai tag, consulta [Accesso alle risorse AWS DMS in base ai tag](#).

Ruoli IAM per AWS DMS

Un [ruolo IAM](#) è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche.

Utilizzo di credenziali temporanee con AWS DMS

Puoi utilizzare le credenziali temporanee per effettuare l'accesso utilizzando la federazione, assumere un ruolo IAM o assumere un ruolo tra più account. [È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come AssumeRoleo GetFederationToken.](#)

AWS DMS supporta l'utilizzo di credenziali temporanee.

Ruoli collegati ai servizi

[I ruoli collegati ai](#) AWS servizi consentono ai servizi di accedere alle risorse di altri servizi per completare un'azione per conto dell'utente. I ruoli collegati ai servizi sono visualizzati nell'account IAM e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non può modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli AWS DMS collegati ai servizi, consulta [Utilizzo di ruoli collegati ai servizi](#)

Ruoli dei servizi

Questa caratteristica consente a un servizio di assumere un [ruolo di servizio](#) per conto dell'utente. Questo ruolo consente al servizio di accedere alle risorse in altri servizi per completare un'azione per conto dell'utente. I ruoli dei servizi sono visualizzati nell'account IAM e sono di proprietà dell'account. Ciò significa che un amministratore IAM può modificare le autorizzazioni per questo ruolo. Tuttavia, questo potrebbe pregiudicare la funzionalità del servizio.

AWS DMS supporta due tipi di ruoli di servizio che è necessario creare per utilizzare determinati endpoint di origine o destinazione:

- Ruoli con autorizzazioni per consentire l'accesso AWS DMS ai seguenti endpoint di origine e destinazione (o alle relative risorse):
 - Amazon DynamoDB come destinazione. Per ulteriori informazioni, consulta [Prerequisiti per l'utilizzo di DynamoDB come destinazione per AWS Database Migration Service](#).
 - OpenSearch come destinazione: per ulteriori informazioni, vedere [Prerequisiti per l'utilizzo del servizio OpenSearch di Amazon come destinazione per AWS Database Migration Service](#)
 - Amazon Kinesis come destinazione. Per ulteriori informazioni, consulta [Prerequisiti per l'utilizzo di un flusso di dati Kinesis come destinazione per AWS Database Migration Service](#).
 - Amazon Redshift come destinazione. È necessario creare il ruolo specificato solo per generare una chiave di crittografia KMS personalizzata per crittografare i dati di destinazione o per specificare un bucket S3 personalizzato per lo storage intermedio delle attività. Per ulteriori informazioni, consulta [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#) o [Impostazioni del bucket Amazon S3](#).
 - Amazon S3 come origine o come destinazione. Per ulteriori informazioni, consulta [Prerequisiti per l'utilizzo di Amazon S3 come sorgente per AWS DMS](#) o [Prerequisiti per l'utilizzo di Amazon S3 come destinazione](#).

Ad esempio, per leggere i dati da un endpoint di origine S3 o per eseguire il push dei dati a un endpoint di destinazione S3, è necessario creare un ruolo di servizio come prerequisito per accedere a S3 per ciascuna di queste operazioni di endpoint.

- Ruoli con autorizzazioni necessarie per utilizzare l'API AWS CLI e AWS DMS: i due ruoli IAM che devi creare sono `dms-vpc-role` e `dms-cloudwatch-logs-role`. Se utilizzi Amazon Redshift come database di destinazione, devi anche creare e aggiungere il ruolo IAM `dms-access-for-endpoint` al tuo AWS account. Per ulteriori informazioni, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

Scegliere un ruolo IAM in AWS DMS

Se utilizzi l'API AWS CLI o l'API AWS DMS per la migrazione del database, devi aggiungere determinati ruoli IAM al tuo AWS account prima di poter utilizzare le funzionalità di AWS DMS. Due di questi sono `dms-vpc-role` e `dms-cloudwatch-logs-role`. Se utilizzi Amazon Redshift come database di destinazione, devi anche aggiungere il ruolo IAM `dms-access-for-endpoint` al tuo AWS account. Per ulteriori informazioni, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

Identity and Access Management per DMS Fleet Advisor

Con le policy IAM basate su identità puoi specificare azioni e risorse consentite o rifiutate, nonché le condizioni in base alle quali le azioni sono consentite o rifiutate. DMS Fleet Advisor supporta specifiche azioni, risorse e chiavi di condizione. Per informazioni su tutti gli elementi utilizzati in una policy JSON, consulta [Documentazione di riferimento degli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

DMS Fleet Advisor utilizza i ruoli IAM per accedere ad Amazon Simple Storage Service. Un [ruolo IAM](#) è un'entità all'interno del tuo AWS account che dispone di autorizzazioni specifiche. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).

AWS Database Migration Service esempi di policy basate sull'identità

Per impostazione predefinita, gli utenti e i ruoli IAM non dispongono dell'autorizzazione per creare o modificare risorse AWS DMS. Inoltre, non possono eseguire attività utilizzando l'API AWS Management Console AWS CLI, o AWS. Un amministratore IAM deve creare policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi allegare queste policy a utenti o IAM che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consultare [Creazione di policy nella scheda JSON](#) nella Guida per l'utente di IAM.

Argomenti

- [Best practice delle policy](#)
- [Utilizzo della console di AWS DMS](#)
- [Consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Accesso a un bucket Amazon S3](#)
- [Accesso alle risorse AWS DMS in base ai tag](#)

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS DMS risorse nel tuo account. Queste azioni 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 politiche 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 privilegio minimo: 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 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 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 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 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 di AWS DMS

La seguente politica consente di accedere a AWS DMS, inclusa la console AWS DMS, e specifica anche le autorizzazioni per determinate azioni necessarie da altri servizi Amazon come Amazon EC2.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "dms:*",
      "Resource": "arn:aws:dms:region:account:resourcetype/id"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:service:region:account:resourcetype/id"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
```

```

        "iam:PassRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:Get*",
        "cloudwatch:List*"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
]
}

```

L'analisi di queste autorizzazioni potrebbe aiutarti a comprendere meglio il motivo per cui ciascuna di esse è necessaria per l'uso della console.

La seguente sezione è necessaria per consentire all'utente di elencare le chiavi AWS KMS e gli alias disponibili per la visualizzazione nella console. Questa voce non è richiesta se si conosce l'ARN (Amazon Resource Name) per la chiave KMS e si sta utilizzando solo la AWS Command Line Interface (AWS CLI).

```
{
    "Effect": "Allow",
    "Action": [
        "kms:ListAliases",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

La seguente sezione è necessaria per determinati tipi di endpoint che richiedono il trasferimento dell'ARN del ruolo con l'endpoint. Inoltre, se i AWS DMS ruoli richiesti non vengono creati in anticipo, la AWS DMS console ha la possibilità di creare il ruolo. Se tutti i ruoli sono configurati in anticipo, sono tutti necessari in `iam:GetRole` e `iam:PassRole`. Per ulteriori informazioni sui ruoli, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

```
{
    "Effect": "Allow",
    "Action": [
        "iam:GetRole",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

La sezione seguente è necessaria perché è AWS DMS necessario creare l'istanza Amazon EC2 e configurare la rete per l'istanza di replica creata. Queste risorse esistono nell'account del cliente, perciò è necessaria la possibilità di eseguire tali azioni per conto del cliente.

```
{
    "Effect": "Allow",
    "Action": [
```

```

        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}

```

La seguente sezione è necessaria per consentire all'utente di visualizzare i parametri dell'istanza di replica.

```

{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:Get*",
        "cloudwatch:List*"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}

```

Questa sezione è necessaria per consentire all'utente di visualizzare i log della replica.

```

{
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}

```

La console AWS DMS crea diversi ruoli che vengono automaticamente collegati all' AWS account quando si utilizza la AWS console DMS. Se utilizzi AWS Command Line Interface (AWS CLI) o l'API AWS DMS per la migrazione, devi aggiungere questi ruoli al tuo account. Per ulteriori informazioni sull'aggiunta di questi ruoli, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

Per ulteriori informazioni sui requisiti per l'utilizzo di questa politica per accedere a AWS DMS, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#)

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 collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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": "*"
    }
  ]
}
```

Accesso a un bucket Amazon S3

AWS DMS utilizza i bucket Amazon S3 come storage intermedio per la migrazione dei database. In genere, AWS DMS gestisce i bucket S3 predefiniti per questo scopo. Tuttavia, in alcuni casi, specialmente quando si utilizza l'API AWS CLI o l'API DMS, AWS AWS DMS consente invece di specificare il proprio bucket S3. Ad esempio, puoi specificare il tuo bucket S3 per la migrazione dei dati a un endpoint di destinazione Amazon Redshift. In questo caso, è necessario creare un ruolo con autorizzazioni basate sulla policy `-managed`. `AWSAmazonDMSRedshiftS3Role`

L'esempio seguente mostra una versione della policy `AmazonDMSRedshiftS3Role`. Consente a AWS DMS di concedere a un utente IAM del tuo AWS account l'accesso a uno dei tuoi bucket Amazon S3. Consente inoltre all'utente di aggiungere, aggiornare ed eliminare oggetti.

Oltre ad assegnare le autorizzazioni `s3:PutObject`, `s3:GetObject` e `s3:DeleteObject` all'utente, la policy assegna anche le autorizzazioni `s3:ListAllMyBuckets`, `s3:GetBucketLocation` e `s3:ListBucket`. Queste sono le autorizzazioni aggiuntive richieste dalla console. Altre autorizzazioni consentono a AWS DMS di gestire il ciclo di vita del bucket. Inoltre, l'operazione `s3:GetObjectAcl` è necessaria per poter copiare gli oggetti.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:ListBucket",
        "s3:DeleteBucket",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:GetObjectVersion",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutBucketVersioning",
        "s3:GetBucketVersioning",
        "s3:PutLifecycleConfiguration",
        "s3:GetLifecycleConfiguration",
        "s3:DeleteBucketPolicy"
      ],
    }
  ],
}
```



```

        "Resource": "arn:aws:s3:::dms-*"
    }
]
}

```

Per ulteriori informazioni sulla creazione di un ruolo basato su questa policy, consulta [Impostazioni del bucket Amazon S3](#).

Accesso alle risorse AWS DMS in base ai tag

Puoi utilizzare le condizioni nella policy basata sulle identità per controllare l'accesso alle risorse di AWS DMS in base ai tag. Questo esempio mostra come è possibile creare una policy che consenta l'accesso a tutti gli AWS endpoint DMS. Tuttavia, l'autorizzazione viene concessa solo se il valore del tag `Owner` del database dell'endpoint è quello del nome dell'utente.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "dms:*",
      "Resource": "arn:aws:dms:*:*:endpoint/*",
      "Condition": {
        "StringEquals": {"dms:endpoint-tag/Owner": "${aws:username}"}
      }
    }
  ]
}

```

Puoi allegare questa policy agli utenti IAM nel tuo account. Se un utente denominato `richard-roe` tenta di accedere a un AWS DMS endpoint, il database dell'endpoint deve essere taggato o. `Owner=richard-roe owner=richard-roe` In caso contrario, a questo utente viene negato l'accesso. La chiave di tag di condizione `Owner` corrisponde a `Owner` e `owner` perché i nomi delle chiavi di condizione non effettuano la distinzione tra maiuscole e minuscole. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente IAM.

Esempi di policy basate sulle risorse per AWS KMS

AWS DMS consente di creare chiavi di AWS KMS crittografia personalizzate per crittografare i dati degli endpoint di destinazione supportati. Per informazioni su come creare e collegare una policy alla chiave di crittografia creata per la crittografia dei dati di destinazione supportati, consulta [Creazione e](#)

[utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#) e [Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3](#).

Argomenti

- [Una policy per una chiave di AWS KMS crittografia personalizzata per crittografare i dati di destinazione di Amazon Redshift](#)
- [Una politica per una chiave di AWS KMS crittografia personalizzata per crittografare i dati di destinazione di Amazon S3](#)

Una policy per una chiave di AWS KMS crittografia personalizzata per crittografare i dati di destinazione di Amazon Redshift

Nell'esempio seguente viene illustrato il JSON per la policy della chiave creata per una chiave di crittografia AWS KMS per crittografare i dati di destinazione Amazon Redshift.

```
{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::987654321098:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    },
    {
      "Sid": "Allow access for Key Administrators",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::987654321098:role/Admin"
        ]
      },
      "Action": [
        "kms:Create*",
        "kms:Describe*",

```

```
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms>Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::987654321098:role/DMS-Redshift-endpoint-access-role"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::987654321098:role/DMS-Redshift-endpoint-access-role"
    ]
  },
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ]
}
```

```

    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "kms:GrantIsForAWSResource": true
      }
    }
  }
]
}

```

Qui è possibile vedere dove la policy della chiave fa riferimento al ruolo per accedere ai dati dell'endpoint di destinazione Amazon Redshift creati prima di generare la chiave. Nell'esempio è `DMS-Redshift-endpoint-access-role`. È inoltre possibile vedere le diverse operazioni di chiave consentite per le diverse entità principali (utenti e ruoli). Ad esempio, qualsiasi utente con `DMS-Redshift-endpoint-access-role` può crittografare, decrittografare e crittografare nuovamente i dati di destinazione. Tale utente può anche generare chiavi di dati da esportare per crittografare i dati all'esterno. AWS KMS Possono anche restituire informazioni dettagliate su una AWS KMS chiave, ad esempio la chiave appena creata. Inoltre, l'utente può gestire i collegamenti alle risorse AWS , ad esempio l'endpoint di destinazione.

Una politica per una chiave di AWS KMS crittografia personalizzata per crittografare i dati di destinazione di Amazon S3

Nell'esempio seguente viene illustrato il JSON per la policy della chiave creata per una chiave di crittografia AWS KMS per crittografare i dati di destinazione Amazon S3.

```

{
  "Id": "key-consolepolicy-3",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Enable IAM User Permissions",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::987654321098:root"
        ]
      },
      "Action": "kms:*",
      "Resource": "*"
    }
  ]
}

```

```
},
{
  "Sid": "Allow access for Key Administrators",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::987654321098:role/Admin"
    ]
  },
  "Action": [
    "kms:Create*",
    "kms:Describe*",
    "kms:Enable*",
    "kms:List*",
    "kms:Put*",
    "kms:Update*",
    "kms:Revoke*",
    "kms:Disable*",
    "kms:Get*",
    "kms>Delete*",
    "kms:TagResource",
    "kms:UntagResource",
    "kms:ScheduleKeyDeletion",
    "kms:CancelKeyDeletion"
  ],
  "Resource": "*"
},
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::987654321098:role/DMS-S3-endpoint-access-role"
    ]
  },
  "Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
}
```

```
{
  "Sid": "Allow attachment of persistent resources",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::987654321098:role/DMS-S3-endpoint-access-role"
    ]
  },
  "Action": [
    "kms:CreateGrant",
    "kms:ListGrants",
    "kms:RevokeGrant"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "kms:GrantIsForAWSResource": true
    }
  }
}
```

Qui è possibile vedere dove la policy della chiave fa riferimento al ruolo per accedere ai dati dell'endpoint di destinazione Amazon S3 creati prima di generare la chiave. Nell'esempio è `DMS-S3-endpoint-access-role`. È inoltre possibile vedere le diverse operazioni di chiave consentite per le diverse entità principali (utenti e ruoli). Ad esempio, qualsiasi utente con `DMS-S3-endpoint-access-role` può crittografare, decrittografare e crittografare nuovamente i dati di destinazione. Tale utente può anche generare chiavi di dati da esportare per crittografare i dati all'esterno. AWS KMS Possono anche restituire informazioni dettagliate su una AWS KMS chiave, ad esempio la chiave appena creata. Inoltre, l'utente può gestire il collegamento alle risorse AWS , ad esempio l'endpoint di destinazione.

Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service

Infatti AWS DMS, un segreto è una chiave crittografata che è possibile utilizzare per rappresentare un set di credenziali utente per autenticare, tramite l'autenticazione segreta, la connessione al database per un endpoint di AWS DMS origine o di destinazione supportato. Per un endpoint Oracle che utilizza anche Oracle Automatic Storage Management (ASM), AWS DMS richiede un segreto aggiuntivo che rappresenti le credenziali utente per accedere a Oracle ASM.

È possibile creare il segreto o i segreti AWS DMS necessari per l'autenticazione segreta utilizzando un servizio per la creazione AWS Secrets Manager, l'archiviazione e il recupero in modo sicuro delle credenziali per accedere ad applicazioni, servizi e risorse IT nel cloud e in locale. È incluso il supporto per la rotazione periodica automatica del valore del segreto crittografato senza l'intervento dell'utente, che fornisce un ulteriore livello di sicurezza per le credenziali. L'attivazione della rotazione dei valori segreti garantisce AWS Secrets Manager inoltre che questa rotazione dei valori segreti avvenga senza alcun effetto sulla migrazione del database che si basa sul segreto. Per autenticare segretamente una connessione del database agli endpoint, crea un segreto e assegnane l'identità o l'ARN a `SecretsManagerSecretId`, da includere nelle impostazioni dell'endpoint. Per autenticare segretamente Oracle ASM come parte di un endpoint Oracle, crea un segreto e assegnane l'identità o l'ARN a `SecretsManagerOracleAsmSecretId`, da includere sempre nelle impostazioni dell'endpoint.

Note

Non puoi usare le credenziali master gestite da Amazon RDS Aurora. Queste credenziali non includono informazioni sull'host o sulla porta, che AWS DMS devono stabilire connessioni. Crea invece un utente e un segreto nuovi. Per informazioni sulla creazione di un utente e un segreto, consulta [Utilizzo di AWS Management Console per creare un ruolo di accesso segreto e segreto](#) di seguito.

Per ulteriori informazioni su AWS Secrets Manager, consulta [What Is AWS Secrets Manager?](#) nella Guida AWS Secrets Manager per l'utente.


AWS DMS supporta l'autenticazione segreta per i seguenti database locali o AWS gestiti sugli endpoint di origine e di destinazione supportati:

- Amazon DocumentDB
- IBM Db2 LUW
- Microsoft SQL Server
- MongoDB
- MySQL
- Oracle
- PostgreSQL
- Amazon Redshift

- SAP ASE

Per la connessione a uno di questi database, puoi scegliere di specificare uno dei seguenti set di valori, ma non entrambi, come parte delle impostazioni dell'endpoint:

- Valori in chiaro per autenticare la connessione al database utilizzando le impostazioni `UserName`, `Password`, `ServerName` e `Port`. Per un endpoint Oracle che utilizza anche Oracle ASM, includi valori in chiaro aggiuntivi per autenticare ASM utilizzando le impostazioni `AsmUserName`, `AsmPassword` e `AsmServerName`.
- Autenticazione dei segreti utilizzando i valori per le impostazioni `SecretsManagerSecretId` e `SecretsManagerAccessRoleArn`. Per un endpoint Oracle che utilizza Oracle ASM, includi valori aggiuntivi per le impostazioni `SecretsManagerOracleAsmSecretId` e `SecretsManagerOracleAsmAccessRoleArn`. I valori dei segreti di queste impostazioni possono includere:
 - `SecretsManagerSecretId`: il nome della risorsa Amazon (ARN) completo, l'ARN parziale o il nome descrittivo di un segreto che hai creato per l'accesso al database degli endpoint in AWS Secrets Manager.
 - `SecretsManagerAccessRoleArn`— L'ARN di un ruolo di accesso segreto che hai creato in IAM per fornire AWS DMS l'accesso a questo `SecretsManagerSecretId` segreto per tuo conto.
 - `SecretsManagerOracleAsmSecretId`: il nome della risorsa Amazon (ARN) completo, l'ARN parziale o il nome descrittivo di un segreto che hai creato per l'accesso a Oracle ASM in AWS Secrets Manager.
 - `SecretsManagerOracleAsmAccessRoleArn`: l'ARN di un ruolo di accesso al segreto che hai creato in IAM per fornire ad AWS DMS l'accesso al segreto `SecretsManagerOracleAsmSecretId` per tuo conto.

 Note

Puoi anche utilizzare un singolo ruolo di accesso segreto per fornire AWS DMS l'accesso sia al `SecretsManagerSecretId` segreto che al `SecretsManagerOracleAsmSecretId` segreto. Se crei questo singolo ruolo di accesso per entrambi i segreti, assicurati di assegnare lo stesso ARN per il ruolo di accesso a entrambi `SecretsManagerAccessRoleArn` e `SecretsManagerOracleAsmAccessRoleArn`. Ad esempio, se il ruolo di accesso

per entrambi i segreti ha il relativo ARN assegnato alla variabile `ARN2xsecrets`, puoi impostare le impostazioni dell'ARN come segue:

```
SecretsManagerAccessRoleArn = ARN2xsecrets;  
SecretsManagerOracleAsmAccessRoleArn = ARN2xsecrets;
```

Per ulteriori informazioni sulla creazione di questi valori, consulta [Utilizzo di AWS Management Console per creare un ruolo di accesso segreto e segreto](#).

Dopo aver creato e specificato le impostazioni necessarie per l'endpoint con il ruolo di accesso al segreto e il segreto, aggiorna le autorizzazioni sugli account utente che eseguono la richiesta API `CreateEndpoint` o `ModifyEndpoint` con questi dettagli del segreto. Assicurati che queste autorizzazioni dell'account includano l'`IAM:GetRole` autorizzazione sul ruolo di accesso segreto e l'`SecretsManager:DescribeSecret` autorizzazione sul segreto. AWS DMS richiede queste autorizzazioni per convalidare sia il ruolo di accesso che il relativo segreto.

Per fornire e verificare le autorizzazioni utente richieste

1. Accedi a AWS Management Console e apri la AWS Identity and Access Management console all'indirizzo. <https://console.aws.amazon.com/iam/>
2. Scegli Utenti, quindi seleziona l'ID utente utilizzato per effettuare le chiamate API `CreateEndpoint` e `ModifyEndpoint`.
3. Nella scheda Autorizzazioni scegli `{}` JSON.
4. Assicurati che l'utente disponga delle autorizzazioni mostrate di seguito.

```
{  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": [  
      "iam:GetRole",  
      "iam:PassRole"  
    ],  
    "Resource": "SECRET_ACCESS_ROLE_ARN"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "secretsmanager:DescribeSecret",
```

```
"Resource": "SECRET_ARN"
}
]
}
```

5. Se l'utente non dispone di tali autorizzazioni, aggiungile.
6. Se utilizzi un ruolo IAM per effettuare chiamate API DMS, ripeti i passaggi precedenti per il rispettivo ruolo.
7. Apri un terminale e usa il AWS CLI per verificare che le autorizzazioni siano state fornite correttamente assumendo il ruolo o l'utente usato sopra.
 - a. Convalida l'autorizzazione dell'utente sull' SecretAccessRole utilizzo del comando IAM.
get-role

```
aws iam get-role --role-name ROLE_NAME
```

Sostituisci *ROLE_NAME* con il nome di SecretsManagerAccessRole.

Se il comando restituisce un messaggio di errore, assicurati che le autorizzazioni siano state specificate correttamente.

- b. Convalida l'autorizzazione dell'utente per il segreto utilizzando il comando Secrets Manager describe-secret.

```
aws secretsmanager describe-secret --secret-id SECRET_NAME OR SECRET_ARN --  
region=REGION_NAME
```

L'utente può essere il nome descrittivo, l'ARN parziale o l'ARN completo. Per ulteriori informazioni, consulta [describe-secret](#).

Se il comando restituisce un messaggio di errore, assicurati che le autorizzazioni siano state specificate correttamente.

Utilizzo di AWS Management Console per creare un ruolo di accesso segreto e segreto

È possibile utilizzare il per AWS Management Console creare un segreto per l'autenticazione degli endpoint e per creare la politica e il ruolo che consentano l'accesso AWS DMS al segreto per conto dell'utente.

Per creare un segreto utilizzando il comando AWS Management Console that AWS DMS can use per autenticare un database per le connessioni agli endpoint di origine e di destinazione

1. Accedi a AWS Management Console e apri la AWS Secrets Manager console all'indirizzo. <https://console.aws.amazon.com/secretsmanager/>
2. Scegli Archivia un nuovo segreto.
3. Nella pagina Archivia un nuovo segreto scegli Altro tipo di segreti in Seleziona il tipo di segreto quindi scegli Testo in chiaro.

Note

Questa è l'unica richiesta di inserimento delle credenziali con testo in chiaro per stabilire d'ora in avanti la connessione al database degli endpoint.

4. Nel campo Testo in chiaro:
 - Per un segreto di cui assegni l'identità a `SecretsManagerSecretId`, immetti la seguente struttura JSON.

```
{
  "username": db_username,
  "password": db_user_password,
  "port": db_port_number,
  "host": db_server_name
}
```

Note

Questo è l'elenco minimo dei membri JSON necessari per autenticare il database degli endpoint. Puoi aggiungere tutte le impostazioni degli endpoint JSON che desideri

come membri JSON usando solo lettere minuscole. Tuttavia, AWS DMS ignora gli eventuali membri JSON aggiuntivi per l'autenticazione dell'endpoint.

Qui *db_username* è il nome dell'utente che accede al database, *db_user_password* è la password dell'utente del database, *db_port_number* è il numero di porta per accedere al database e *db_server_name* è il nome (indirizzo) del server di database sul Web, come nell'esempio seguente.

```
{
  "username": "admin",
  "password": "some_password",
  "port": "8190",
  "host": "oracle101.abcdefghij.us-east-1.rds.amazonaws.com"
}
```

- Per un segreto di cui assegni l'identità a `SecretsManagerOracleAsmSecretId`, immetti la seguente struttura JSON.

```
{
  "asm_user": asm_username,
  "asm_password": asm_user_password,
  "asm_server": asm_server_name
}
```

Note

Questo è l'elenco minimo dei membri JSON necessari per autenticare Oracle ASM per un endpoint Oracle. È anche l'elenco completo che è possibile specificare in base alle impostazioni degli endpoint Oracle ASM disponibili.

Qui *asm_username* è il nome dell'utente che accede a Oracle ASM, *asm_user_password* è la password dell'utente Oracle ASM e *asm_server_name* è il nome (indirizzo) del server Oracle ASM sul Web, inclusa la porta, come nell'esempio seguente.

```
{
  "asm_user": "oracle_asm_user",
  "asm_password": "oracle_asm_password",
}
```

```
"asm_server": "oracle101.abcdefghij.us-east-1.rds.amazonaws.com:8190/+ASM"  
}
```

5. Seleziona una chiave di AWS KMS crittografia per crittografare il segreto. È possibile accettare la chiave di crittografia predefinita creata per il servizio da AWS Secrets Manager o selezionare una AWS KMS chiave creata dall'utente.
6. Specifica un nome per fare riferimento a questo segreto e una descrizione facoltativa. Questo è il nome descrittivo che utilizzi come valore per `SecretsManagerSecretId` o `SecretsManagerOracleAsmSecretId`.
7. Se desideri abilitare la rotazione automatica nel segreto, devi selezionare o creare una AWS Lambda funzione con l'autorizzazione a ruotare le credenziali del segreto come descritto. Tuttavia, prima di impostare la rotazione automatica per utilizzare la funzione Lambda, assicurati che le impostazioni di configurazione della funzione aggiungano al valore della variabile di ambiente `EXCLUDE_CHARACTERS` i seguenti quattro caratteri.

```
;.:+{}
```

AWS DMS non ammette questi caratteri nelle password utilizzate per le credenziali degli endpoint. La configurazione della funzione Lambda per escluderli impedisce ad AWS Secrets Manager di generare questi caratteri come parte dei valori della password ruotate. Dopo aver impostato la rotazione automatica per utilizzare la funzione Lambda, ruota AWS Secrets Manager immediatamente il segreto per convalidare la configurazione segreta.

Note

A seconda della configurazione del motore di database, è possibile che il database non recuperi le credenziali ruotate. In questo caso, è necessario riavviare manualmente l'attività per aggiornare le credenziali.

8. Rivedi e archivia il tuo segreto in AWS Secrets Manager. È quindi possibile cercare ogni segreto in base al relativo nome descrittivo in AWS Secrets Manager, quindi recuperare l'ARN segreto come valore `SecretsManagerOracleAsmSecretId` o, se appropriato, `SecretsManagerSecretId` per autenticare l'accesso alla connessione al database degli endpoint e a Oracle ASM (se utilizzato).

Per creare la politica di accesso segreto e il ruolo su cui impostare **SecretsManagerAccessRoleArn** o **SecretsManagerOracleAsmAccessRoleArn**, che consente di accedere AWS DMSAWS Secrets Manager al segreto appropriato

1. Accedi AWS Management Console e apri la console AWS Identity and Access Management (IAM) all'[indirizzo https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
2. Seleziona Policy, quindi scegli Crea policy.
3. Scegli JSON e inserisci la seguente policy per consentire l'accesso e la decrittografia del tuo segreto.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": secret_arn,
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": kms_key_arn,
    }
  ]
}
```

Qui *secret_arn* è l'ARN del tuo segreto, che puoi ottenere da `SecretsManagerSecretId` o `SecretsManagerOracleAsmSecretId`, come appropriato, e *kms_key_arn* è l'ARN della chiave AWS KMS che stai usando per crittografare il segreto, come nell'esempio seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:us-east-2:123456789012:secret:MySQLTestSecret-qeHamH"
    }
  ]
}
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:kms:us-
east-2:123456789012:key/761138dc-0542-4e58-947f-4a3a8458d0fd"
    }
  ]
}
```

Note

Se si utilizza la chiave di crittografia predefinita creata da AWS Secrets Manager, non è necessario specificare le AWS KMS autorizzazioni per *kms_key_arn*.
Se desideri che la policy fornisca l'accesso a entrambi i segreti, specifica semplicemente un oggetto risorsa JSON aggiuntivo per l'altro *secret_arn*.
Se il segreto si trova in un account diverso, il ruolo `SecretsManagerAccessRoleArn` necessita di una policy aggiuntiva per verificare il segreto tra gli account. Per questi casi d'uso, aggiungi l'azione `secretsmanager:DescribeSecret` alla policy. Per maggiori dettagli sulla configurazione di un segreto per più account, consulta [Autorizzazioni ai AWS segreti di Secrets Manager per gli utenti di un account diverso](#).

4. Rivedi e crea la policy con un nome descrittivo e, facoltativamente, una descrizione.
5. Seleziona Ruoli, quindi scegli Crea ruolo.
6. Per il tipo di entità attendibile, scegli Servizio AWS .
7. Scegli DMS dall'elenco dei servizi come servizio attendibile, quindi seleziona Successivo: Autorizzazioni.
8. Cerca e collega la policy che hai creato nella fase 4, quindi procedi con l'aggiunta di eventuali tag ed esamina il ruolo. A questo punto, modifica le relazioni di trust relative al ruolo in modo da utilizzare il responsabile del servizio AWS DMS regionale come entità affidabile. Questo principale ha il seguente formato.

```
dms.region-name.amazonaws.com
```

Qui *region-name* è il nome della regione, ad esempio us-east-1. Segue quindi un responsabile del servizio AWS DMS regionale per questa regione.

```
dms.us-east-1.amazonaws.com
```

9. Dopo aver modificato l'entità attendibile per il ruolo, crea il ruolo con un nome descrittivo e, facoltativamente, una descrizione. Ora puoi cercare il nuovo ruolo in base al suo nome descrittivo in IAM, quindi recuperare il ruolo ARN come valore `SecretsManagerAccessRoleArn` o `SecretsManagerOracleAsmAccessRoleArn` per autenticare la connessione al database degli endpoint.

Per utilizzare Secrets Manager con un'istanza di replica in una sottorete privata

1. Crea un endpoint VPC con Secrets Manager e annota il DNS per l'endpoint. Per ulteriori informazioni sulla creazione di un endpoint VPC con Secrets Manager, consulta [Connessione a Secrets Manager tramite un endpoint VPC](#) nella Guida per l'utente di AWS Secrets Manager.
2. Collega il gruppo di sicurezza dell'istanza di replica all'endpoint VPC di Secrets Manager.
3. Per le regole di uscita del gruppo di sicurezza dell'istanza di replica, consenti tutto il traffico per la destinazione `0.0.0.0/0`.
4. Imposta l'attributo aggiuntivo di connessione dell'endpoint `secretsManagerEndpointOverride=secretsManager endpoint DNS` per fornire il DNS dell'endpoint VPC di Secrets Manager, come illustrato nell'esempio seguente.

```
secretsManagerEndpointOverride=vpce-1234a5678b9012c-12345678.secretsmanager.eu-west-1.vpce.amazonaws.com
```

Utilizzo di ruoli collegati ai servizi per AWS DMS

AWS Database Migration Service utilizza [ruoli collegati al servizio AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato al servizio è un tipo di ruolo IAM univoco collegato direttamente a AWS DMS. I ruoli collegati ai servizi sono definiti automaticamente da AWS DMS e includono tutte le autorizzazioni richieste dal servizio per eseguire chiamate agli altri servizi AWS per tuo conto.

Un ruolo collegato ai servizi semplifica la configurazione di AWS DMS perché non dovrai più aggiungere manualmente le autorizzazioni necessarie. AWS DMS definisce le autorizzazioni dei

relativi ruoli associati ai servizi e, salvo diversamente definito, AWS DMS potrà assumere solo i propri ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. Questa procedura protegge le risorse di AWS DMS perché impedisce la rimozione involontaria delle autorizzazioni 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 Yes (Sì) nella colonna Service-linked roles (Ruoli collegati ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Ruoli collegati ai servizi per le funzionalità AWS DMS

Argomenti

- [Ruolo collegato al servizio per AWS DMS Fleet Advisor](#)
- [Ruolo collegato ai servizi per AWS DMS serverless](#)

Ruolo collegato al servizio per AWS DMS Fleet Advisor

AWS DMS Fleet Advisor usa il ruolo collegato ai servizi denominato `AWSServiceRoleForDMSFleetAdvisor` per gestire le metriche Amazon CloudWatch.

Questo ruolo collegato ai servizi è collegato alle seguenti policy gestite:

`AWSDMSFleetAdvisorServiceRolePolicy`. Per gli aggiornamenti a questa policy, consulta [AWS politiche gestite per AWS Database Migration Service](#).

Ai fini dell'assunzione, il ruolo collegato ai servizi `AWSServiceRoleForDMSFleetAdvisor` considera attendibili i seguenti servizi:

- `dms-fleet-advisor.amazonaws.com`

La policy delle autorizzazioni del ruolo denominata `AWSDMSFleetAdvisorServiceRolePolicy` consente ad AWS DMS Fleet Advisor di eseguire le seguenti azioni sulle risorse specificate:

- Operazione: `cloudwatch:PutMetricData` su `all AWS resources`

Questa autorizzazione consente ai principali di pubblicare punti dati dei parametri su Amazon CloudWatch. AWS DMS Fleet Advisor richiede questa autorizzazione per visualizzare i grafici con i parametri del database di CloudWatch.

Il seguente esempio di codice mostra la policy `AWSDMSFleetAdvisorServiceRolePolicy` utilizzata per creare il ruolo `AWSDMSFleetAdvisorServiceRolePolicy`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "*",
      "Action": "cloudwatch:PutMetricData",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/DMS/FleetAdvisor"
        }
      }
    }
  ]
}
```

È necessario configurare le autorizzazioni per consentire a un'entità IAM, ad esempio un utente, un gruppo o un ruolo, di creare, modificare o eliminare un ruolo collegato ai servizi. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS DMS Fleet Advisor

Puoi utilizzare la console IAM per creare un ruolo collegato ai servizi con il caso d'uso DMS - Fleet Advisor. In AWS CLI o in AWS API, crea un ruolo collegato ai servizi con il nome di servizio `dms-fleet-advisor.amazonaws.com`. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Assicurati di creare questo ruolo prima di creare un raccoglitore di dati. DMS Fleet Advisor utilizza questo ruolo per visualizzare grafici con le metriche di database nella AWS Management Console. Per ulteriori informazioni, consulta [Creazione di un raccoglitore di dati](#).

Modifica di un ruolo collegato ai servizi per AWS DMS Fleet Advisor

AWS DMS non consente di modificare il ruolo collegato ai servizi `AWSServiceRoleForDMSFleetAdvisor`. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS DMS Fleet Advisor

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato ai servizi prima di poterlo eliminare manualmente.

Note

Se il servizio AWS DMS utilizza tale ruolo quando tenti di eliminare le risorse, è possibile che l'eliminazione non abbia esito positivo. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AWS DMS utilizzate da `AWSServiceRoleForDMSFleetAdvisor`

1. Accedere alla AWS Management Console e aprire la console AWS DMS all'indirizzo <https://console.aws.amazon.com/dms/v2/>.
2. Nel riquadro di navigazione, scegli Raccoglitori di dati in Scopri. Viene visualizzata la pagina Raccoglitori di dati.
3. Scegli il tuo raccoglitore di dati e seleziona Elimina.
4. Per confermare l'eliminazione, inserisci il nome del raccoglitore di dati nel campo di immissione del testo. Quindi, scegli Elimina.

Important

Quando elimini un raccoglitore di dati DMS, DMS Fleet Advisor elimina dall'inventario tutti i database che hai individuato utilizzando questo raccoglitore.

Dopo aver eliminato tutti i raccoglitori di dati, puoi eliminare il ruolo collegato ai servizi.

Per eliminare manualmente il ruolo collegato ai servizi utilizzando IAM

Utilizza la console IAM, la AWS CLI o l'API AWS per eliminare il ruolo collegato al servizio AWSServiceRoleForDMSFleetAdvisor. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Regioni supportate per il ruolo collegati ai servizi AWS DMS Fleet Advisor

AWS DMS Fleet Advisor supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta [Regioni AWS supportate](#).

Ruolo collegato ai servizi per AWS DMS serverless

AWS DMS Serverless utilizza il ruolo collegato al servizio denominato.

AWSServiceRoleForDMSServerless AWS DMS utilizza questo ruolo collegato ai servizi per creare e gestire AWS DMS risorse per tuo conto, come Amazon CloudWatch metrics. AWS DMS utilizza questo ruolo in modo che tu debba occuparti solo delle repliche. Questo ruolo collegato ai servizi è collegato alle seguenti policy gestite: AWSDMSServerlessServiceRolePolicy. Per gli aggiornamenti a questa policy, consulta [AWS politiche gestite per AWS Database Migration Service](#).

Il ruolo AWSServiceRoleForDMSServerless collegato al servizio prevede che i seguenti servizi assumano il ruolo:

- `dms.amazonaws.com`

Il seguente esempio di codice mostra la AWSDMSServerlessServiceRolePolicy politica utilizzata per creare il ruolo. AWSServiceRoleForDMSServerless

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "id0",
      "Effect": "Allow",
      "Action": [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
            "dms:req-tag/ResourceCreatedBy": "DMSServerless"
        }
    },
    {
        "Sid": "id1",
        "Effect": "Allow",
        "Action": [
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationTasks"
        ],
        "Resource": "*"
    },
    {
        "Sid": "id2",
        "Effect": "Allow",
        "Action": [
            "dms:StartReplicationTask",
            "dms:StopReplicationTask",
            "dms>DeleteReplicationTask",
            "dms>DeleteReplicationInstance"
        ],
        "Resource": [
            "arn:aws:dms:*:*:rep:*",
            "arn:aws:dms:*:*:task:*"
        ],
        "Condition": {
            "StringEqualsIgnoreCase": {
                "aws:ResourceTag/ResourceCreatedBy": "DMSServerless"
            }
        }
    },
    {
        "Sid": "id3",
        "Effect": "Allow",
        "Action": [
            "dms:TestConnection",
            "dms>DeleteConnection"
        ],
        "Resource": [
            "arn:aws:dms:*:*:rep:*",
            "arn:aws:dms:*:*:endpoint:*"
        ]
    }
]
```

```
}  
]  
}
```

È necessario configurare le autorizzazioni per consentire a un'entità IAM, ad esempio un utente, un gruppo o un ruolo, di creare, modificare o eliminare un ruolo collegato ai servizi. Per ulteriori informazioni, consulta [Autorizzazioni del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per AWS DMS serverless

Quando si crea una replica, AWS DMS serverless crea a livello di codice un ruolo collegato a un servizio AWS DMS serverless. Puoi visualizzare questo ruolo nella console IAM. Puoi anche scegliere di creare questo ruolo manualmente. Per creare il ruolo manualmente, utilizza la console IAM per creare un ruolo collegato al servizio con lo use case DMS. Nella AWS CLI o nell' AWS API, crea un ruolo collegato al servizio utilizzando `dms.amazonaws.com` for the service name. Per ulteriori informazioni, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM. Se elimini il ruolo collegato ai servizi, puoi utilizzare lo stesso processo per crearlo nuovamente.

Note

Se elimini un ruolo mentre sono presenti repliche nel tuo account, la replica genera un errore.

Modifica di un ruolo collegato ai servizi per AWS DMS serverless

AWS DMS non consente di modificare il ruolo collegato al `AWSServiceRoleForDMSServerless` servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Puoi tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato ai servizi per AWS DMS serverless

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Note

Se il AWS DMS servizio utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare AWS DMS le risorse utilizzate da AWSServiceRoleForDMSServerless

1. Accedere AWS Management Console e aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Nel riquadro di navigazione scegli Serverless in Scopri. Viene visualizzata la pagina Serverless.
3. Seleziona la replica serverless e scegli Elimina.
4. Per confermare l'eliminazione, inserisci il nome della replica serverless nel campo di immissione del testo. Quindi, scegli Elimina.

Dopo aver eliminato tutte le repliche serverless, puoi eliminare il ruolo collegato ai servizi.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo AWSServiceRoleForDMSServerless collegato al servizio. Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi AWS DMS serverless

AWS DMS Serverless supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile.

Risoluzione dei problemi relativi AWS Database Migration Service all'identità e all'accesso

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con un AWS DMS IAM.

Argomenti

- [Non sono autorizzato a eseguire alcuna azione in AWS DMS](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)

- [Sono un amministratore e desidero consentire ad altri di accedere AWS DMS](#)
- [Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS DMS risorse](#)

Non sono autorizzato a eseguire alcuna azione in AWS DMS

Se ti AWS Management Console dice che non sei autorizzato a eseguire un'azione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è la persona da cui si sono ricevuti il nome utente e la password.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` IAM tenta di utilizzare la console per visualizzare i dettagli su un endpoint AWS DMS ma non dispone `dms:DescribeEndpoint` delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
dms:DescribeEndpoint on resource: my-postgresql-target
```

In questo caso, Mateo chiede al suo amministratore di aggiornare le sue policy per poter accedere alla risorsa dell'endpoint `my-postgresql-target` mediante l'operazione `dms:DescribeEndpoint`.

Non sono autorizzato a eseguire `iam:PassRole`

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS DMS.

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.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS DMS. Tuttavia, l'operazione 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.

Sono un amministratore e desidero consentire ad altri di accedere AWS DMS

Per consentire ad altri di accedere AWS DMS, devi creare un'entità IAM (utente o ruolo) per la persona o l'applicazione che necessita dell'accesso. Tale utente o applicazione utilizzerà le credenziali dell'entità per accedere ad AWS. Dovrai quindi collegare all'entità una policy che conceda le autorizzazioni corrette in AWS DMS.

Per iniziare immediatamente, consulta [Creazione dei primi utenti e gruppi delegati IAM](#) nella Guida per l'utente di IAM.

Voglio consentire a persone esterne al mio AWS account di accedere alle mie AWS DMS risorse

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 degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se AWS DMS supporta queste funzionalità, consulta [Come AWS Database Migration Service funziona con IAM](#).
- Per scoprire 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 IAM.
- Per scoprire la differenza tra l'utilizzo di ruoli e politiche basate sulle risorse per l'accesso tra account diversi, consulta [Cross Account Resource Access in IAM nella IAM User Guide](#).

Autorizzazioni IAM necessarie per utilizzare AWS DMS

Utilizza autorizzazioni IAM e ruoli IAM determinati per usare AWS DMS. Se hai effettuato l'accesso come utente IAM e desideri utilizzarla AWS DMS, l'amministratore dell'account deve allegare la policy descritta in questa sezione all'utente, al gruppo o al ruolo IAM che utilizzi per eseguire. AWS DMS Per ulteriori informazioni sulle autorizzazioni IAM, consulta la [Guida per l'utente di IAM](#).

La seguente policy fornisce l'accesso AWS DMS e le autorizzazioni per determinate azioni necessarie da altri servizi Amazon come IAM AWS KMS, Amazon EC2 e Amazon. CloudWatch CloudWatch monitora la AWS DMS migrazione in tempo reale e raccoglie e tiene traccia delle metriche che indicano lo stato di avanzamento della migrazione. È possibile utilizzare CloudWatch Logs per eseguire il debug dei problemi relativi a un'attività.

Note

È possibile limitare ulteriormente l'accesso alle AWS DMS risorse utilizzando i tag. Per ulteriori informazioni sulla limitazione dell'accesso alle AWS DMS risorse mediante l'uso di tag, consulta. [Controllo granulare degli accessi tramite i nomi e i tag delle risorse](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "dms:*",
      "Resource": "arn:aws:dms:region:account:resourcetype/id"
    },
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListAliases",
        "kms:DescribeKey"
      ],
      "Resource": "arn:aws:service:region:account:resourcetype/id"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:Get*",
        "cloudwatch:List*"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
},
{
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
]
}
```

L'analisi di queste autorizzazioni seguenti potrebbe aiutarti a comprendere meglio il motivo per cui ciascuna di esse è necessaria.

La sezione seguente è necessaria per consentire all'utente di chiamare le operazioni AWS DMS API.

```
{
    "Effect": "Allow",
    "Action": "dms:*",
    "Resource": "arn:aws:dms:region:account:resourcetype/id"
}
```

La sezione seguente è necessaria per consentire all'utente di elencare le AWS KMS chiavi e gli alias disponibili per la visualizzazione nella console. Questa voce non è obbligatoria se conosci l'Amazon Resource Name (ARN) per la chiave KMS e stai utilizzando solo il AWS Command Line Interface (CLI).

```
{
    "Effect": "Allow",
    "Action": [
        "kms:ListAliases",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

La seguente sezione è necessaria per determinati tipi di endpoint che richiedono il trasferimento dell'ARN del ruolo IAM con l'endpoint. Inoltre, se i AWS DMS ruoli richiesti non vengono creati in anticipo, la AWS DMS console può creare il ruolo. Se tutti i ruoli sono configurati in anticipo, tutto ciò di cui hai bisogno è `iam:GetRole` e `iam:PassRole`. Per ulteriori informazioni sui ruoli, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

```
{
    "Effect": "Allow",
    "Action": [
        "iam:GetRole",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
    ],
    "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

La sezione seguente è necessaria perché è AWS DMS necessario creare l'istanza Amazon EC2 e configurare la rete per l'istanza di replica creata. Queste risorse esistono nell'account del cliente, perciò è necessaria la possibilità di eseguire tali azioni per conto del cliente.

```
{
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeVpcs",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeSubnets",
    "ec2:DescribeSecurityGroups",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:CreateNetworkInterface",
    "ec2>DeleteNetworkInterface"
  ],
  "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

La seguente sezione è necessaria per consentire all'utente di visualizzare i parametri dell'istanza di replica.

```
{
  "Effect": "Allow",
  "Action": [
    "cloudwatch:Get*",
    "cloudwatch:List*"
  ],
  "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

Questa sezione è necessaria per consentire all'utente di visualizzare i log della replica.

```
{
  "Effect": "Allow",
  "Action": [
    "logs:DescribeLogGroups",
    "logs:DescribeLogStreams",
    "logs:FilterLogEvents",
    "logs:GetLogEvents"
  ],
  "Resource": "arn:aws:service:region:account:resourcetype/id"
}
```

```
}
```

La AWS DMS console crea diversi ruoli che vengono automaticamente collegati all' AWS account quando si utilizza la AWS DMS console. Se utilizzi AWS Command Line Interface (AWS CLI) o l' AWS DMS API per la migrazione, devi aggiungere questi ruoli al tuo account. Per ulteriori informazioni sull'aggiunta di questi ruoli, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and

Se utilizzi l'API AWS CLI o l' AWS DMS API per la migrazione del database, devi aggiungere tre ruoli IAM al tuo AWS account prima di poter utilizzare le funzionalità di AWS DMS. Due di questi sono `dms-vpc-role` e `dms-cloudwatch-logs-role`. Se utilizzi Amazon Redshift come database di destinazione, devi anche aggiungere il ruolo IAM `dms-access-for-endpoint` al tuo AWS account.

Gli aggiornamenti alle policy gestite sono automatici. Se stai usando una policy personalizzata con i ruoli IAM, assicurati di controllare periodicamente gli aggiornamenti per la policy gestita in questa documentazione. È possibile visualizzare i dettagli della policy gestita utilizzando una combinazione dei comandi `get-policy` e `get-policy-version`.

Ad esempio, il comando `get-policy` seguente recupera le informazioni sul ruolo IAM specificato.

```
aws iam get-policy --policy-arn arn:aws:iam::aws:policy/service-role/
AmazonDMSVPCManagementRole
```

Le informazioni restituite dal comando sono le seguenti.

```
{
  "Policy": {
    "PolicyName": "AmazonDMSVPCManagementRole",
    "Description": "Provides access to manage VPC settings for AWS managed customer
configurations",
    "CreateDate": "2015-11-18T16:33:19Z",
    "AttachmentCount": 1,
    "IsAttachable": true,
    "PolicyId": "ANPAJHKIGMBQI4AEFFSY0",
    "DefaultVersionId": "v3",
    "Path": "/service-role/",
    "Arn": "arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole",
    "UpdateDate": "2016-05-23T16:29:57Z"
  }
}
```

Il comando `get-policy-version` seguente recupera le informazioni sulla policy IAM.

```
aws iam get-policy-version --policy-arn arn:aws:iam::aws:policy/service-role/  
AmazonDMSVPCManagementRole --version-id v3
```

Le informazioni restituite dal comando sono le seguenti.

```
{  
  "PolicyVersion": {  
    "CreateDate": "2016-05-23T16:29:57Z",  
    "VersionId": "v3",  
    "Document": {  
      "Version": "2012-10-17",  
      "Statement": [  
        {  
          "Action": [  
            "ec2:CreateNetworkInterface",  
            "ec2:DescribeAvailabilityZones",  
            "ec2:DescribeInternetGateways",  
            "ec2:DescribeSecurityGroups",  
            "ec2:DescribeSubnets",  
            "ec2:DescribeVpcs",  
            "ec2>DeleteNetworkInterface",  
            "ec2:ModifyNetworkInterfaceAttribute"  
          ],  
          "Resource": "arn:aws:service:region:account:resourcetype/id",  
          "Effect": "Allow"  
        }  
      ]  
    },  
    "IsDefaultVersion": true  
  }  
}
```

Gli stessi comandi possono essere utilizzati per ottenere informazioni su AmazonDMSCloudWatchLogsRole e sulla policy gestita AmazonDMSRedshiftS3Role.

Note

Se utilizzi la AWS DMS console per la migrazione del database, questi ruoli vengono aggiunti automaticamente al tuo AWS account.

Le procedure seguenti creano i ruoli IAM `dms-vpc-role`, `dms-cloudwatch-logs-role` e `dms-access-for-endpoint`.

Per creare il ruolo `dms-vpc-role` IAM da utilizzare con l' AWS DMS API AWS CLI or

1. Crea un file JSON con la policy IAM seguente. Denominare il file JSON `dmsAssumeRolePolicyDocument.json`.

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

Crea il ruolo AWS CLI utilizzando il comando seguente.

```
aws iam create-role --role-name dms-vpc-role --assume-role-policy-document file://
dmsAssumeRolePolicyDocument.json
```

2. Collegare la policy `AmazonDMSVPCManagementRole` a `dms-vpc-role` utilizzando il comando seguente.

```
aws iam attach-role-policy --role-name dms-vpc-role --policy-arn
arn:aws:iam::aws:policy/service-role/AmazonDMSVPCManagementRole
```

Per creare il ruolo `dms-cloudwatch-logs-role` IAM da utilizzare con l' AWS DMS API AWS CLI or

1. Crea un file JSON con la policy IAM seguente. Denominare il file JSON `dmsAssumeRolePolicyDocument2.json`.

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

Crea il ruolo AWS CLI utilizzando il comando seguente.

```
aws iam create-role --role-name dms-cloudwatch-logs-role --assume-role-policy-
document file://dmsAssumeRolePolicyDocument2.json
```

2. Collegare la policy `AmazonDMSCloudWatchLogsRole` a `dms-cloudwatch-logs-role` utilizzando il comando seguente.

```
aws iam attach-role-policy --role-name dms-cloudwatch-logs-role --policy-arn
arn:aws:iam::aws:policy/service-role/AmazonDMSCloudWatchLogsRole
```

Se utilizzi Amazon Redshift come database di destinazione, è necessario creare il ruolo IAM `dms-access-for-endpoint` per fornire l'accesso ad Amazon S3.

Per creare il ruolo `dms-access-for-endpoint` IAM da utilizzare con Amazon Redshift come database di destinazione

1. Crea un file JSON con la policy IAM seguente. Denominare il file JSON `dmsAssumeRolePolicyDocument3.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Sid": "2",
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Crea il ruolo AWS CLI utilizzando il seguente comando.

```
aws iam create-role --role-name dms-access-for-endpoint --assume-role-policy-document file://dmsAssumeRolePolicyDocument3.json
```

3. Collegare la policy AmazonDMSRedshiftS3Role al ruolo dms-access-for-endpoint utilizzando il comando seguente.

```
aws iam attach-role-policy --role-name dms-access-for-endpoint \  
  --policy-arn arn:aws:iam::aws:policy/service-role/AmazonDMSRedshiftS3Role
```

Ora dovresti disporre delle politiche IAM per utilizzare l' AWS DMS API AWS CLI or.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. Nel AWS, l'impersonificazione tra servizi può portare al confuso problema del vice. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato per utilizzare le proprie autorizzazioni e agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Si consiglia di utilizzare [aws:SourceArn](#) le chiavi di contesto della condizione [aws:SourceAccount](#) globale nelle politiche delle risorse per limitare le autorizzazioni che AWS Database Migration Service forniscono un altro servizio alla risorsa. Se il valore `aws:SourceArn` non contiene l'ID account, ad esempio un nome dell'istanza di replica (ARN) AWS DMS, devi utilizzare entrambe le chiavi di contesto delle condizioni globali per limitare le autorizzazioni. Se si utilizzano entrambe le chiavi di contesto delle condizioni globali e il valore `aws:SourceArn` contiene l'ID account, il valore `aws:SourceAccount` e l'account nel valore `aws:SourceArn` deve utilizzare lo stesso ID account nella stessa dichiarazione di policy. Utilizzare `aws:SourceArn` se si desidera consentire l'associazione di una sola risorsa all'accesso tra servizi. Utilizza `aws:SourceAccount` se desideri consentire l'associazione di qualsiasi risorsa in tale account all'uso tra servizi.

AWS DMS supporta opzioni alternative confuse a partire dalla versione 3.4.7 e successive. Per ulteriori informazioni, consulta [AWS Note di rilascio di Database Migration Service 3.4.7](#). Se l'istanza di replica utilizza AWS DMS 3.4.6 o versione precedente, assicurati di eseguire l'aggiornamento alla versione più recente prima di impostare le opzioni "confused deputy".

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non conosci l'ARN completo della risorsa o scegli più risorse, utilizza la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:dms:*:123456789012:rep:*`.

Argomenti

- [Ruoli IAM da utilizzare con l' AWS DMS API per la prevenzione della confusione tra servizi](#)
- [La policy IAM prevede l'archiviazione delle valutazioni preliminari in Amazon S3 per la prevenzione di "confused deputy" tra servizi](#)

- [Utilizzo di Amazon DynamoDB come endpoint di destinazione per la prevenzione della confusione tra AWS DMS servizi](#)

Ruoli IAM da utilizzare con l' AWS DMS API per la prevenzione della confusione tra servizi

Per utilizzare l'API AWS CLI o l' AWS DMS API per la migrazione del database, devi aggiungere i ruoli `dms-vpc-role` e `dms-cloudwatch-logs-role` IAM al tuo AWS account prima di poter utilizzare le funzionalità di AWS DMS. Per ulteriori informazioni, consulta [Creazione dei ruoli IAM da utilizzare con l' AWS DMS API AWS CLI and](#).

L'esempio seguente mostra le policy per l'utilizzo del ruolo `dms-vpc-role` con l'istanza di replica `my-replication-instance`. Usa queste policy per evitare il problema del "confused deputy".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "your_account_id"
        },
        "ArnEqual": {
          "AWS:SourceArn": "arn:aws:dms:your_region:your_account_id:rep:my-  
replication-instance"
        }
      }
    }
  ]
}
```

La policy IAM prevede l'archiviazione delle valutazioni preliminari in Amazon S3 per la prevenzione di "confused deputy" tra servizi

Per archiviare i risultati della valutazione preliminare nel bucket S3, crea una policy IAM che consenta ad AWS DMS di gestire gli oggetti in Amazon S3. Per ulteriori informazioni, consulta [Creazione di risorse IAM](#).

L'esempio seguente mostra una politica di fiducia con condizioni sostitutive confuse impostate su un ruolo IAM che consente di accedere AWS DMS a tutte le attività e le esecuzioni di valutazione con un account utente specifico.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "your_account_id"
        },
        "ArnLike": {
          "AWS:SourceArn": [
            "arn:aws:dms:your_region:your_account_id:assessment-run:*",
            "arn:aws:dms:region:your_account_id:task:*"
          ]
        }
      }
    }
  ]
}
```

Utilizzo di Amazon DynamoDB come endpoint di destinazione per la prevenzione della confusione tra AWS DMS servizi

Per utilizzare Amazon DynamoDB come endpoint di destinazione per la migrazione del database, devi creare il ruolo IAM che AWS DMS consenta di assumere e concedere l'accesso alle tabelle

DynamoDB. Quindi, usa questo ruolo quando crei l'endpoint DynamoDB di destinazione in AWS DMS. Per ulteriori informazioni, consulta [Utilizzo di Amazon DynamoDB come destinazione](#).

L'esempio seguente mostra una policy di fiducia con condizioni sostitutive confuse impostate su un ruolo IAM che consente a tutti gli AWS DMS endpoint di accedere alle tabelle DynamoDB.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "dms.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "AWS:SourceAccount": "your_account_id"
        },
        "ArnLike": {
          "AWS:SourceArn":
            "arn:aws:dms:your_region:your_account_id:endpoint:*"
        }
      }
    }
  ]
}
```

AWS politiche gestite per AWS Database Migration Service

Argomenti

- [AWS politica gestita: AmazonDMSVPC ManagementRole](#)
- [AWS politica gestita: AWSDMSServerlessServiceRolePolicy](#)
- [AWS politica gestita: AmazonDMS CloudWatch LogsRole](#)
- [AWS politica gestita: AWSDMSFleetAdvisorServiceRolePolicy](#)
- [AWS DMS aggiornamenti alle politiche AWS gestite](#)

AWS politica gestita: AmazonDMSVPC ManagementRole

Questa politica è allegata al `dms-vpc-role` ruolo, che consente di eseguire azioni AWS DMS per tuo conto.

Questa politica concede le autorizzazioni dei contributori che consentono di gestire le risorse AWS DMS di rete.

Dettagli dell'autorizzazione

Questa politica include le seguenti operazioni:

- `ec2:CreateNetworkInterface`— AWS DMS necessita di questa autorizzazione per creare interfacce di rete. Queste interfacce sono essenziali per consentire all'istanza di AWS DMS replica di connettersi ai database di origine e di destinazione.
- `ec2:DescribeAvailabilityZones`— Questa autorizzazione consente di AWS DMS recuperare informazioni sulle zone di disponibilità in una regione. AWS DMS utilizza queste informazioni per garantire la ridondanza e la disponibilità delle risorse nelle zone corrette.
- `ec2:DescribeInternetGateways`— AWS DMS potrebbe richiedere questa autorizzazione per comprendere i gateway Internet configurati nel VPC. Queste informazioni sono fondamentali se l'istanza o i database di replica richiedono l'accesso a Internet.
- `ec2:DescribeSecurityGroups`— I gruppi di sicurezza controllano il traffico in entrata e in uscita verso istanze e risorse. AWS DMS deve descrivere i gruppi di sicurezza per configurare correttamente le interfacce di rete e garantire una comunicazione adeguata tra l'istanza di replica e i database.
- `ec2:DescribeSubnets`— Questa autorizzazione consente di AWS DMS elencare le sottoreti in un VPC. AWS DMS utilizza queste informazioni per avviare le istanze di replica nelle sottoreti appropriate, assicurando che abbiano la connettività di rete necessaria.
- `ec2:DescribeVpcs`— La descrizione dei VPC è essenziale per comprendere l'ambiente di rete in cui AWS DMS risiedono l'istanza di replica e i database. Ciò include la conoscenza dei blocchi CIDR e di altre configurazioni specifiche del VPC.
- `ec2>DeleteNetworkInterface`— AWS DMS necessita di questa autorizzazione per ripulire le interfacce di rete che ha creato una volta che non sono più necessarie. Questo aiuta nella gestione delle risorse ed evita costi inutili.
- `ec2:ModifyNetworkInterfaceAttribute`— Questa autorizzazione è necessaria per AWS DMS modificare gli attributi delle interfacce di rete che gestisce. Ciò potrebbe includere la regolazione delle impostazioni per garantire la connettività e la sicurezza.

- `ec2:DescribeDhcpOptions`— AWS DMS recupera i dettagli del set di opzioni DHCP per il VPC specificato. Queste informazioni sono necessarie per configurare correttamente la rete per le istanze di replica.
- `ec2:DescribeNetworkInterfaces`— AWS DMS recupera informazioni sulle interfacce di rete esistenti all'interno del VPC. Queste informazioni sono necessarie AWS DMS per configurare correttamente le interfacce di rete e garantire una connettività di rete adeguata per il processo di migrazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInternetGateways",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politica gestita: `AWSDMSServerlessServiceRolePolicy`

Questa politica è allegata al `AWSServiceRoleForDMSServerless` ruolo, che consente di AWS DMS eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta [Ruolo collegato ai servizi per AWS DMS serverless](#).

Questa politica concede ai collaboratori le autorizzazioni che consentono di gestire le risorse di AWS DMS replica.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- **dms**— Consente ai responsabili di interagire con le risorse. AWS DMS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "id0",
      "Effect": "Allow",
      "Action": [
        "dms:CreateReplicationInstance",
        "dms:CreateReplicationTask"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "dms:req-tag/ResourceCreatedBy": "DMSServerless"
        }
      }
    },
    {
      "Sid": "id1",
      "Effect": "Allow",
      "Action": [
        "dms:DescribeReplicationInstances",
        "dms:DescribeReplicationTasks"
      ],
      "Resource": "*"
    },
    {
      "Sid": "id2",
      "Effect": "Allow",
      "Action": [
        "dms:StartReplicationTask",
        "dms:StopReplicationTask",
        "dms>DeleteReplicationTask",
        "dms>DeleteReplicationInstance"
      ],
      "Resource": [
        "arn:aws:dms:*:*:rep:*",
        "arn:aws:dms:*:*:task:*"
      ]
    }
  ]
}
```

```

        "Condition": {
            "StringEqualsIgnoreCase": {
                "aws:ResourceTag/ResourceCreatedBy": "DMSServerless"
            }
        },
        {
            "Sid": "id3",
            "Effect": "Allow",
            "Action": [
                "dms:TestConnection",
                "dms>DeleteConnection"
            ],
            "Resource": [
                "arn:aws:dms:*:*:rep:*",
                "arn:aws:dms:*:*:endpoint:*"
            ]
        }
    ]
}

```

AWS politica gestita: AmazonDMS CloudWatch LogsRole

Questa politica è allegata al `dms-cloudwatch-logs-role` ruolo, che consente di AWS DMS eseguire azioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS DMS](#).

Questa politica concede le autorizzazioni per i collaboratori che consentono di pubblicare i log AWS DMS di replica nei log. CloudWatch

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- **logs**— Consente ai responsabili di pubblicare i log nei Logs. CloudWatch Questa autorizzazione è necessaria per poter AWS DMS essere utilizzata CloudWatch per visualizzare i registri di replica.

```

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

```

```

    {
      "Sid": "AllowDescribeOnAllLogGroups",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowDescribeOfAllLogStreamsOnDmsTasksLogGroup",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*"
      ]
    },
    {
      "Sid": "AllowCreationOfDmsLogGroups",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:dms-tasks-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:"
      ]
    },
    {
      "Sid": "AllowCreationOfDmsLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
        "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-stream:dms-serverless-*"
      ]
    },
  ],
}

```

```
{
  "Sid": "AllowUploadOfLogEventsToDmsLogStream",
  "Effect": "Allow",
  "Action": [
    "logs:PutLogEvents"
  ],
  "Resource": [
    "arn:aws:logs:*:*:log-group:dms-tasks-*:log-stream:dms-task-*",
    "arn:aws:logs:*:*:log-group:dms-serverless-replication-*:log-
stream:dms-serverless-*"
  ]
}
```

AWS politica gestita: AWSDMSFleetAdvisorServiceRolePolicy

Non puoi collegarti AWSDMSFleetAdvisorServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo legato al servizio che consente a AWS DMS Fleet Advisor di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi per AWS DMS](#).

Questa politica concede le autorizzazioni per i contributori che consentono a AWS DMS Fleet Advisor di pubblicare le metriche di Amazon. CloudWatch

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `cloudwatch`— Consente ai responsabili di pubblicare punti dati metrici su Amazon. CloudWatch Questa autorizzazione è necessaria per consentire a AWS DMS Fleet Advisor di CloudWatch visualizzare grafici con metriche del database.

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

```

    "Effect": "Allow",
    "Resource": "*",
    "Action": "cloudwatch:PutMetricData",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": "AWS/DMS/FleetAdvisor"
      }
    }
  }
}

```

AWS DMS aggiornamenti alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite AWS DMS da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei AWS DMS documenti.

Modifica	Descrizione	Data
ManagementRoleAmazonDMSVPC — Modifica	AWS DMS aggiunti <code>ec2:DescribeDhcpOptions</code> e <code>ec2:DescribeNetworkInterfaces</code> operazioni per consentire la gestione delle impostazioni AWS DMS di rete per tuo conto.	17 giugno 2024
AWSDMSServerlessServiceRolePolicy : nuova policy	AWS DMS ha aggiunto il <code>AWSDMSServerlessServiceRolePolicy</code> ruolo AWS DMS per consentire la creazione e la gestione di servizi per tuo conto, come la pubblicazione delle CloudWatch metriche di Amazon.	22 maggio 2023

Modifica	Descrizione	Data
AmazonDMS CloudWatch LogsRole — Modifica	AWS DMS ha aggiunto l'ARN per le risorse serverless a ciascuna delle autorizzazioni concesse, per consentire il caricamento dei log di replica dalle configurazioni di AWS DMS replica serverless a Logs. CloudWatch	22 maggio 2023
AWS DMS Fleet Advisor ServiceRolePolicy : nuova policy	AWS DMS Fleet Advisor ha aggiunto una nuova politica per consentire la pubblicazione dei punti dati delle metriche su Amazon CloudWatch.	6 marzo 2023
AWS DMS ha iniziato a tenere traccia delle modifiche	AWS DMS ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	6 marzo 2023

Convalida della conformità per AWS Database Migration Service

Revisori di terze parti valutano la sicurezza e la conformità di AWS Database Migration Service come parte di più programmi di conformità di AWS. Sono inclusi i seguenti programmi:

- SOC
- PCI
- ISO
- FedRAMP
- DoD CC SRG
- HIPAA BAA
- MTCS
- CS
- K-ISMS
- ENS High
- OSPAR
- HITRUST CSF

Per un elenco dei servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consulta [Servizi AWS che rientrano nell'ambito del programma di conformità](#). Per informazioni generali, consulta [Programmi per la conformità di AWS](#).

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Downloading reports in AWS artifact](#).

La responsabilità di conformità durante l'utilizzo dei AWS DMS è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWS mette a disposizione le seguenti risorse:

- [Guide Quick Start per la sicurezza e la conformità](#) - Queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- [Architecting for HIPAA security and compliance on Amazon Web Services](#): questo whitepaper descrive come le aziende possono utilizzare AWS per creare applicazioni conformi alla normativa HIPAA.

- [Risorse per la conformità di AWS](#): una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- [AWS Config](#): questo servizio AWS valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti di settore.
- [AWS Security Hub](#): questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza in AWS Database Migration Service

L'infrastruttura globale di AWS è basata su Regioni e zone di disponibilità AWS. AWS Le Regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e velocità effettiva elevata. Con le zone di disponibilità, è possibile progettare e gestire le applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo.

Per ulteriori informazioni sulle Regioni e le Zone di disponibilità AWS, consulta [Infrastruttura globale di AWS](#).

Oltre all'infrastruttura globale AWS, AWS DMS fornisce la disponibilità elevata e il supporto di failover per un'istanza di replica che utilizza un'implementazione Multi-AZ quando scegli l'opzione Multi-AZ .

In un'implementazione multi-AZ, AWS DMS effettua automaticamente il provisioning e mantiene una replica in standby dell'istanza di replica in un'altra zona di disponibilità. L'istanza di replica primaria viene replicata in modo sincrono nella replica di standby. Se l'istanza di replica primaria incorre in un guasto o non risponde, l'istanza di standby riprende tutte le attività in esecuzione con un'interruzione minima. Poiché l'istanza primaria replica costantemente il suo stato sull'istanza di standby, un'implementazione Multi-AZ riscontra una certa riduzione delle prestazioni.

Per ulteriori informazioni sull'utilizzo delle implementazioni Multi-AZ, consulta [Utilizzo di un'istanza di AWS DMS replica](#).

Sicurezza dell'infrastruttura in AWS Database Migration Service

Come servizio gestito, AWS Database Migration Service è protetto dalla sicurezza di rete globale 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.

Utilizza le chiamate API pubblicate di AWS per accedere a AWS DMS 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 qualsiasi posizione di rete. AWS DMS inoltre supporta le policy di accesso basate sulle risorse, che possono specificare limitazioni per azioni e risorse, ad esempio, in base all'indirizzo IP di origine. È inoltre possibile utilizzare le policy AWS DMS per controllare l'accesso da endpoint Amazon VPC o cloud privati virtuali (VPC) specifici. Di fatto, questo isola l'accesso di rete a una risorsa AWS DMS specificata solo dal VPC specifico all'interno della rete AWS. Per ulteriori informazioni sull'utilizzo delle policy di accesso basate su risorse AWS DMS, inclusi gli esempi, consulta [Controllo granulare degli accessi tramite i nomi e i tag delle risorse](#).

Per limitare le comunicazioni con AWS DMS all'interno di un singolo VPC, puoi creare un endpoint di interfaccia VPC che ti consenta di connetterti ad AWS DMS tramite AWS PrivateLink. AWS PrivateLink aiuta a garantire che qualsiasi chiamata ad AWS DMS e i relativi risultati associati rimangano confinati nel VPC specifico per il quale è stato creato l'endpoint di interfaccia. È quindi possibile specificare l'URL per questo endpoint di interfaccia come opzione con ogni comando AWS DMS eseguito utilizzando la AWS CLI o un SDK. In questo modo è possibile garantire che tutte le comunicazioni con AWS DMS rimangano confinate nel VPC e siano altrimenti invisibili sulla rete Internet pubblica.

Per creare un endpoint di interfaccia per accedere a DMS in un singolo VPC

1. Accedere ad AWS Management Console e aprire la console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione scegli Endpoint. Viene visualizzata la pagina Crea endpoint in cui è possibile creare l'endpoint di interfaccia da un VPC ad AWS DMS.
3. Scegli Servizi AWS, quindi cerca e seleziona un valore per Nome del servizio, in questo caso AWS DMS nel seguente modulo.

```
com.amazonaws.region.dms
```

Qui, *region* specifica la regione AWS in cui viene eseguito AWS DMS, ad esempio `com.amazonaws.us-west-2.dms`.

4. Per VPC scegli il VPC da cui creare l'endpoint di interfaccia, ad esempio `vpc-12abcd34`.
5. Scegli un valore per Zona di disponibilità e ID sottorete. Questi valori devono indicare una posizione in cui l'endpoint AWS DMS scelto può essere eseguito, ad esempio `us-west-2a` (`usw2-az1`) e `subnet-ab123cd4`.
6. Scegli Abilita nome DNS per creare l'endpoint con un nome DNS. Questo nome DNS è composto dall'ID dell'endpoint (`vpce-12abcd34efg567hij`) seguito da un trattino e da una stringa casuale (`ab12dc34`). Questi elementi sono separati dal nome del servizio tramite un punto in ordine inverso separato da punti, con `vpce` aggiunto (`dms.us-west-2.vpce.amazonaws.com`).

Un esempio è `vpce-12abcd34efg567hij-ab12dc34.dms.us-west-2.vpce.amazonaws.com`.

7. Per Gruppo di sicurezza scegli un gruppo da usare per l'endpoint.

Quando configuri il gruppo di sicurezza, assicurati di consentire le chiamate HTTPS in uscita. Per ulteriori informazioni, consulta [Creazione dei gruppi di sicurezza](#) nella Guida per l'utente di Amazon VPC.

8. Scegli Accesso completo o un valore personalizzato per Policy. Ad esempio, puoi scegliere una policy personalizzata simile alla seguente che limiti l'accesso dell'endpoint a determinate azioni e risorse.

```
{  
  "Statement": [  
    {  
      "Action": "dms:CreateEndpoint",  
      "Effect": "Deny",  
      "Resource": "*" }  
    ]  
}
```

```
{
  "Action": "dms:*",
  "Effect": "Allow",
  "Resource": "*",
  "Principal": "*"
},
{
  "Action": [
    "dms:ModifyReplicationInstance",
    "dms>DeleteReplicationInstance"
  ],
  "Effect": "Deny",
  "Resource": "arn:aws:dms:us-west-2:<account-id>:rep:<replication-instance-
id>",
  "Principal": "*"
}
]
```

Qui, la policy di esempio consente qualsiasi chiamata API AWS DMS, ad eccezione dell'eliminazione o della modifica di un'istanza di replica specifica.

A questo punto puoi specificare l'opzione di un URL formato utilizzando il nome DNS creato nella fase 6. La specifichi per ogni comando della CLI o operazione API AWS DMS per accedere all'istanza del servizio utilizzando l'endpoint di interfaccia creato. Ad esempio, potrebbe essere necessario eseguire il comando `DescribeEndpoints` della CLI DMS in questo VPC come mostrato di seguito.

```
$ aws dms describe-endpoints --endpoint-url https://vpce-12abcd34efg567hij-
ab12dc34.dms.us-west-2.vpce.amazonaws.com
```

Se abiliti l'opzione DNS privato, non occorre specificare l'URL dell'endpoint nella richiesta.

Per ulteriori informazioni sulla creazione e l'utilizzo di endpoint di interfaccia VPC (inclusa l'attivazione dell'opzione DNS privato), consulta [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida per l'utente di Amazon VPC.

Controllo granulare degli accessi tramite i nomi e i tag delle risorse

Puoi utilizzare nomi e tag di risorse basati su Amazon Resource Names (ARN) per gestire l'accesso alle AWS DMS risorse. Per farlo, occorre definire l'operazione consentita o includere istruzioni condizionali nelle policy IAM.

Utilizzo dei nomi delle risorse per il controllo dell'accesso

È possibile creare un account utente IAM e assegnare una policy in base all'ARN della risorsa AWS DMS .

La seguente policy nega l'accesso all'istanza di AWS DMS replica con l'ARN `arn:aws:dms:us-east-1:152683116:rep:doh67ztoXglixmihkiTV`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dms:*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:dms:us-east-1:152683116:rep:D0H67ZT0XGLIXMIHKITV"
    }
  ]
}
```

Ad esempio, i seguenti comandi hanno esito negativo se la policy è attiva.

```
$ aws dms delete-replication-instance
  --replication-instance-arn "arn:aws:dms:us-
east-1:152683116:rep:D0H67ZT0XGLIXMIHKITV"
```

```
A client error (AccessDeniedException) occurred when calling the
DeleteReplicationInstance
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:DeleteReplicationInstance on resource: arn:aws:dms:us-
east-1:152683116:rep:D0H67ZT0XGLIXMIHKITV
```

```
$ aws dms modify-replication-instance
  --replication-instance-arn "arn:aws:dms:us-
east-1:152683116:rep:D0H67ZT0XGLIXMIHKITV"
```

A client error (AccessDeniedException) occurred when calling the ModifyReplicationInstance operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform: dms:ModifyReplicationInstance on resource: arn:aws:dms:us-east-1:152683116:rep:D0H67ZT0XGLIXMIHKITV

Puoi anche specificare policy IAM che limitano AWS DMS l'accesso agli endpoint e alle attività di replica.

La seguente policy limita l'accesso a un AWS DMS endpoint utilizzando l'ARN dell'endpoint.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dms:*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:dms:us-
east-1:152683116:endpoint:D6E37YBXTNH0A6XRQSZCUGX"
    }
  ]
}
```

Ad esempio, i seguenti comandi hanno esito negativo se la policy che usa l'ARN dell'endpoint è attiva.

```
$ aws dms delete-endpoint
  --endpoint-arn "arn:aws:dms:us-east-1:152683116:endpoint:D6E37YBXTNH0A6XRQSZCUGX"
```

A client error (AccessDeniedException) occurred when calling the DeleteEndpoint operation:


```
User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
  dms:DeleteEndpoint
on resource: arn:aws:dms:us-east-1:152683116:endpoint:D6E37YBXTNH0A6XRQSZCUGX

$ aws dms modify-endpoint
  --endpoint-arn "arn:aws:dms:us-east-1:152683116:endpoint:D6E37YBXTNH0A6XRQSZCUGX"
```

A client error (AccessDeniedException) occurred when calling the ModifyEndpoint operation:

```
User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
  dms:ModifyEndpoint
on resource: arn:aws:dms:us-east-1:152683116:endpoint:D6E37YBXTNH0A6XRQSZCUGX
```

La seguente politica limita l'accesso a un' AWS DMS attività utilizzando l'ARN dell'attività.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dms:*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:dms:us-east-1:152683116:task:U03YR4N47DXH3ATT4YMW0IT"
    }
  ]
}
```

Ad esempio, i seguenti comandi hanno esito negativo se la policy che usa l'ARN dell'attività è attiva.

```
$ aws dms delete-replication-task
  --replication-task-arn "arn:aws:dms:us-
east-1:152683116:task:U03YR4N47DXH3ATT4YMW0IT"
```

A client error (AccessDeniedException) occurred when calling the DeleteReplicationTask operation:

```
User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
  dms>DeleteReplicationTask
```

```
on resource: arn:aws:dms:us-east-1:152683116:task:U03YR4N47DXH3ATT4YMW0IT
```

Utilizzo dei tag per controllare l'accesso

AWS DMS definisce una serie di coppie chiave-valore comuni che sono disponibili per l'uso nelle politiche definite dal cliente senza requisiti di etichettatura aggiuntivi. Per ulteriori informazioni sull'etichettatura AWS DMS delle risorse, vedere. [Assegnazione di tag alle risorse in AWS Database Migration Service](#)

Di seguito sono elencati i tag standard disponibili per l'uso con AWS DMS:

- `aws: CurrentTime` — Rappresenta la data e l'ora della richiesta, permettendo la limitazione dell'accesso in base a criteri temporali.
- `aws: EpochTime` — Questo tag è simile al `CurrentTime` tag `aws:` precedente, tranne per il fatto che l'ora corrente è rappresentata come il numero di secondi trascorsi dall'epoca Unix.
- `aws: MultiFactorAuthPresent` — Questo è un tag booleano che indica se la richiesta è stata firmata o meno tramite l'autenticazione a più fattori.
- `aws: MultiFactorAuthAge` — Fornisce l'accesso all'età del token di autenticazione a più fattori (in secondi).
- `aws:principaltype:` fornisce accesso al tipo di principale (utente, account, utente federato, ecc.) per la richiesta corrente.
- `aws: SourceIp` — Rappresenta l'indirizzo IP di origine dell'utente che emette la richiesta.
- `aws: UserAgent` — Fornisce informazioni sull'applicazione client che richiede una risorsa.
- `aws:userid:` fornisce accesso all'ID dell'utente che invia la richiesta.
- `aws:username:` fornisce accesso al nome dell'utente che invia la richiesta.
- `dms: InstanceClass` — Fornisce l'accesso alle dimensioni di calcolo degli host delle istanze di replica.
- `dms: StorageSize` — Fornisce l'accesso alla dimensione del volume di archiviazione (in GB).

Inoltre, è possibile definire tag personalizzati. I tag definiti dal cliente sono semplici coppie chiave-valore che vengono mantenute nel servizio di tagging. AWS È possibile aggiungerle alle risorse AWS DMS , incluse le istanze di replica, gli endpoint e le attività. Questi tag sono abbinati mediante istruzioni "condizionali" IAM nelle policy e vengono indicati tramite un tag condizionale specifico. Le

chiavi dei tag hanno come prefisso "dms", il tipo di risorsa e il prefisso "tag". Di seguito è illustrato il formato del tag.

```
dms:{resource type}-tag/{tag key}={tag value}
```

Ad esempio, supponi di voler definire una policy che consente solo una chiamata API per un'istanza di replica che contiene il tag "stage=production". La seguente istruzione condizionale corrisponde a una risorsa con un determinato tag.

```
"Condition":
{
  "streq":
  {
    "dms:rep-tag/stage":"production"
  }
}
```

Aggiungi il tag seguente a un'istanza di replica che corrisponde alla condizione di questa policy.

```
stage production
```

Oltre ai tag già assegnati alle AWS DMS risorse, è possibile scrivere anche politiche per limitare le chiavi e i valori dei tag che possono essere applicati a una determinata risorsa. In questo caso, il prefisso del tag è "req".

Ad esempio, la seguente istruzione di policy limita i tag che un utente può assegnare a una determinata risorsa a un elenco specifico di valori consentiti.

```
"Condition":
{
  "streq":
  {
    "dms:rep-tag/stage": [ "production", "development", "testing" ]
  }
}
```

I seguenti esempi di policy limitano l'accesso a una AWS DMS risorsa in base ai tag delle risorse.

La seguente policy limita l'accesso a un'istanza di replica in cui il valore di tag è "Desktop" e la chiave di tag è "Env":

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dms:*"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "dms:rep-tag/Env": [
            "Desktop"
          ]
        }
      }
    }
  ]
}
```

I seguenti comandi hanno esito positivo o negativo in base alla policy IAM che limita l'accesso quando il valore di tag è "Desktop" e la chiave di tag è "Env".

```
$ aws dms list-tags-for-resource
--resource-name arn:aws:dms:us-east-1:152683116:rep:46DH0U7J0JY0JXWDOZNFEN
--endpoint-url http://localhost:8000
{
  "TagList": [
    {
      "Value": "Desktop",
      "Key": "Env"
    }
  ]
}

$ aws dms delete-replication-instance
--replication-instance-arn "arn:aws:dms:us-
east-1:152683116:rep:46DH0U7J0JY0JXWDOZNFEN"
A client error (AccessDeniedException) occurred when calling the
DeleteReplicationInstance
```

```
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:DeleteReplicationInstance on resource: arn:aws:dms:us-
east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN
```

```
$ aws dms modify-replication-instance
  --replication-instance-arn "arn:aws:dms:us-
east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN"
```

A client error (AccessDeniedException) occurred when calling the
ModifyReplicationInstance

```
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:ModifyReplicationInstance on resource: arn:aws:dms:us-
east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN
```

```
$ aws dms add-tags-to-resource
  --resource-name arn:aws:dms:us-east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN
  --tags Key=CostCenter,Value=1234
```

A client error (AccessDeniedException) occurred when calling the AddTagsToResource
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:AddTagsToResource on resource: arn:aws:dms:us-
east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN

```
$ aws dms remove-tags-from-resource
  --resource-name arn:aws:dms:us-east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN
  --tag-keys Env
```

A client error (AccessDeniedException) occurred when calling the
RemoveTagsFromResource

```
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:RemoveTagsFromResource on resource: arn:aws:dms:us-
east-1:152683116:rep:46DHOU7J0JY0JXWDOZNFEN
```

La seguente policy limita l'accesso a un AWS DMS endpoint in cui il valore del tag è «Desktop» e la chiave del tag è «Env».

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

```

        "dms:*"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "dms:endpoint-tag/Env": [
                "Desktop"
            ]
        }
    }
}
]
}

```

I seguenti comandi hanno esito positivo o negativo in base alla policy IAM che limita l'accesso quando il valore di tag è "Desktop" e la chiave di tag è "Env".

```

$ aws dms list-tags-for-resource
  --resource-name arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
{
  "TagList": [
    {
      "Value": "Desktop",
      "Key": "Env"
    }
  ]
}

```

```

$ aws dms delete-endpoint
  --endpoint-arn "arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I"

```

A client error (AccessDeniedException) occurred when calling the DeleteEndpoint operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform: dms:DeleteEndpoint on resource: arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I

```

$ aws dms modify-endpoint
  --endpoint-arn "arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I"

```

```
A client error (AccessDeniedException) occurred when calling the ModifyEndpoint
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:ModifyEndpoint on resource: arn:aws:dms:us-
east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
```

```
$ aws dms add-tags-to-resource
  --resource-name arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
  --tags Key=CostCenter,Value=1234
```

```
A client error (AccessDeniedException) occurred when calling the AddTagsToResource
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:AddTagsToResource on resource: arn:aws:dms:us-
east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
```

```
$ aws dms remove-tags-from-resource
  --resource-name arn:aws:dms:us-east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
  --tag-keys Env
```

```
A client error (AccessDeniedException) occurred when calling the
RemoveTagsFromResource
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:RemoveTagsFromResource on resource: arn:aws:dms:us-
east-1:152683116:endpoint:J2YCZPNGOLF52344IZWA6I
```

La seguente policy limita l'accesso a un'attività di replica in cui il valore di tag è "Desktop" e la chiave di tag è "Env".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "dms:*"
      ],
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "dms:task-tag/Env": [
            "Desktop"
          ]
        }
      }
    }
  ]
}
```

```
    }
  }
]
}
```

I seguenti comandi hanno esito positivo o negativo in base alla policy IAM che limita l'accesso quando il valore di tag è "Desktop" e la chiave di tag è "Env".

```
$ aws dms list-tags-for-resource
  --resource-name arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3
{
  "TagList": [
    {
      "Value": "Desktop",
      "Key": "Env"
    }
  ]
}

$ aws dms delete-replication-task
  --replication-task-arn "arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3"
```

A client error (AccessDeniedException) occurred when calling the DeleteReplicationTask operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform: dms:DeleteReplicationTask on resource: arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3

```
$ aws dms add-tags-to-resource
  --resource-name arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3
  --tags Key=CostCenter,Value=1234
```

A client error (AccessDeniedException) occurred when calling the AddTagsToResource operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform: dms:AddTagsToResource on resource: arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3

```
$ aws dms remove-tags-from-resource
  --resource-name arn:aws:dms:us-east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3
  --tag-keys Env
```



```
A client error (AccessDeniedException) occurred when calling the
  RemoveTagsFromResource
operation: User: arn:aws:iam::152683116:user/dmstestusr is not authorized to perform:
dms:RemoveTagsFromResource on resource: arn:aws:dms:us-
east-1:152683116:task:RB7N24J2XBUPS3RFABZTG3
```

Impostazione di una chiave di crittografia e specificazione delle autorizzazioni AWS KMS

AWS DMS crittografa lo storage utilizzato da un'istanza di replica e le informazioni di connessione all'endpoint. Per crittografare lo storage utilizzato da un'istanza di replica, AWS DMS utilizza una chiave AWS Key Management Service (AWS KMS) univoca per l'account. AWS È possibile visualizzare e gestire questa chiave con. AWS KMS Puoi utilizzare la chiave KMS predefinita nel tuo account (aws/dms) o puoi creare una chiave KMS personalizzata. Per la crittografia, puoi anche utilizzare un'eventuale chiave KMS esistente.

Note

Qualsiasi chiave personalizzata o esistente utilizzata come AWS KMS chiave di crittografia deve essere una chiave simmetrica. AWS DMS non supporta l'uso di chiavi di crittografia asimmetriche. Per ulteriori informazioni sulle chiavi di crittografia simmetriche e asimmetriche, consulta <https://docs.aws.amazon.com/kms/latest/developerguide/symmetric-asymmetric.html> nella Guida per gli sviluppatori di AWS Key Management Service .

La chiave KMS predefinita (aws/dms) viene creata quando avvii per la prima volta un'istanza di replica se non hai selezionato una chiave KMS personalizzata nella sezione Avanzato della pagina Crea istanza di replica. Se utilizzi la chiave KMS predefinita, le sole autorizzazioni da concedere all'account utente IAM utilizzato per la migrazione sono `kms:ListAliases` e `kms:DescribeKey`. Per ulteriori informazioni su come utilizzare la chiave KMS predefinita, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

Per usare una chiave KMS personalizzata, assegna le autorizzazioni per la chiave KMS personalizzata utilizzando una delle opzioni riportate di seguito:

- Aggiungi l'account utente IAM utilizzato per la migrazione come amministratore chiave o utente chiave per la AWS KMS chiave personalizzata. Ciò assicura che le necessarie autorizzazioni AWS KMS vengano concesse all'account utente IAM. Questa operazione si aggiunge alle autorizzazioni IAM che devi concedere all'account utente IAM per l'utilizzo di AWS DMS. Per ulteriori informazioni sull'assegnazione delle autorizzazioni all'utente di una chiave, consulta [Consente agli utenti della chiave di utilizzare la chiave KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

- Se non desideri aggiungere l'account utente IAM come amministratore della chiave o utente della chiave per la chiave KMS personalizzata, aggiungi le seguenti autorizzazioni aggiuntive alle autorizzazioni IAM che devi concedere all'account utente IAM per l'utilizzo di AWS DMS.

```
{
    "Effect": "Allow",
    "Action": [
        "kms:ListAliases",
        "kms:DescribeKey",
        "kms:CreateGrant",
        "kms:Encrypt",
        "kms:ReEncrypt*"
    ],
    "Resource": "*"
},
```

AWS DMS funziona anche con gli alias delle chiavi KMS. Per ulteriori informazioni sulla creazione delle chiavi AWS KMS e sull'assegnazione agli utenti dell'accesso a una chiave KMS, consulta la [Guida per gli sviluppatori di AWS KMS](#).

Se non specifichi un identificatore di chiave KMS, AWS DMS utilizza la chiave di crittografia predefinita. AWS KMS crea la chiave di crittografia predefinita AWS DMS per il tuo AWS account. Il tuo AWS account ha una chiave di crittografia predefinita diversa per ogni AWS regione.

Per gestire le AWS KMS chiavi utilizzate per crittografare le AWS DMS risorse, utilizza il AWS Key Management Service. AWS KMS combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Utilizzando AWS KMS, è possibile creare chiavi di crittografia e definire le politiche che controllano il modo in cui tali chiavi possono essere utilizzate.

È possibile trovare AWS KMS nel AWS Management Console

1. Accedi AWS Management Console e apri la console AWS Key Management Service (AWS KMS) all'[indirizzo https://console.aws.amazon.com/kms](https://console.aws.amazon.com/kms).
2. Per modificare il Regione AWS, usa il selettore della regione nell'angolo in alto a destra della pagina.
3. Scegliete una delle seguenti opzioni per lavorare con i tasti: AWS KMS

- Per visualizzare le chiavi dell'account che AWS crea e gestisce per te, nel riquadro di navigazione, scegli chiavi AWS gestite.
- Per visualizzare le chiavi nell'account creato e gestito dall'utente, nel riquadro di navigazione, seleziona Chiavi gestite dal cliente.

AWS KMS supporta AWS CloudTrail, in modo da poter controllare l'utilizzo delle chiavi per verificare che le chiavi vengano utilizzate in modo appropriato. AWS KMS Le tue chiavi possono essere utilizzate in combinazione con AWS DMS AWS servizi supportati come Amazon RDS, Amazon S3, Amazon Redshift e Amazon EBS.

Puoi anche creare AWS KMS chiavi personalizzate specificamente per crittografare i dati di destinazione per i seguenti endpoint: AWS DMS

- Amazon Redshift: per ulteriori informazioni, consulta [Creazione e utilizzo delle chiavi AWS KMS per la crittografia dei dati di destinazione Amazon Redshift](#).
- Amazon S3: per ulteriori informazioni, consulta [Creazione di chiavi AWS KMS per la crittografia di oggetti di destinazione Amazon S3](#).

Dopo aver creato le AWS DMS risorse con una chiave KMS, non puoi modificare la chiave di crittografia per tali risorse. Assicurati di determinare i requisiti della chiave di crittografia prima di creare AWS DMS le tue risorse.

Sicurezza di rete per AWS Database Migration Service

I requisiti di sicurezza per la rete che crei durante l'utilizzo AWS Database Migration Service dipendono da come configuri la rete. Le regole generali per la sicurezza della rete per AWS DMS sono le seguenti:

- L'istanza di replica deve avere accesso agli endpoint di origine e di destinazione. Il gruppo di sicurezza per l'istanza di replica deve avere liste di controllo degli accessi di rete o regole che consentono l'uscita dall'istanza sulla porta del database agli endpoint del database.
- Gli endpoint del database devono includere le liste di controllo degli accessi di rete e le regole dei gruppi di sicurezza che consentono l'accesso in entrata dall'istanza di replica. Puoi ottenere tutto questo utilizzando il gruppo di sicurezza dell'istanza di replica, l'indirizzo IP privato, l'indirizzo IP pubblico o l'indirizzo pubblico del gateway NAT, a seconda della configurazione.
- Se la rete utilizza un tunnel VPN, l'istanza Amazon EC2 che agisce come gateway NAT deve utilizzare un gruppo di sicurezza con regole che consentono all'istanza di replica di inviare il traffico attraverso tale tunnel.

Per impostazione predefinita, il gruppo di sicurezza VPC utilizzato dall'istanza di AWS DMS replica dispone di regole che consentono l'uscita a 0.0.0.0/0 su tutte le porte. Se modifichi il gruppo di sicurezza o utilizzi il tuo gruppo di sicurezza, l'uscita deve quantomeno essere consentita verso gli endpoint di origine e di destinazione sulle rispettive porte del database.

Ogni configurazione di rete che puoi utilizzare per la migrazione del database richiede considerazioni di sicurezza specifiche:

- [Configurazione con tutti i componenti di migrazione del database in un VPC](#): il gruppo di sicurezza utilizzato dagli endpoint deve consentire l'ingresso sulla porta del database dall'istanza di replica. Assicurati che il gruppo di sicurezza utilizzato dall'istanza di replica abbia ingresso agli endpoint; in caso contrario, puoi creare una regola nel gruppo di sicurezza utilizzato dagli endpoint, che autorizzi l'indirizzo IP privato dell'accesso all'istanza di replica.
- [Configurazione con più VPC](#): il gruppo di sicurezza utilizzato dall'istanza di replica deve avere una regola per l'intervallo VPC e la porta sul database.
- [Configurazione per una rete verso un VPC utilizzando AWS Direct Connect o una VPN](#): un tunnel VPN che consente il tunneling del traffico dal VPC a una VPN on-premise. In questa configurazione, il VPC include una regola di routing che invia il traffico destinato a un determinato indirizzo IP o intervallo a un host che può eseguire il bridging del traffico dal VPC al VPN locale.

In questo caso, l'host NAT include le proprie impostazioni del gruppo di sicurezza che devono consentire il traffico dall'indirizzo IP privato o dal gruppo di sicurezza dell'istanza di replica all'istanza NAT.

- [Configurazione di una rete per un VPC mediante Internet](#): il gruppo di sicurezza VPC deve includere regole di instradamento che inviano al gateway Internet il traffico non destinato al VPC. In questa configurazione, la connessione all'endpoint viene eseguita dall'indirizzo IP pubblico sull'istanza di replica.
- [Configurazione con un'istanza DB RDS non in un VPC su un'istanza DB in un VPC utilizzando ClassicLink](#)— Quando l'istanza database Amazon RDS di origine o di destinazione non si trova in un VPC e non condivide un gruppo di sicurezza con il VPC in cui si trova l'istanza di replica, è possibile configurare un server proxy e ClassicLink utilizzarlo per connettere i database di origine e di destinazione.
- L'endpoint di origine si trova all'esterno del VPC utilizzato dall'istanza di replica e usa un gateway NAT: puoi configurare un gateway Network Address Translation (NAT) utilizzando un singolo indirizzo IP elastico associato a un'unica interfaccia di rete elastica. Questa interfaccia di rete elastica, riceve quindi un identificatore NAT (nat-#####). Se il VPC include una route predefinita a quel gateway NAT anziché al gateway Internet, l'istanza di replica viene invece visualizzata per contattare l'endpoint del database utilizzando l'indirizzo IP pubblico del gateway Internet. In questo caso, l'ingresso all'endpoint del database all'esterno del VPC deve consentire l'ingresso dall'indirizzo NAT anziché dall'indirizzo IP pubblico dell'istanza di replica.
- Endpoint VPC per motori non RDBMS: AWS DMS non supporta endpoint VPC per motori non RDBMS.

Utilizzo di SSL con AWS Database Migration Service

È possibile crittografare le connessioni per gli endpoint di origine e di destinazione utilizzando il protocollo Secure Sockets Layer (SSL). A tale scopo, puoi utilizzare la console di AWS DMS gestione o l' AWS DMS API per assegnare un certificato a un endpoint. Puoi anche utilizzare la AWS DMS console per gestire i tuoi certificati.

Non tutti i database utilizzano SSL allo stesso modo. L'edizione compatibile con MySQL di Amazon Aurora usa il nome del server, l'endpoint dell'istanza primaria nel cluster, come endpoint per SSL. Un endpoint Amazon Redshift utilizza già una connessione SSL e non richiede la configurazione di tale connessione da parte di AWS DMS. Un endpoint Oracle richiede altri passaggi; per ulteriori informazioni, consulta [Supporto SSL per un endpoint Oracle](#).

Argomenti

- [Limiti per l'utilizzo di SSL con AWS DMS](#)
- [Gestione dei certificati](#)
- [Abilitazione di SSL per un endpoint compatibile con MySQL, PostgreSQL o SQL Server](#)

Per assegnare un certificato a un endpoint, è possibile fornire il certificato root o la catena di certificati CA intermedi che portano al root (come un bundle di certificati), che si utilizza per firmare il certificato SSL del server distribuito sull'endpoint. I certificati vengono accettati solo come file X509 in formato PEM. Quando si importa un certificato, si riceve un Amazon Resource Name (ARN) da utilizzare per specificare quel certificato per un endpoint. Se si utilizza Amazon RDS, è possibile scaricare l'autorità di certificazione (CA) root e il bundle di certificati forniti nel file `rds-combined-ca-bundle.pem` ospitato da Amazon RDS. Per ulteriori informazioni sul download di questo file, consulta [Utilizzo di SSL/TLS per crittografare una connessione a un'istanza database](#) nella Guida per l'utente di Amazon RDS.

È possibile scegliere tra diverse modalità SSL per l'utilizzo della verifica del certificato SSL.

- Nessuno: la connessione non è crittografata. Questa opzione non è sicura, ma richiede un overhead minore.
- Richiedi: la connessione è crittografata tramite SSL (TLS) ma non viene effettuata alcuna verifica CA. Questa opzione è più sicura e richiede un overhead maggiore.
- Verifica CA: la connessione è crittografata. Questa opzione è più sicura e richiede un overhead maggiore. Questa opzione verifica il certificato del server.

- **Verifica completa:** la connessione è crittografata. Questa opzione è più sicura e richiede un overhead maggiore. Questa opzione verifica il certificato del server e verifica che il nome host del server corrisponda all'attributo del nome host del certificato.

Non tutte le modalità SSL sono adatte a tutti gli endpoint del database. La tabella seguente mostra quali modalità SSL sono supportate per ogni motore di database.

Motore database	nessuno	require	verify-ca	verify-full
MySQL/MariaDB/ Amazon Aurora MySQL	Predefinita	Non supportato	Supportato	Supportato
Microsoft SQL Server	Predefinita	Supportato	Non supportato	Supportata
PostgreSQL	Predefinita	Supportato	Supportato	Supportato
Amazon Redshift	Predefinita	SSL non abilitato	SSL non abilitato	SSL non abilitato
Oracle	Predefinita	Non supportato	Supportata	Non supportato
SAP ASE	Predefinita	SSL non abilitato	SSL non abilitato	Supportato
MongoDB	Predefinita	Supportato	Non supportato	Supportata
Db2 LUW	Predefinita	Non supportato	Supportata	Non supportato
Db2 per z/OS	Predefinita	Non supportato	Supportata	Non supportato

Note

L'opzione Modalità SSL della console DMS o dell'API non si applica ad alcuni servizi di flusso di dati e NoSQL, come Kinesis e DynamoDB. Tali servizi sono sicuri per impostazione predefinita, quindi DMS mostra che la modalità SSL non è impostata (Modalità SSL=Nessuno). Per utilizzare SSL non è necessario eseguire alcuna configurazione aggiuntiva per l'endpoint. Ad esempio, l'utilizzo di Kinesis come endpoint di destinazione è

sicuro per impostazione predefinita. Tutte le chiamate API a Kinesis utilizzano SSL, quindi non è necessaria un'opzione SSL aggiuntiva nell'endpoint DMS. È possibile inserire dati e recuperarli in modo sicuro tramite gli endpoint SSL utilizzando il protocollo HTTPS, usato da DMS per impostazione predefinita per la connessione a un flusso di dati Kinesis.

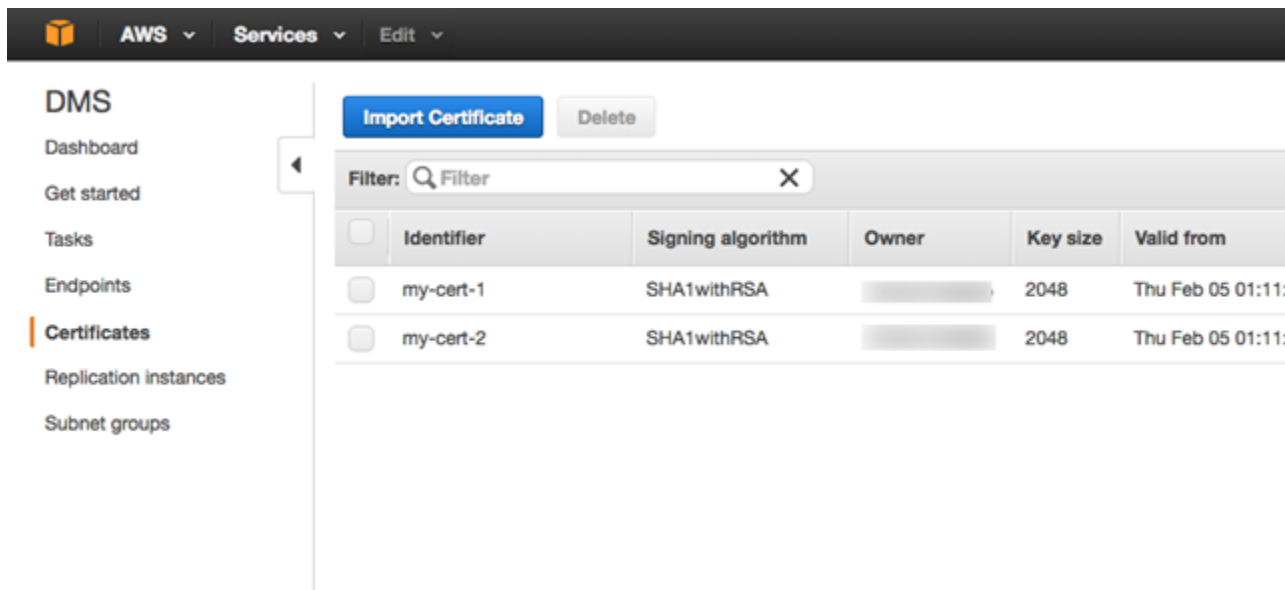
Limiti per l'utilizzo di SSL con AWS DMS

Di seguito sono riportate le limitazioni relative all'uso di SSL con AWS DMS:

- Le connessioni SSL agli endpoint di destinazione di Amazon Redshift non sono supportate. AWS DMS utilizza un bucket Amazon S3 per trasferire dati al database Amazon Redshift. Questa trasmissione è crittografata da Amazon Redshift per impostazione predefinita.
- Possono verificarsi timeout SQL durante l'esecuzione di attività Change Data Capture (CDC) con gli endpoint Oracle abilitati per SSL. Se riscontri questo problema, per cui i contatori CDC non riflettono i numeri attesi, imposta il parametro `MinimumTransactionSize` nella sezione `ChangeProcessingTuning` delle impostazioni delle attività su un valore più basso. Puoi iniziare con un valore minimo di 100. Per ulteriori informazioni sul parametro `MinimumTransactionSize`, vedi [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).
- I certificati possono essere importati solo nei formati `.pem` e `.sso` (wallet Oracle).
- In alcuni casi, il certificato SSL del server può essere firmato da un'autorità di certificazione intermedia (CA). In tal caso, verifica che l'intera catena di certificati che porta dalla CA intermedia fino alla CA root venga importata come un singolo file `.pem`.
- Se utilizzi certificati autofirmati sul tuo server, scegli `require` come modalità SSL. La modalità SSL `require` ritiene implicitamente attendibile il certificato SSL del server e non tenta di convalidare che il certificato è stato firmato da una CA.

Gestione dei certificati

Puoi utilizzare la console DMS per visualizzare e gestire i certificati SSL. La console DMS può essere utilizzata anche per importare i certificati.



Abilitazione di SSL per un endpoint compatibile con MySQL, PostgreSQL o SQL Server

È possibile aggiungere una connessione SSL a un endpoint appena creato o a un endpoint esistente.

Per creare un AWS DMS endpoint con SSL

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/.](https://console.aws.amazon.com/dms/v2/)

Se hai effettuato l'accesso come utente AWS Identity and Access Management (IAM), assicurati di disporre delle autorizzazioni di accesso AWS DMS appropriate. Per ulteriori informazioni sulle autorizzazioni necessarie per la migrazione del database, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Nel riquadro di navigazione, scegliere Certificates (Certificati).
3. Scegliere Import Certificate (Importa certificato).
4. Caricare il certificato da utilizzare per la crittografia della connessione a un endpoint.

Note

Puoi anche caricare un certificato utilizzando la AWS DMS console quando crei o modifichi un endpoint selezionando Aggiungi nuovo certificato CA nella pagina Crea endpoint del database.

Per Aurora serverless come destinazione, ottieni il certificato indicato in [Utilizzo di TLS/SSL con Aurora serverless](#).

5. Creare un endpoint come descritto in [Fase 2: specificazione degli endpoint di origine e di destinazione](#)

Per modificare un AWS DMS endpoint esistente per utilizzare SSL

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni necessarie per la migrazione del database, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Nel riquadro di navigazione, scegliere Certificates (Certificati).
3. Scegliere Import Certificate (Importa certificato).
4. Caricare il certificato da utilizzare per la crittografia della connessione a un endpoint.

Note

Puoi anche caricare un certificato utilizzando la AWS DMS console quando crei o modifichi un endpoint selezionando Aggiungi nuovo certificato CA nella pagina Crea endpoint del database.

5. Nel riquadro di navigazione, scegliere Endpoints (Endpoint), selezionare l'endpoint modificare, quindi scegliere Modify (Modifica).
6. Scegliere un valore per SSL mode (Modalità SSL).

Se si sceglie la modalità verify-ca o verify-full, specificare il certificato che si desidera utilizzare per certificato emesso da una CA, come illustrato di seguito.

Create database endpoint

A database endpoint is used by the replication server to connect to a database. The database specified in the endpoint can be on-prem. Details should be specified in the form below. It is recommended that you test your endpoint connections here to avoid errors during pr

Endpoint type* Source Target ⓘ

Endpoint identifier* ⓘ

Source engine* ⓘ

Server name*

Port*

SSL mode* ⓘ

CA certificate* ⓘ

[Add new CA certificate](#)

User name*

Password*

▶ Advanced

7. Scegli Modifica.
8. Quando l'endpoint è stato modificato, scegliere l'endpoint e scegliere Test connection (Testa la connessione) per verificare che la connessione SSL funzioni.

Dopo aver creato gli endpoint di origine e di destinazione, creare un'attività che utilizza questi endpoint. Per ulteriori informazioni sulla creazione di un'attività, consulta [Fase 3: creazione di un'attività e migrazione dei dati](#).

Modifica della password del database

Nella maggior parte dei casi, la modifica della password del database per l'endpoint di origine o di destinazione è semplice. Se è necessario modificare la password del database per un endpoint che si sta attualmente utilizzando per un'attività di migrazione o replica, il processo richiede alcuni passaggi aggiuntivi. La procedura seguente descrive come farlo.

Per modificare la password del database per un endpoint in un'attività di migrazione o replica

1. [Accedi AWS Management Console e apri la AWS DMS console all'indirizzo https://console.aws.amazon.com/dms/v2/.](https://console.aws.amazon.com/dms/v2/)

Se hai eseguito l'accesso come utente IAM, verifica di disporre delle autorizzazioni appropriate per accedere a AWS DMS. Per ulteriori informazioni sulle autorizzazioni richieste, consulta [Autorizzazioni IAM necessarie per utilizzare AWS DMS](#).

2. Dal riquadro di navigazione, scegli Attività di migrazione del database.
3. Scegliere l'attività che utilizza l'endpoint di cui modificare la password, quindi scegliere Stop (Interrompi).
4. Mentre l'attività è interrotta, è possibile modificare la password del database dell'endpoint utilizzando gli strumenti nativi utilizzati per gestire il database.
5. Tornare alla console di gestione DMS e scegliere Endpoints (Endpoint) dal riquadro di navigazione.
6. Scegliere l'endpoint del database di cui è stata modificata la password, quindi scegliere Modify (Modifica).
7. Digita la nuova password nel riquadro Password, quindi scegli Salva.
8. Dal riquadro di navigazione, scegli Attività di migrazione del database.
9. Scegli l'attività precedentemente interrotta, quindi seleziona Riavvia/Riprendi.
10. Scegli Riavvia o Riprendi, a seconda di come vuoi continuare l'attività, quindi seleziona Avvia attività.

Quote per AWS Database Migration Service

Di seguito sono riportate le quote delle risorse e i vincoli per la denominazione di AWS Database Migration Service (AWS DMS).

La dimensione massima di un database che AWS DMS può migrare dipende da diversi fattori, tra cui l'ambiente di origine, la distribuzione dei dati nel database di origine e il livello di occupazione del sistema di origine.

Il modo migliore per determinare se il tuo sistema specifico è idoneo per l'utilizzo di AWS DMS è testarlo. Esegui l'avvio lentamente per stabilire la configurazione, quindi aggiungi alcuni oggetti complessi. Infine, tenta un pieno carico come test.

Quote di risorse per AWS Database Migration Service

Ogni account AWS prevede delle quote per ciascuna regione AWS per il numero di risorse AWS DMS che è possibile creare. Una volta raggiunta la quota della risorsa, le ulteriori richieste di creazione di tale risorsa restituiranno un errore con un'eccezione.

Nella tabella seguente sono elencate le risorse AWS DMS e le relative quote per regione AWS.

Risorsa	Quota predefinita
Limitazione (della larghezza di banda della rete) delle richieste API	Al massimo 200 richieste al secondo
Frequenza di aggiornamento delle richieste API	8 richieste al secondo
Istanze di replica per account utente	60
Quantità totale di storage per un'istanza di replica	30.000 GB
Sottoscrizioni a eventi per account utente	60
Gruppi di sottoreti di replica per account utente	60
Sottoreti per gruppo di sottoreti di replica	60
Endpoint per account utente	1.000

Risorsa	Quota predefinita
Endpoint per istanza di replica	100
Attività per account utente	600
Attività per istanza di replica	200
Certificati per account utente	100
Provider di dati per account utente	1.000
Profili dell'istanza per account utente	60
Progetti di migrazione per account utente	10
Raccoglitori di dati DMS per account utente	10
Raccomandazioni sulla destinazione generate contemporaneamente	100
Numero di file che il raccoglitore di dati DMS può caricare all'ora	500
Migrazioni di dati omogenee per account utente	600
Migrazioni di dati omogenee eseguite contemporaneamente	100
Migrazioni di dati omogenee per progetto di migrazione	10
Repliche serverless	100

Per ulteriori informazioni sulla quota di limitazione (della larghezza di banda della rete) delle richieste API e sulla frequenza di aggiornamento, consulta [Informazioni sulla limitazione \(della larghezza di banda della rete\) delle richieste API](#).

La quota di 30.000 GB per lo storage si applica a tutte le istanze di replica AWS DMS in una determinata regione AWS. Questo spazio di storage viene utilizzato per memorizzare le modifiche nella cache se la destinazione non è in grado di sostenere il carico dell'origine e per l'archiviazione delle informazioni di log.

Informazioni sulla limitazione (della larghezza di banda della rete) delle richieste API

AWS DMS supporta una quota di richieste API variabile, con il valore massimo di 200 chiamate API al secondo. In altre parole, le tue richieste API vengono limitate quando superano questa velocità. Inoltre, puoi impostare il limite su un minor numero di chiamate API al secondo, a seconda del tempo necessario ad AWS DMS per aggiornare la quota prima di effettuare un'altra richiesta API. Questa quota si applica sia quando esegui le chiamate API direttamente sia quando vengono effettuate per tuo conto nell'ambito dell'utilizzo della Console di gestione AWS DMS.

Per capire come funziona la limitazione (della larghezza di banda della rete) delle richieste API, è utile immaginare che AWS DMS gestisca un bucket di token che tiene traccia delle richieste API. In questo scenario, ogni token del bucket consente di effettuare una singola chiamata API. Non puoi avere più di 200 token contemporaneamente nel bucket. Quando effettui una chiamata API, AWS DMS rimuove un token dal bucket. Se effettui 200 chiamate API in meno di un secondo, il bucket è vuoto e qualsiasi tentativo di effettuare un'altra chiamata API fallisce. Per ogni secondo in cui non effettui una chiamata API, AWS DMS aggiunge 8 token al bucket, fino a un massimo di 200 token. Questa è la frequenza di aggiornamento della richiesta API di AWS DMS. In qualsiasi momento dopo la limitazione (della larghezza di banda della rete), quando i token sono stati aggiunti al tuo bucket, puoi effettuare tante altre chiamate API quanti sono i token disponibili, fino a quando le chiamate non vengono nuovamente limitate.

Se utilizzi la AWS CLI per eseguire le chiamate API limitate, AWS DMS restituisce un errore simile al seguente:

```
An error occurred (ThrottlingException) when calling the AwsDmsApiCall operation (reached max retries: 2): Rate exceeded
```

Qui *AwsDmsApiCall* è il nome dell'operazione API AWS DMS che è stata limitata, ad esempio `DescribeTableStatistics`. È quindi possibile riprovare o effettuare una chiamata diversa dopo un ritardo sufficiente per evitare la limitazione (della larghezza di banda della rete).

Note

A differenza della limitazione (della larghezza di banda della rete) delle richieste API gestita da altri servizi, come Amazon EC2, non è possibile ordinare un aumento delle quote della limitazione delle richieste API gestite da AWS DMS.

Risoluzione dei problemi relativi alle attività di migrazione in AWS Database Migration Service

Di seguito sono disponibili gli argomenti relativi alla risoluzione dei problemi per AWS Database Migration Service (AWS DMS). Questi argomenti ti consentono di risolvere i problemi più comuni utilizzando AWS DMS e i database degli endpoint selezionati.

Se hai aperto un caso del Supporto AWS, il tecnico dell'assistenza può identificare un potenziale problema con una delle configurazioni del database degli endpoint. Il tecnico può anche chiederti di eseguire uno script di supporto per ottenere di diagnostica sul database. Per informazioni dettagliate su come scaricare, eseguire e caricare le informazioni di diagnostica da questo tipo di script di supporto, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Ai fini della risoluzione dei problemi, AWS DMS raccoglie i file di traccia e dump nell'istanza di replica. Puoi fornire questi file a AWS Support nel caso in cui si verifichi un problema che richieda la risoluzione dei problemi. Per impostazione predefinita, DMS elimina i file di traccia e di dump più vecchi di trenta giorni. Per disattivare la raccolta di file trace and dump, apri un caso con AWS Support.

Argomenti

- [Attività di migrazione eseguite lentamente](#)
- [La barra di stato dell'attività non si sposta](#)
- [L'attività è stata completata ma non è stato migrato nulla](#)
- [Indici secondari e chiavi esterne mancanti](#)
- [AWS DMS non crea registri CloudWatch](#)
- [Problemi con la connessione ad Amazon RDS](#)
- [Problemi di rete](#)
- [Blocco del CDC dopo il pieno carico](#)
- [Errori di violazione delle chiavi primarie al riavvio di un'attività](#)
- [Il caricamento iniziale dello schema ha esito negativo](#)
- [Esito negativo delle attività con errore sconosciuto](#)
- [L'attività riavvia il caricamento delle tabelle dall'inizio](#)

- [Il numero di tabelle per attività causa problemi](#)
- [Attività non riuscite durante la creazione della chiave primaria in una colonna LOB](#)
- [Record duplicati nella tabella di destinazione senza chiave primaria](#)
- [Endpoint di origine nell'intervallo IP riservato](#)
- [Timestamp confusi nelle query di Amazon Athena](#)
- [Risoluzione dei problemi con Oracle](#)
- [Risoluzione dei problemi relativi a MySQL](#)
- [Risoluzione dei problemi relativi a PostgreSQL](#)
- [Risoluzione dei problemi relativi a Microsoft SQL Server](#)
- [Risoluzione dei problemi relativi ad Amazon Redshift](#)
- [Risoluzione dei problemi relativi ad Amazon Aurora MySQL](#)
- [Risoluzione dei problemi relativi a SAP ASE](#)
- [Risoluzione dei problemi relativi a IBM Db2](#)
- [Risoluzione dei problemi di latenza in AWS Database Migration Service](#)
- [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#)
- [Utilizzo dell'AMI di supporto AWS DMS diagnostico](#)

Attività di migrazione eseguite lentamente

Sono molteplici i problemi che possono causare l'esecuzione lenta di un'attività di migrazione o il rallentamento delle attività successive rispetto a quella iniziale.

Il motivo più comune per l'esecuzione lenta di un'attività di migrazione è l'allocazione di risorse insufficienti per l'istanza di replica AWS DMS. Per assicurarti che l'istanza disponga di risorse sufficienti per le attività in esecuzione, controlla l'utilizzo di CPU, memoria, file di swap e IOPS dell'istanza di replica. Ad esempio, più attività con Amazon Redshift come endpoint richiedono un utilizzo intensivo di IO. Per una migrazione più efficiente, puoi aumentare gli IOPS per l'istanza di replica o suddividere le attività su più istanze di replica.

Per ulteriori informazioni sulla determinazione delle dimensioni dell'istanza di replica, consulta [Selezione della dimensione migliore per un'istanza di replica](#).

Puoi aumentare la velocità di un carico di migrazione iniziale nel modo seguente:

- Se la destinazione è un'istanza database Amazon RDS, verifica che la configurazione Multi-AZ non sia abilitata per l'istanza database di destinazione.
- Disattiva eventuali backup automatici o la registrazione sul database di destinazione durante il caricamento e attiva nuovamente queste funzionalità una volta completata la migrazione.
- Se la funzionalità è disponibile sulla destinazione, utilizza la capacità di IOPS allocata.
- Se i dati di migrazione contengono LOB, verifica che l'attività sia ottimizzata per la migrazione di LOB. Per ulteriori informazioni sull'ottimizzazione dei LOB, consulta [Impostazioni delle attività dei metadati di destinazione](#).

La barra di stato dell'attività non si sposta

La barra di stato dell'attività fornisce una stima dell'avanzamento dell'attività. La qualità di questa stima dipende dalla qualità delle statistiche della tabella del database di origine; migliori sono le statistiche della tabella, più accurata è la stima.

Per un'attività con una sola tabella che non prevede alcuna statistica delle righe stimate, AWS DMS non è in grado di fornire alcuna stima della percentuale di completamento. In questo caso, utilizza lo stato dell'attività e l'indicazione delle righe caricate per confermare che l'attività è effettivamente in esecuzione e in avanzamento.

L'attività è stata completata ma non è stato migrato nulla

Effettua le seguenti operazioni se non è stato migrato nulla dopo il completamento dell'attività.

- Verifica che l'utente che ha creato l'endpoint abbia accesso in lettura alla tabella che intendi migrare.
- Controlla che l'oggetto che vuoi migrare sia una tabella. Se si tratta di una vista, aggiorna le mappature della tabella e specifica il localizzatore di oggetti come "visualizzazione" o "tutto". Per ulteriori informazioni, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione dalla console](#).

Indici secondari e chiavi esterne mancanti

AWS DMS crea tabelle, chiavi primarie e, in alcuni casi, indici univoci, ma non crea altri oggetti non necessari per migrare in modo efficiente i dati dall'origine. Ad esempio, non crea indici secondari, vincoli di chiavi non primarie o impostazioni predefinite dei dati.

Per eseguire la migrazione di oggetti secondari dal database, utilizza gli strumenti nativi del database in caso di migrazione allo stesso motore di database rispetto al database di origine. Usa AWS Schema Conversion Tool (AWS SCT) se esegui la migrazione di oggetti secondari a un motore di database diverso rispetto a quello impiegato dal database di origine.

AWS DMSnon crea registri CloudWatch

Se l'attività di replica non crea CloudWatch registri, assicurati che il ruolo sia assegnato al tuo account. `dms-cloudwatch-logs-role` Se questo ruolo non è presente, procedi come segue per crearlo:

1. Accedi alla AWS Management Console e apri la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Scegli la scheda Ruoli. Scegli Crea ruolo.
3. Nella sezione Seleziona il tipo di identità attendibile scegli Servizio AWS.
4. Nella sezione Scegli un caso d'uso seleziona DMS.
5. Scegli Successivo: Autorizzazioni.
6. Entra **AmazonDMSCloudWatchLogsRole** nel campo di ricerca e seleziona la casella accanto ad AmazonDMS. CloudWatchLogsRole Ciò concede le AWS DMS autorizzazioni di accesso. CloudWatch
7. Scegliere Next: Tags (Successivo: Tag).
8. Scegliere Next:Review (Successivo: Rivedi).
9. Per Nome ruolo immetti **dms-cloudwatch-logs-role**. Il nome rispetta la distinzione tra maiuscole e minuscole.
10. Scegli Crea ruolo.

Problemi con la connessione ad Amazon RDS

Possono essere diversi i motivi per cui non riesci a connetterti a un'istanza database Amazon RDS che hai impostato come origine o destinazione. Di seguito sono riportati alcuni punti da controllare:

- Verifica che la combinazione nome utente e password sia corretta.
- Verifica che il valore di endpoint mostrato nella console di Amazon RDS per l'istanza sia lo stesso dell'identificatore dell'endpoint che hai utilizzato per creare l'endpoint AWS DMS.

- Verifica che il valore di porta mostrato nella console Amazon RDS per l'istanza corrisponda alla porta assegnata all'endpoint AWS DMS.
- Verifica che il gruppo di sicurezza assegnato all'istanza database di Amazon RDS consenta connessioni dall'istanza di replica AWS DMS.
- Se l'istanza di replica AWS DMS e l'istanza database Amazon RDS non si trovano nello stesso cloud privato virtuale (VPC), verifica che l'istanza database sia accessibile pubblicamente.

Messaggio di errore: Incorrect thread connection string: incorrect thread value 0 (Stringa di connessione del thread errata: valore 0 del thread errato)

Spesso, questo errore si verifica durante il test della connessione a un endpoint. Questo errore indica che la stringa di connessione non è valida. Ad esempio, contiene uno spazio dopo l'indirizzo IP dell'host. Un altro esempio è un carattere non valido copiato nella stringa di connessione.

Problemi di rete

Il problema di rete più comune riguarda il gruppo di sicurezza VPC utilizzato dall'istanza di replica AWS DMS. Per impostazione predefinita, questo gruppo di sicurezza dispone di regole che consentono la configurazione dell'uscita su 0.0.0.0/0 su tutte le porte. In molti casi, si modifica questo gruppo di sicurezza o si utilizza il proprio gruppo di sicurezza. Assicurati almeno di consentire l'uscita agli endpoint di origine e di destinazione sulle rispettive porte del database.

Altri problemi relativi alla configurazione possono essere:

- Istanza di replica ed endpoint di origine e di destinazione nello stesso VPC: il gruppo di sicurezza utilizzato dagli endpoint deve consentire l'ingresso sulla porta del database dall'istanza di replica. Assicurati che il gruppo di sicurezza utilizzato dall'istanza di replica abbia accesso agli endpoint. In alternativa, puoi creare una regola nel gruppo di sicurezza utilizzato dagli endpoint, che autorizzi l'indirizzo IP privato dell'accesso all'istanza di replica.
- L'endpoint di origine è esterno al VPC utilizzato dall'istanza di replica (utilizzando un gateway Internet): il gruppo di sicurezza VPC deve includere le regole di instradamento che inviano al gateway Internet il traffico non destinato al VPC. In questa configurazione, la connessione all'endpoint viene eseguita dall'indirizzo IP pubblico sull'istanza di replica.
- L'endpoint di origine è esterno al VPC utilizzato dall'istanza di replica (utilizzando un gateway NAT): puoi configurare un gateway Network Address Translation (NAT) utilizzando un singolo

indirizzo IP elastico associato a un'unica interfaccia di rete elastica. Questo gateway NAT riceve un identificatore NAT (nat-#####).

In alcuni casi, il VPC include un percorso predefinito verso il gateway NAT anziché il gateway Internet. In questi casi, l'istanza di replica contatta l'endpoint del database utilizzando l'indirizzo IP pubblico del gateway NAT. In questo caso, l'ingresso all'endpoint del database all'esterno del VPC deve consentire l'ingresso dall'indirizzo NAT anziché dall'indirizzo IP pubblico dell'istanza di replica.

Per informazioni sull'uso del server dei nomi on-premise, consulta [Utilizzo del server dei nomi in locale](#).

Blocco del CDC dopo il pieno carico

Il rallentamento o il blocco delle modifiche di replica può verificarsi dopo la migrazione di un caricamento completo se più impostazioni di AWS DMS sono in conflitto tra loro.

Ad esempio, supponi che il parametro Modalità di preparazione della tabella di destinazione sia impostato su Nessuna operazione o Tronca. In questo caso, hai richiesto ad AWS DMS di non eseguire alcuna configurazione sulle tabelle di destinazione, inclusa la creazione di indici primari e unici. Se non hai creato chiavi primarie o univoche sulle tabelle di destinazione, AWS DMS esegue una scansione completa delle tabelle per ogni aggiornamento. Questo approccio può influire in modo significativo sulle prestazioni.

Errori di violazione delle chiavi primarie al riavvio di un'attività

Questo errore può verificarsi quando i dati rimangono nel database di destinazione da un'attività di migrazione precedente. Se l'opzione Modalità di preparazione della tabella di destinazione è impostata su Nessuna operazione, AWS DMS non effettua alcuna preparazione sulla tabella di destinazione, inclusa la pulizia dei dati inseriti da un'attività precedente.

Per riavviare l'attività ed evitare questi errori, rimuovi le righe inserite nelle tabelle di destinazione dalla precedente esecuzione dell'attività.

Il caricamento iniziale dello schema ha esito negativo

In alcuni casi, il caricamento iniziale dello schema potrebbe non riuscire con l'errore `Operation:getSchemaListDetails:errType=, status=0, errMessage=, errDetails=.`

In questi casi, l'account utente utilizzato da AWS DMS per connettersi all'endpoint di origine non dispone delle autorizzazioni necessarie.

Esito negativo delle attività con errore sconosciuto

Le cause dei tipi di errore sconosciuto possono essere diverse. Tuttavia, spesso riscontriamo che il problema riguarda risorse insufficienti allocate all'istanza di replica AWS DMS.

Controlla l'utilizzo di CPU, memoria, file di swap e IOPS dell'istanza di replica per verificare che l'istanza disponga di risorse sufficienti per eseguire la migrazione. Per ulteriori informazioni sul monitoraggio, consulta [Parametri di AWS Database Migration Service](#).

L'attività riavvia il caricamento delle tabelle dall'inizio

AWS DMS riavvia il caricamento delle tabelle dall'inizio quando non ha terminato il caricamento iniziale di una tabella. Quando un'attività viene riavviata, AWS DMS ricarica le tabelle dall'inizio se il caricamento iniziale non è stato completato.

Il numero di tabelle per attività causa problemi

Non è previsto alcun limite per il numero di tabelle per attività di replica. Tuttavia, come regola generale, si consiglia di limitare il numero di tabelle in un'attività a meno di 60.000. Spesso, se una singola attività impiega più di 60.000 tabelle, può verificarsi un sovraccarico delle risorse utilizzate.

Attività non riuscite durante la creazione della chiave primaria in una colonna LOB

In modalità LOB completa o modalità LOB limitata, AWS DMS non supporta la replica delle chiavi primarie che sono tipi di dati LOB.

DMS esegue inizialmente la migrazione di una riga con una colonna LOB come null, quindi aggiorna successivamente la colonna LOB. Pertanto, quando la chiave primaria viene creata su una colonna LOB, l'inserimento iniziale non riesce poiché la chiave primaria non può essere null. Come soluzione alternativa, aggiungi un'altra colonna come chiave primaria e rimuovi la chiave primaria dalla colonna LOB.

Record duplicati nella tabella di destinazione senza chiave primaria

L'esecuzione di un'attività di pieno carico e CDC può creare record duplicati sulle tabelle di destinazione prive di chiave primaria o indice univoco. Per evitare la duplicazione dei record nelle tabelle di destinazione durante le attività di pieno carico e CDC, assicurati che le tabelle di destinazione dispongano di una chiave primaria o di un indice univoco.

Endpoint di origine nell'intervallo IP riservato

Se un database di origine AWS DMS utilizza un indirizzo IP compreso nell'intervallo IP riservato 192.168.0.0/24, il test di connessione dell'endpoint di origine non riesce. La procedura seguente fornisce una possibile soluzione alternativa:

1. Trova un'istanza Amazon EC2 che non si trova nell'intervallo riservato in grado di comunicare al database di origine in 192.168.0.0/24.
2. Installare un proxy socat ed eseguirlo. Di seguito viene riportato un esempio.

```
yum install socat

socat -d -d -lmlocal2 tcp4-listen:database_port,bind=0.0.0.0,reuseaddr,fork
tcp4:source_database_ip_address:database_port
&
```

Utilizza l'indirizzo IP dell'istanza Amazon EC2 e la porta del database indicata in precedenza per l'endpoint AWS DMS. Assicurati che l'endpoint disponga del gruppo di sicurezza che consente la comunicazione con AWS DMS sulla porta del database. Tieni presente che il proxy deve essere in esecuzione per tutta la durata dell'attività DMS. A seconda del caso d'uso, potrebbe essere necessario automatizzare la configurazione del proxy.

Timestamp confusi nelle query di Amazon Athena

Se i timestamp sono confusi nelle query Athena, usa l'[ModifyEndpoint](#) azione AWS Management Console o per impostare il valore per il `parquetTimestampInMilliseconds` tuo endpoint Amazon S3 su `true`. Per ulteriori informazioni, consulta [S3Settings](#).

Risoluzione dei problemi con Oracle

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database Oracle.

Argomenti

- [Estrazione dei dati dalle viste](#)
- [Migrazione di LOB da Oracle 12c](#)
- [Passaggio tra Oracle LogMiner e Binary Reader](#)
- [Errore: Oracle CDC stopped 122301 Oracle CDC maximum retry counter exceeded \(CDC Oracle arrestato 122301 Numero di nuovi tentativi di CDC Oracle superato\).](#)
- [Aggiunta automatica di log supplementare a un endpoint di origine Oracle](#)
- [Le modifiche ai LOB non vengono acquisite](#)
- [Errore: ORA-12899: valore eccessivo per colonna nome-colonna](#)
- [Il tipo di dati NUMBER viene interpretato in modo errato](#)
- [Record mancanti durante il pieno carico](#)
- [Errore della tabella](#)
- [Errore: impossibile recuperare gli ID di destinazione di log redo archiviati da Oracle](#)
- [Valutazione delle prestazioni di lettura dei log redo o di archiviazione di Oracle](#)

Estrazione dei dati dalle viste

Puoi estrarre i dati da una vista una tantum. Non è possibile eseguire l'estrazione per la replica continua. Per poter estrarre i dati dalle viste, è necessario aggiungere il codice seguente alla sezione Impostazioni endpoint nella pagina dell'endpoint di origine Oracle. Quando estrai dati da una vista, quest'ultima viene mostrata come tabella sullo schema di destinazione.

```
"ExposeViews": true
```

Migrazione di LOB da Oracle 12c

AWS DMS può utilizzare due metodi per acquisire le modifiche a un database Oracle, Binary Reader e Oracle LogMiner. Per impostazione predefinita, AWS DMS utilizza Oracle LogMiner per acquisire le modifiche. Tuttavia, su Oracle 12c, Oracle LogMiner non supporta le colonne LOB. Per acquisire le modifiche alle colonne LOB su Oracle 12c, utilizza Binary Reader.

Passaggio tra Oracle LogMiner e Binary Reader

AWS DMS può utilizzare due metodi per acquisire le modifiche a un database Oracle di origine, Binary Reader e Oracle LogMiner. L'impostazione predefinita LogMiner è Oracle. Per passare a utilizzare Binary Reader per l'acquisizione delle modifiche, effettua le seguenti operazioni:

Per utilizzare Binary Reader per l'acquisizione delle modifiche

1. Accedi a AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Endpoint.
3. Seleziona l'endpoint di origine Oracle su cui desideri utilizzare Binary Reader.
4. Scegli Modifica.
5. Seleziona Avanzato, quindi per Attributi aggiuntivi di connessione aggiungi il seguente codice:

```
useLogminerReader=N
```

6. Utilizza uno strumento per sviluppatori Oracle, ad esempio SQL-Plus, per fornire il seguente privilegio aggiuntivo all'account utente AWS DMS impiegato per la connessione all'endpoint Oracle.

```
SELECT ON V_$TRANSPORTABLE_PLATFORM
```

Errore: Oracle CDC stopped 122301 Oracle CDC maximum retry counter exceeded (CDC Oracle arrestato 122301 Numero di nuovi tentativi di CDC Oracle superato).

Questo errore si verifica quando i log di archivio Oracle necessari sono stati rimossi dal server prima che AWS DMS potesse utilizzarli per acquisire le modifiche. Aumenta le policy relative al periodo di conservazione dei log sul server di database. Per un database Amazon RDS, esegui la procedura seguente per aumentare il periodo di conservazione dei log. Ad esempio, il codice seguente aumenta il periodo di conservazione dei log su un'istanza database di Amazon RDS a 24 ore.

```
exec rdsadmin.rdsadmin_util.set_configuration('archivelog retention hours',24);
```

Aggiunta automatica di log supplementare a un endpoint di origine Oracle

Per impostazione predefinita, la funzionalità di log supplementare di AWS DMS è disattivata. Per attivare automaticamente la funzionalità di log supplementare per un endpoint di origine Oracle, effettua le seguenti operazioni:

Per aggiungere automaticamente il log supplementare a un endpoint di origine Oracle

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Endpoint.
3. Seleziona l'endpoint di origine Oracle a cui desideri aggiungere il log supplementare.
4. Scegli Modifica.
5. Seleziona Avanzato, quindi per Attributi aggiuntivi di connessione aggiungi il seguente codice:

```
addSupplementalLogging=Y
```

6. Scegli Modifica.

Le modifiche ai LOB non vengono acquisite

Attualmente, per acquisire le modifiche ai LOB, una tabella deve disporre di una chiave primaria per AWS DMS. Se una tabella contenente LOB non dispone di una chiave primaria, puoi effettuare diverse operazioni per acquisire le modifiche ai LOB:

- Aggiungere una chiave primaria alla tabella. A tale scopo, è sufficiente aggiungere una colonna ID e popolarla con una sequenza mediante un trigger.
- Crea una vista materializzata della tabella che includa un ID generato dal sistema come chiave primaria e migra la vista materializzata anziché la tabella.
- Creare uno standby logico, aggiungere una chiave primaria alla tabella ed eseguire la migrazione dallo standby logico.

Errore: ORA-12899: valore eccessivo per colonna *nome-colonna*

L'errore "ORA-12899: valore eccessivo per colonna *nome-colonna*" è spesso causato da un paio di problemi.

Uno di questi problemi è una mancata corrispondenza tra i set di caratteri utilizzati dai database di origine e di destinazione.

Un altro problema è causato dalle impostazioni NLS (National Language Support) differenti tra i due database. Questo errore si verifica di frequente quando il parametro NLS_LENGTH_SEMANTICS del database di origine è impostato su CHAR e il parametro NLS_LENGTH_SEMANTICS del database di destinazione è impostato su BYTE.

Il tipo di dati NUMBER viene interpretato in modo errato

Il tipo di dati NUMBER di Oracle viene convertito in diversi tipi di dati AWS DMS, a seconda della precisione e del dimensionamento di NUMBER. Queste conversioni sono documentate qui [Tipi di dati di origine per Oracle](#). Il modo in cui il tipo NUMBER viene convertito può essere modificato anche utilizzando le impostazioni degli endpoint per l'endpoint di origine Oracle. Queste impostazioni degli endpoint sono documentate in [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

Record mancanti durante il pieno carico

Quando si esegue un pieno carico, AWS DMS cerca le transazioni aperte a livello di database e attende che il commit della transazione venga completato. Ad esempio, con l'impostazione `TransactionConsistencyTimeout=600` dell'attività, AWS DMS attende 10 minuti anche se la transazione aperta si trova su una tabella non inclusa nella mappatura della tabella. Tuttavia, se la transazione aperta si trova su una tabella inclusa nella mappatura della tabella e il commit della transazione non viene completato in tempo, risulteranno record mancanti nella tabella di destinazione.

Puoi modificare l'impostazione `TransactionConsistencyTimeout` dell'attività e aumentare il tempo di attesa se sai che il commit delle transazioni aperte richiede più tempo.

Inoltre, tieni presente che il valore predefinito dell'impostazione `FailOnTransactionConsistencyBreach` dell'attività è `false`. Ciò significa che AWS DMS continua ad applicare altre transazioni ma le transazioni aperte vengono perse. Se desideri che

l'operazione abbia esito negativo quando le transazioni aperte non vengono chiuse in tempo, puoi impostare `FailOnTransactionConsistencyBreach` su `true`.

Errore della tabella

`Table Error` appare nelle statistiche della tabella durante la replica se una clausola `WHERE` non fa riferimento a una colonna di chiave primaria e il log supplementare non viene utilizzato per tutte le colonne.

Per risolvere questo problema, attiva il log supplementare per tutte le colonne della tabella di riferimento. Per ulteriori informazioni, consulta [Impostazione del log supplementare](#).

Errore: impossibile recuperare gli ID di destinazione di log redo archiviati da Oracle

Questo errore si verifica quando l'origine Oracle non ha generato alcun log di archiviazione o se `V$ARCHIVED_LOG` è vuoto. È possibile risolvere l'errore cambiando i log manualmente.

Per un database Amazon RDS, esegui la procedura seguente per cambiare i file di log. La procedura `switch_logfile` non ha parametri.

```
exec rdsadmin.rdsadmin_util.switch_logfile;
```

Per un database di origine Oracle autogestito, utilizza il comando seguente per forzare un cambio di log.

```
ALTER SYSTEM SWITCH LOGFILE ;
```

Valutazione delle prestazioni di lettura dei log redo o di archiviazione di Oracle

Se riscontri problemi di prestazioni con l'origine Oracle, puoi valutare le prestazioni di lettura dei log redo o di archiviazione di Oracle per trovare i modi per migliorare le prestazioni. Per testare le prestazioni di lettura dei log redo o di archiviazione, usa l'[Amazon machine image \(AMI\) AWS DMS](#).

Puoi utilizzare l'AMI di diagnostica AWS DMS per effettuare le seguenti operazioni:

- Utilizza il metodo `bFile` per valutare le prestazioni dei file di log redo.
- Utilizzate il `LogMiner` metodo per valutare le prestazioni dei redo log file.

- Utilizza il metodo PL/SQL (dbms_lob.read) per valutare le prestazioni dei file di log redo.
- Utilizza il single-thread per valutare le prestazioni di lettura su ASMFile.
- Utilizza il multi-thread per valutare le prestazioni di lettura su ASMFile.
- Utilizza la funzione Direct OS Readfile() Windows o Pread64 Linux per valutare il file di log redo.

Quindi è possibile adottare misure correttive in base ai risultati.

Per testare le prestazioni di lettura di un file di log redo o di archiviazione di Oracle

1. Crea un'istanza AWS DMS AMI di diagnostica Amazon EC2 e connettiti.

Per ulteriori informazioni, consulta [Utilizzo dell'AMI di supporto diagnostico AWS DMS](#).

2. Esegui il comando awsreplperf.

```
$ awsreplperf
```

Il comando visualizza le opzioni dell'utilità AWS DMS per le prestazioni di lettura Oracle.

```
0. Quit
1. Read using Bfile
2. Read using LogMiner
3. Read file PL/SQL (dms_lob.read)
4. Read ASMFile Single Thread
5. Read ASMFile Multi Thread
6. Readfile() function
```

3. Seleziona un'opzione dall'elenco.
4. Immetti le seguenti informazioni sulla connessione al database e sul log di archiviazione.

```
Oracle user name [system]:
Oracle password:

Oracle connection name [orcllx]:
Connection format hostname:port/instance

Oracle event trace? [N]:
Default N = No or Y = Yes

Path to redo or archive log file []:
```

- Esamina l'output visualizzato per le informazioni pertinenti sulle prestazioni di lettura. Ad esempio, quanto segue mostra l'output che può derivare dalla selezione dell'opzione numero 2, Read using LogMiner.

```

Enter your choice>>2
Oracle user name: [system] >> * * *
Oracle password :
Oracle connection name : [orcl1x] >> * * * 0:1521/porcl
Oracle event trace ? : [N] >>n
Full path to redo or archive log file: [ ] >>+EBSFRA/PORCL/ONLINELOG/group_11.1380.1101828345
Elapsed Time : 7044.83973 sec
Read speed in : 0.088575 MB/sec
LogMinerRead: counted 1198389 redo log rows, total undo / redo size : 655073562
  
```

- Per uscire dall'utilità, immetti 0 (zero).

Passaggi successivi

- Quando i risultati mostrano che la velocità di lettura è inferiore a una soglia accettabile, esegui lo [script di supporto diagnostico Oracle](#) sull'endpoint, esamina le sezioni Tempo di attesa, Profilo del carico e Profilo dell'I/O. Quindi modifica qualsiasi configurazione anomala per migliorare le prestazioni di lettura. Ad esempio, se i tuoi file di log redo hanno una dimensione massima di 2 GB, prova ad aumentare LOG_BUFFER a 200 MB per migliorare le prestazioni.
- Consulta [Best practice per AWS DMS](#) per assicurarti che l'istanza di replica DMS, l'attività e gli endpoint siano configurati in modo ottimale.

Risoluzione dei problemi relativi a MySQL

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database MySQL.

Argomenti

- [L'attività CDC ha esito negativo per l'endpoint dell'istanza database di Amazon RDS perché la registrazione binaria è disabilitata](#)
- [Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività](#)
- [Aggiunta di commit automatico a un endpoint compatibile con MySQL](#)
- [Disabilitazione delle chiavi esterne su un endpoint di destinazione compatibile con MySQL](#)
- [Caratteri sostituiti con punto interrogativo](#)
- [Voci di log "Evento errato"](#)

- [Change Data Capture con MySQL 5.5](#)
- [Aumento del periodo di conservazione dei log binari per istanze database di Amazon RDS](#)
- [Messaggio di log: Some changes from the source database had no impact when applied to the target database \(Alcune modifiche dal database di origine non hanno avuto alcun impatto quando applicate al database di destinazione\).](#)
- [Errore: Identifier too long \(Identificatore troppo lungo\)](#)
- [Errore: Unsupported Character Set Causes Field Data Conversion to Fail \(Il set di caratteri non supportato causa l'esito negativo della conversione dei dati di campo\)](#)
- [Errore: Codepage 1252 to UTF8 \[120112\] A field data conversion failed \(Tabella codici 1252 su UTF8 \[120112\] Esito negativo di una conversione dei dati di campo\)](#)
- [Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati](#)

L'attività CDC ha esito negativo per l'endpoint dell'istanza database di Amazon RDS perché la registrazione binaria è disabilitata

Questo problema si verifica con le istanze database di Amazon RDS perché i backup automatici sono disabilitati. Abilita i backup automatici impostando il periodo di retention dei backup su un valore diverso da zero.

Le connessioni a un'istanza MySQL di destinazione vengono disconnesse durante un'attività

Se un'attività con LOB si disconnette da una destinazione MySQL potrebbe essere restituito il seguente tipo di errori nel log dell'attività.

```
[TARGET_LOAD ]E: RetCode: SQL_ERROR SqlState: 08S01 NativeError:
2013 Message: [MySQL][ODBC 5.3(w) Driver][mysqld-5.7.16-log]Lost connection
to MySQL server during query [122502] ODBC general error.
```

```
[TARGET_LOAD ]E: RetCode: SQL_ERROR SqlState: HY000 NativeError:
2006 Message: [MySQL][ODBC 5.3(w) Driver]MySQL server has gone away
[122502] ODBC general error.
```

In questo caso, potresti dover modificare alcune impostazioni delle attività.

Per risolvere il problema relativo alla disconnessione di un'attività da una destinazione MySQL, effettua le seguenti operazioni:

- Verifica che la variabile di database `max_allowed_packet` sia impostata su un valore sufficiente a contenere il LOB di maggiori dimensioni.
- Verifica che le seguenti variabili siano impostate su un valore di timeout di ampia durata. È consigliabile utilizzare un valore di almeno 5 minuti per ciascuna di queste variabili.
 - `net_read_timeout`
 - `net_write_timeout`
 - `wait_timeout`

Per informazioni sull'impostazione delle variabili di sistema MySQL, consulta [Server System Variables](#) nella [documentazione di MySQL](#).

Aggiunta di commit automatico a un endpoint compatibile con MySQL

Per aggiungere il commit automatico a un endpoint di destinazione compatibile con MySQL

1. Accedere AWS Management Console e aprire la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Endpoint.
3. Seleziona l'endpoint di destinazione compatibile con MySQL a cui desideri aggiungere il commit automatico.
4. Scegli Modifica.
5. Seleziona Avanzato, quindi per Attributi aggiuntivi di connessione aggiungi il seguente codice:

```
Initstmt= SET AUTOCOMMIT=1
```

6. Scegli Modifica.

Disabilitazione delle chiavi esterne su un endpoint di destinazione compatibile con MySQL

Puoi disabilitare i controlli delle chiavi esterne su MySQL aggiungendo quanto segue a Attributi aggiuntivi di connessione nella sezione Avanzato dell'endpoint di destinazione MySQL, Amazon Aurora edizione compatibile con MySQL o MariaDB.

Per disabilitare le chiavi esterne su un endpoint di destinazione compatibile con MySQL

1. Accedi AWS Management Console e apri la AWS DMS console all'[indirizzo https://console.aws.amazon.com/dms/v2/](https://console.aws.amazon.com/dms/v2/).
2. Scegli Endpoint.
3. Seleziona l'endpoint di destinazione MySQL, Aurora MySQL o MariaDB su cui desideri disabilitare le chiavi esterne.
4. Scegli Modifica.
5. Seleziona Avanzato, quindi per Attributi aggiuntivi di connessione aggiungi il seguente codice:

```
Initstmt=SET FOREIGN_KEY_CHECKS=0
```

6. Scegli Modifica.

Caratteri sostituiti con punto interrogativo

Questo problema si verifica con maggiore frequenza quando i caratteri dell'endpoint di origine sono stati codificati da un set di caratteri non supportato da AWS DMS.

Voci di log "Evento errato"

In genere, le voci "Evento errato" nei log di migrazione indicano che sull'endpoint del database di origine è stata tentata un'operazione DDL (Data Definition Language) non supportata. Le operazioni DDL non supportate causano un evento che l'istanza di replica non può ignorare, quindi viene registrato un evento errato.

Per risolvere questo problema, riavvia l'attività dall'inizio. Questa operazione ricarica le tabelle e avvia l'acquisizione delle modifiche in un momento successivo all'operazione DDL non supportata.

Change Data Capture con MySQL 5.5

Acquisizione dei dati di modifica (CDC) AWS DMS per database compatibili con Amazon RDS MySQL richiede la registrazione binaria basata su riga dell'immagine completa e tale funzionalità non è supportata in MySQL 5.5 o versioni precedenti. Per utilizzare AWS DMS CDC, devi aggiornare l'istanza database di Amazon RDS a MySQL versione 5.6.

Aumento del periodo di conservazione dei log binari per istanze database di Amazon RDS

AWS DMS richiede la conservazione dei file di log binari per la funzionalità Change Data Capture. Per aumentare il periodo di conservazione dei log su un'istanza database di Amazon RDS, utilizza la seguente procedura. L'esempio seguente consente di aumentare il periodo di conservazione dei log binari a 24 ore.

```
call mysql.rds_set_configuration('binlog retention hours', 24);
```

Messaggio di log: Some changes from the source database had no impact when applied to the target database (Alcune modifiche dal database di origine non hanno avuto alcun impatto quando applicate al database di destinazione).

Quando AWS DMS aggiorna un valore di colonna del database MySQL mantenendo il valore esistente, da MySQL viene restituito un messaggio di `zero rows affected`. Questo comportamento è diverso da altri motori di database come Oracle e SQL Server. Questi motori aggiornano la riga anche quando il valore di sostituzione è lo stesso di quello corrente.

Errore: Identifier too long (Identificatore troppo lungo)

Il seguente errore si verifica quando un identificatore è troppo lungo:

```
TARGET_LOAD E: RetCode: SQL_ERROR SqlState: HY000 NativeError:  
1059 Message: MySQLhttp://ODBC 5.3(w) Driverhttp://mysqld-5.6.10Identifier  
name 'name' is too long 122502 ODBC general error. (ar_odbc_stmt.c:4054)
```

In alcuni casi, si imposta AWS DMS per creare le tabelle e le chiavi primarie nel database di destinazione. In questi casi, DMS non utilizza per le chiavi primarie gli stessi nomi usati nel database di origine. Crea invece il nome della chiave primaria in base al nome della tabella. Se il nome della tabella è lungo, la lunghezza dell'identificatore generato automaticamente può superare i limiti consentiti per MySQL.

Per risolvere questo problema, l'approccio attuale consiste nel creare preventivamente le tabelle e le chiavi primarie nel database di destinazione. Quindi per popolare le tabelle di destinazione utilizza un'attività con l'impostazione Modalità di preparazione della tabella di destinazione impostata su Nessuna operazione o Tronca.

Errore: Unsupported Character Set Causes Field Data Conversion to Fail (Il set di caratteri non supportato causa l'esito negativo della conversione dei dati di campo)

Il seguente errore si verifica quando un set di caratteri non supportato causa l'esito negativo della conversione dei dati di campo:

```
"[SOURCE_CAPTURE ]E: Column 'column-name' uses an unsupported character set [120112]
A field data conversion failed. (mysql_endpoint_capture.c:2154)
```

Controlla i parametri del database correlati alle connessioni. Per impostare questi parametri è possibile utilizzare il seguente comando.

```
SHOW VARIABLES LIKE '%char%';
```

Errore: Codepage 1252 to UTF8 [120112] A field data conversion failed (Tabella codici 1252 su UTF8 [120112] Esito negativo di una conversione dei dati di campo)

Il seguente errore può verificarsi durante una migrazione se nel database MySQL di origine vi sono caratteri non della tabella codici 1252.

```
[SOURCE_CAPTURE ]E: Error converting column 'column_xyz' in table  
'table_xyz with codepage 1252 to UTF8 [120112] A field data conversion failed.  
(mysql_endpoint_capture.c:2248)
```

Come soluzione alternativa, puoi utilizzare l'attributo aggiuntivo di connessione `CharsetMapping` con l'endpoint MySQL di origine per specificare la mappatura del set di caratteri. Potrebbe essere necessario riavviare l'attività di migrazione AWS DMS dall'inizio se si aggiunge questa impostazione dell'endpoint.

Ad esempio, la seguente impostazione dell'endpoint potrebbe essere utilizzata per un endpoint di origine MySQL in cui il set di caratteri di origine è `Utf8` o `latin1`. 65001 è l'identificatore della tabella codici UTF8.

```
CharsetMapping=utf8,65001  
CharsetMapping=latin1,65001
```

Indici, chiavi esterne o aggiornamenti o eliminazioni a cascata non migrati

AWS DMS non supporta la migrazione di oggetti secondari come indici e chiavi esterne. Per replicare le modifiche apportate alle tabelle secondarie da un'operazione di aggiornamento o eliminazione a cascata, è necessario che il vincolo di chiave esterna di attivazione sia abilitato sulla tabella di destinazione. Per aggirare questa limitazione, crea manualmente la chiave esterna nella tabella di destinazione. Quindi, crea una singola attività per il pieno carico e la CDC oppure due attività separate per il pieno carico e la CDC, come descritto di seguito:

Creazione di un'unica attività che supporti pieno carico e CDC

Questa procedura descrive come migrare chiavi esterne e indici utilizzando una singola attività per il pieno carico e la CDC.

Creazione di un'attività di pieno carico e CDC

1. Crea manualmente le tabelle con chiavi esterne e indici sulla destinazione in modo che corrispondano alle tabelle di origine.
2. Aggiungi il seguente un attributo aggiuntivo di connessione all'endpoint di destinazione AWS DMS:

```
Initstmt=SET FOREIGN_KEY_CHECKS=0;
```

3. Crea l'attività AWS DMS con `TargetTablePrepMode` impostato su `DO_NOTHING`.
4. Imposta `Stop task after full load completes` su `StopTaskCachedChangesApplied`.
5. Avvia l'attività. AWS DMS interrompe l'attività automaticamente una volta terminato il pieno carico e applica le modifiche memorizzate nella cache.
6. Rimuovi l'attributo aggiuntivo di connessione `SET FOREIGN_KEY_CHECKS` che hai aggiunto in precedenza.
7. Riprendi l'attività. L'attività entra nella fase CDC e applica le modifiche in corso dal database di origine alla destinazione.

Creazione delle attività di pieno carico e CDC separatamente

Queste procedure descrivono come migrare chiavi esterne e indici utilizzando attività separate per il pieno carico e la CDC.

Creazione di un'attività di pieno carico

1. Crea manualmente le tabelle con chiavi esterne e indici sulla destinazione in modo che corrispondano alle tabelle di origine.
2. Aggiungi il seguente attributo aggiuntivo di connessione all'endpoint di destinazione AWS DMS:

```
Initstmt=SET FOREIGN_KEY_CHECKS=0;
```

3. Crea l'attività AWS DMS con il parametro `TargetTablePrepMode` impostato su `DO_NOTHING` e `EnableValidation` impostato su `FALSE`.
4. Avvia l'attività. AWS DMS interrompe l'attività automaticamente una volta terminato il pieno carico e applica le modifiche memorizzate nella cache.
5. Una volta completata l'attività, annota l'ora di inizio dell'attività di pieno carico in UTC o il nome e la posizione del file di log binario, per avviare l'attività di sola CDC. Fai riferimento ai log per ottenere il timestamp in UTC dall'ora iniziale di avvio del pieno carico.

Creazione di un'attività di sola CDC

1. Rimuovi l'attributo aggiuntivo di connessione SET FOREIGN_KEY_CHECKS che hai impostato in precedenza.
2. Crea l'attività di sola CDC con la posizione di avvio impostata sull'ora di inizio del pieno carico indicata nel passaggio precedente. In alternativa, è possibile utilizzare la posizione del log binario registrata nel passaggio precedente. Imposta TargetTablePrepMode su DO_NOTHING. Abilita la convalida dei dati configurando l'impostazione EnableValidation su TRUE, se necessario.
3. Avvia l'attività di sola CDC e monitora i log per individuare eventuali errori.

Note

Questa soluzione alternativa si applica solo a una migrazione da MySQL a MySQL. Non è possibile utilizzare il metodo con la funzionalità dell'applicazione in batch perché questa richiede che le tabelle di destinazione non abbiano chiavi esterne attive.

Risoluzione dei problemi relativi a PostgreSQL

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database PostgreSQL.

Argomenti

- [I tipi di dati JSON sono troncati](#)
- [Le colonne di un tipo di dati definito dall'utente non vengono migrate correttamente](#)
- [Errore: No schema has been selected to create in \(Nessuno schema selezionato per la creazione\)](#)
- [Le operazioni di eliminazione e aggiornamento su una tabella non vengono replicate mediante CDC](#)
- [Le istruzioni Truncate non vengono propagate](#)
- [Come evitare che PostgreSQL acquisisca DDL](#)
- [Selezione dello schema in cui vengono creati gli oggetti di database per l'acquisizione di DDL](#)
- [Tabelle Oracle mancanti dopo la migrazione a PostgreSQL](#)
- [ReplicationSlotDiskUsage aumenta e restart_Isn smette di andare avanti durante transazioni lunghe, come i carichi di lavoro ETL](#)

- [Un'attività che utilizza la vista come origine non dispone di righe copiate](#)

I tipi di dati JSON sono troncati

AWS DMS considera il tipo di dati JSON in PostgreSQL come una colonna del tipo di dati LOB. Di conseguenza, se utilizzi la modalità LOB limitata, il limite delle dimensioni di LOB si applica ai dati JSON.

Ad esempio, supponi che la modalità LOB limitata sia impostata su 4.096 KB. In questo caso, qualsiasi dato JSON di dimensioni superiori a 4.096 KB viene troncato al limite di 4.096 KB e non supera il test di convalida in PostgreSQL.

Le seguenti informazioni di log indicano il troncamento del file JSON a causa dell'impostazione della modalità LOB limitata e il conseguente esito negativo della convalida.

```
03:00:49
2017-09-19T03:00:49 [TARGET_APPLY ]E: Failed to execute statement:
'UPDATE "public"."delivery_options_quotes" SET "id"=? , "enabled"=? ,
"new_cart_id"=? , "order_id"=? , "user_id"=? , "zone_id"=? , "quotes"=? ,
"start_at"=? , "end_at"=? , "last_quoted_at"=? , "created_at"=? ,
"updated_at"=? WHERE "id"=? ' [1022502] (ar_odbc_stmt
2017-09-19T03:00:49 [TARGET_APPLY ]E: Failed to execute statement:
'UPDATE "public"."delivery_options_quotes" SET "id"=? , "enabled"=? ,
"new_cart_id"=? , "order_id"=? , "user_id"=? , "zone_id"=? , "quotes"=? ,
"start_at"=? , "end_at"=? , "last_quoted_at"=? , "created_at"=? ,
"updated_at"=? WHERE "id"=? ' [1022502] (ar_odbc_stmt.c:2415)
#
03:00:49
2017-09-19T03:00:49 [TARGET_APPLY ]E: RetCode: SQL_ERROR SqlState:
22P02 NativeError: 1 Message: ERROR: invalid input syntax for type json;,
Error while executing the query [1022502] (ar_odbc_stmt.c:2421)
2017-09-19T03:00:49 [TARGET_APPLY ]E: RetCode: SQL_ERROR SqlState:
22P02 NativeError: 1 Message: ERROR: invalid input syntax for type json;,
Error while executing the query [1022502] (ar_odbc_stmt.c:2421)
```


Le colonne di un tipo di dati definito dall'utente non vengono migrate correttamente

Quando si esegue la replica da un'origine PostgreSQL, AWS DMS crea la tabella di destinazione con gli stessi tipi di dati per tutte le colonne, tranne le colonne con i tipi di dati definiti dall'utente. In questi casi, il tipo di dati viene creato come "carattere variabile" nella destinazione.

Errore: No schema has been selected to create in (Nessuno schema selezionato per la creazione)

In alcuni casi, potresti visualizzare l'errore «SQL_ERROR SqlState: 3F000:7 Messaggio NativeError: ERROR: nessuno schema è stato selezionato per la creazione in».

Questo errore può verificarsi quando la mappatura della tabella JSON contiene un valore jolly per lo schema e il database di origine non supporta tale valore.

Le operazioni di eliminazione e aggiornamento su una tabella non vengono replicate mediante CDC

Le operazioni di eliminazione e aggiornamento durante l'acquisizione dei dati di modifica (CDC) vengono ignorate se la tabella di origine non ha una chiave primaria. AWS DMS supporta l'acquisizione dei dati di modifica (CDC) per tabelle PostgreSQL con chiavi primarie.

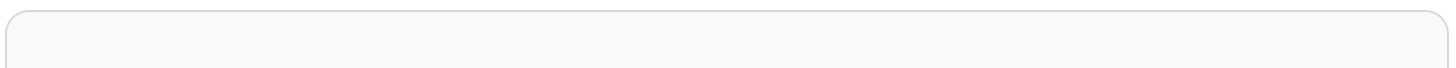
Se una tabella non dispone di una chiave primaria, i log write-ahead (WAL) non includono un'immagine precedente della riga di database. In questo caso, AWS DMS non è in grado di aggiornare la tabella. Per replicare le operazioni di eliminazione, crea una chiave primaria sulla tabella di origine.

Le istruzioni Truncate non vengono propagate

Quando utilizzi l'acquisizione dei dati di modifica (CDC), le operazioni TRUNCATE non sono supportate da AWS DMS.

Come evitare che PostgreSQL acquisisca DDL

Per evitare che un endpoint di destinazione PostgreSQL acquisisca istruzioni DDL, aggiungi l'istruzione Impostazione dell'endpoint riportata di seguito.



```
"CaptureDDLs": "N"
```

Selezione dello schema in cui vengono creati gli oggetti di database per l'acquisizione di DDL

Puoi controllare in quale schema vengono creati gli oggetti di database correlati all'acquisizione di DDL. Aggiungi la seguente istruzione Impostazione dell'endpoint. Il parametro Impostazione dell'endpoint è disponibile nella scheda dell'endpoint di origine.

```
"DdlArtifactsSchema": "xyzddl-schema"
```

Tabelle Oracle mancanti dopo la migrazione a PostgreSQL

In questo caso, le tabelle e i dati sono generalmente ancora accessibili.

Per impostazione predefinita, per i nomi di tabella Oracle utilizza i caratteri maiuscoli e PostgreSQL i caratteri minuscoli. Quando esegui una migrazione da Oracle a PostgreSQL, ti suggeriamo di fornire le regole di trasformazione nella sezione di mappatura delle tabelle dell'attività. Queste sono regole di trasformazione per convertire le maiuscole e le minuscole dei nomi delle tabelle.

Se hai eseguito la migrazione delle tabelle senza utilizzare le regole di trasformazione per convertire le maiuscole e le minuscole dei nomi delle tabelle, racchiudi i nomi delle tabelle tra virgolette quando vi fai riferimento.

ReplicationSlotDiskUsage aumenta e restart_lsn smette di andare avanti durante transazioni lunghe, come i carichi di lavoro ETL

Quando la replica logica è abilitata, il numero massimo di modifiche conservate in memoria per transazione è 4 MB. Dopodiché, le modifiche vengono riversate su disco. Di conseguenza ReplicationSlotDiskUsage aumenta e restart_lsn non avanza finché la transazione non viene completata/interrotta e il rollback non termina. Poiché si tratta di una transazione lunga, il rollback può richiedere tempi lunghi.

Pertanto, evita transazioni di lunga durata quando la replica logica è abilitata. Prova invece a suddividere la transazione in diverse transazioni più piccole.

Un'attività che utilizza la vista come origine non dispone di righe copiate

Per migrare una vista, imposta `table-type` su `all` o `view`. Per ulteriori informazioni, consulta [Specifica della selezione delle tabelle e delle regole di trasformazione dalla console](#).

Le origini che supportano le viste sono riportate di seguito.

- Oracle
- Microsoft SQL Server
- MySQL
- PostgreSQL
- IBM Db2 LUW
- SAP Adaptive Server Enterprise (ASE)

Risoluzione dei problemi relativi a Microsoft SQL Server

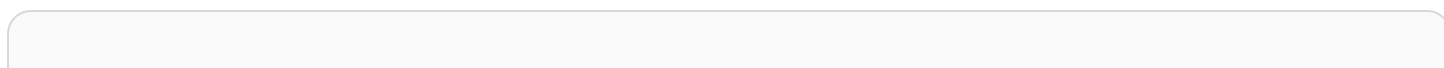
Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database Microsoft SQL Server.

Argomenti

- [Errori durante l'acquisizione di modifiche per il database SQL Server](#)
- [Colonne di identità mancanti](#)
- [Errore: SQL Server non supporta le pubblicazioni](#)
- [Le modifiche non vengono visualizzate nella destinazione](#)
- [Tabella non uniforme mappata tra le partizioni](#)

Errori durante l'acquisizione di modifiche per il database SQL Server

Spesso, gli errori che si verificano durante l'acquisizione dei dati di modifica (CDC) possono indicare che uno dei prerequisiti non è stato soddisfatto. Ad esempio, il prerequisito trascurato più di frequente è un backup completo del database. Il log delle attività indica questa omissione con il seguente errore:



```
SOURCE_CAPTURE E: No FULL database backup found (under the 'FULL' recovery model).  
To enable all changes to be captured, you must perform a full database backup.  
120438 Changes may be missed. (sqlserver_log_queries.c:2623)
```

Esamina i prerequisiti per l'utilizzo di SQL Server come origine elencati in [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#).

Colonne di identità mancanti

AWS DMS non supporta le colonne di identità quando crei uno schema di destinazione. Devi aggiungerle dopo il completamento del caricamento iniziale.

Errore: SQL Server non supporta le pubblicazioni

Il seguente errore viene generato quando utilizzi SQL Server Express come endpoint di origine:

```
RetCode: SQL_ERROR SqlState: HY000 NativeError: 21106  
Message: This edition of SQL Server does not support publications.
```

Attualmente, AWS DMS non supporta SQL Server Express come origine o destinazione.

Le modifiche non vengono visualizzate nella destinazione

Per acquisire le modifiche in modo coerente, AWS DMS richiede che un database SQL Server di origine utilizzi il modello di ripristino dei dati 'FULL' o 'BULK LOGGED'. Il modello "SIMPLE" non è supportato.

Il modello di ripristino dei dati "SIMPLE" registra le informazioni minime necessarie per consentire agli utenti di ripristinare i propri database. Tutte le voci di log inattive vengono automaticamente troncate quando si verifica un checkpoint.

Tutte le operazioni sono ancora registrate. Tuttavia, non appena si verifica un checkpoint, il log viene troncato automaticamente. Questo troncamento significa che il log diventa disponibile per il riutilizzo e le voci di log più vecchie possono essere sovrascritte. Quando le voci di log vengono sovrascritte, le modifiche non possono essere acquisite. Questo è il motivo per cui AWS DMS non supporta il modello di recupero dati SIMPLE. Per informazioni sugli altri prerequisiti necessari per l'utilizzo di

SQL Server come origine, consulta [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#).

Tabella non uniforme mappata tra le partizioni

Durante l'acquisizione dei dati di modifica (CDC), la migrazione di una tabella con una struttura specializzata viene sospesa quando AWS DMS non è in grado di eseguire correttamente la CDC sulla tabella. Vengono inviati messaggi come questi:

```
[SOURCE_CAPTURE ]W: Table is not uniformly mapped across partitions. Therefore - it is
excluded from CDC (sqlserver_log_metadata.c:1415)
[SOURCE_CAPTURE ]I: Table has been mapped and registered for CDC.
(sqlserver_log_metadata.c:835)
```

Quando si esegue il CDC nelle tabelle di SQL Server, AWS DMS analizza i tlog di SQL Server. Su ogni record tlog AWS DMS analizza i valori esadecimali contenenti dati per le colonne inserite, aggiornate o eliminate durante una modifica.

Per analizzare il record esadecimale, AWS DMS legge i metadati della tabella dalle tabelle di sistema di SQL Server. Tali tabelle di sistema identificano quali sono le colonne della tabella appositamente strutturate e rivelano alcune delle loro proprietà interne, come "xoffset" e "null bit position".

AWS DMS prevede che i metadati siano gli stessi per tutte le partizioni non elaborate della tabella. In alcuni casi, tuttavia, le tabelle particolarmente strutturate non hanno gli stessi metadati su tutte le partizioni. AWS DMS può sospendere la CDC su quella tabella per evitare di analizzare le modifiche in modo errato e fornire alla destinazione dati errati. Le soluzioni alternative sono:

- Se la tabella dispone di un indice cluster, eseguire una ricostruzione dell'indice.
- Se la tabella non dispone di un indice cluster, aggiungi un indice cluster alla tabella (è possibile eliminarlo in seguito, se necessario).

Risoluzione dei problemi relativi ad Amazon Redshift

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database Amazon Redshift.

Argomenti

- [Caricamento in un cluster Amazon Redshift in una regione AWS diversa rispetto a quella dell'istanza di replica](#)
- [Errore: Relation "awsdms_apply_exceptions" already exists \(Relazione "awsdms_apply_exceptions" già esistente\)](#)
- [Errori con tabelle il cui nome inizia con "awsdms_changes"](#)
- [Visualizzazione di tabelle nei cluster con nomi simili a dms.awsdms_changes000000000XXXX](#)
- [Autorizzazioni necessarie per l'utilizzo di Amazon Redshift](#)

Caricamento in un cluster Amazon Redshift in una regione AWS diversa rispetto a quella dell'istanza di replica

Non puoi caricare in un cluster Amazon Redshift in una regione AWS diversa rispetto a quella dell'istanza di replica AWS DMS. DMS richiede che l'istanza di replica e il cluster Amazon Redshift si trovino nella stessa regione.

Errore: Relation "awsdms_apply_exceptions" already exists (Relazione "awsdms_apply_exceptions" già esistente)

Spesso, l'errore "Relazione "awsdms_apply_exceptions" già esistente" si verifica quando un endpoint Redshift viene specificato come endpoint PostgreSQL. Per risolvere questo problema, modifica l'endpoint e l'impostazione Target engine (Motore di destinazione) in "redshift".

Errori con tabelle il cui nome inizia con "awsdms_changes"

I messaggi di errore delle tabelle con nomi che iniziano con "awsdms_changes" si verificano quando due attività che tentano di caricare dati nello stesso cluster Amazon Redshift vengono eseguite contemporaneamente. A causa della modalità di denominazione delle tabelle temporanee, le attività simultanee possono entrare in conflitto durante l'aggiornamento della stessa tabella.

Visualizzazione di tabelle nei cluster con nomi simili a dms.awsdms_changes000000000XXXX

AWS DMS crea tabelle temporanee quando i dati vengono caricati da file archiviati in Amazon S3. I nomi di queste tabelle temporanee includono il prefisso `dms.awsdms_changes`. Queste tabelle sono necessarie per consentire a AWS DMS di memorizzare i dati al primo caricamento e prima che vengano inseriti nella rispettiva tabella di destinazione finale.

Autorizzazioni necessarie per l'utilizzo di Amazon Redshift

Per utilizzare AWS DMS con Amazon Redshift, l'account utente che usi per accedere ad Amazon Redshift deve disporre delle seguenti autorizzazioni:

- CRUD (selezione, inserimento, aggiornamento, eliminazione)
- Caricamento in blocco
- Creazione, modifica, rimozione (se richieste dalla definizione dell'attività)

Per visualizzare i prerequisiti necessari per l'utilizzo di Amazon Redshift come destinazione, consulta [Utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service](#).

Risoluzione dei problemi relativi ad Amazon Aurora MySQL

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database Amazon Aurora MySQL.

Argomenti

- [Errore: CHARACTER SET UTF8 fields terminated by ',' enclosed by "" lines terminated by '\n' \(Campi SET DI CARATTERI UTF8 terminati da ',' racchiusi tra "" righe terminate da '\n'\)](#)

Errore: CHARACTER SET UTF8 fields terminated by ',' enclosed by "" lines terminated by '\n' (Campi SET DI CARATTERI UTF8 terminati da ',' racchiusi tra "" righe terminate da '\n')

Se utilizzi Amazon Aurora MySQL come destinazione, potresti vedere nei log un errore come il seguente. Questo tipo di errore in genere indica che ANSI_QUOTES fa parte del parametro SQL_MODE. Se ANSI_QUOTES fa parte del parametro SQL_MODE, le doppie virgolette vengono considerate come virgolette semplici e ciò può creare problemi quando esegui un'attività.

Per risolvere questo errore, rimuovi ANSI_QUOTES dal parametro SQL_MODE.

```
2016-11-02T14:23:48 [TARGET_LOAD ]E: Load data sql statement. load data local infile
"/rdsdbdata/data/tasks/7X04FJHCV0N7TYTLQ6RX3CQH DU/data_files/4/LOAD000001DF.csv" into
table
`VOSPUSER`.`SANDBOX_SRC_FILE` CHARACTER SET UTF8 fields terminated by ','
```

```
enclosed by ''' lines terminated by '\n'( `SANDBOX_SRC_FILE_ID`, `SANDBOX_ID`,  
`FILENAME`, `LOCAL_PATH`, `LINES_OF_CODE`, `INSERT_TS`, `MODIFIED_TS`, `MODIFIED_BY`,  
`RECORD_VER`, `REF_GUID`, `PLATFORM_GENERATED`, `ANALYSIS_TYPE`, `SANITIZED`, `DYN_TYPE`,  
`CRAWL_STATUS`, `ORIG_EXEC_UNIT_VER_ID` ) ; (provider_syntax_manager.c:2561)
```

Risoluzione dei problemi relativi a SAP ASE

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database SAP ASE.

Errore: le colonne LOB hanno valori NULL quando l'origine ha un indice univoco composto con valori NULL

Quando si utilizza SAP ASE come origine con tabelle configurate con un indice univoco composto che consente valori NULL, è possibile che i valori LOB non vengano migrati durante la replica continua. Questo comportamento è in genere il risultato di ANSI_NULL impostato su 1 sul client dell'istanza di replica DMS per impostazione predefinita.

Per garantire che i campi LOB migrino correttamente, includi l'impostazione dell'endpoint 'AnsiNull=0' nell'endpoint di origine AWS DMS dell'attività.

Risoluzione dei problemi relativi a IBM Db2

Di seguito vengono descritti i problemi specifici relativi all'uso di AWS DMS con i database IBM Db2.

Errore: la funzione Riprendi dal timestamp non è un'attività supportata

Per la replica continua (CDC), se prevedi di avviare la replica da un timestamp specifico, imposta l'attributo di connessione StartFromContext sul timestamp richiesto. Per ulteriori informazioni, consulta [Impostazioni degli endpoint quando si utilizza Db2 LUW](#). L'impostazione di StartFromContext sul timestamp richiesto evita il seguente problema:

```
Last Error Resume from timestamp is not supported Task error notification received  
from  
subtask 0, thread 0 [reptask/replicationtask.c:2822] [1020455] 'Start from timestamp'  
was blocked to prevent Replicate from  
scanning the log (to find the timestamp). When using IBM DB2 for LUW, 'Start from  
timestamp' is only supported if an actual  
change was captured by this Replicate task earlier to the specified timestamp.
```


Risoluzione dei problemi di latenza in AWS Database Migration Service

Questa sezione fornisce una panoramica delle cause più comuni della latenza delle attività AWS DMS durante la fase di replica continua (CDC). AWS DMS replica i dati in modo asincrono. La latenza è il ritardo tra il momento in cui una modifica è stata salvata sull'origine e il momento in cui la modifica è stata replicata sulla destinazione. La latenza può essere causata da un'errata configurazione dei componenti di replica, ad esempio:

- Endpoint oppure origine dati di origine
- Endpoint oppure origine dati di destinazione
- Istanze di replica
- La rete tra questi componenti

Ti consigliamo di eseguire una migrazione di test come prova concettuale per raccogliere le informazioni sulla replica. Quindi puoi utilizzare queste informazioni per ottimizzare la configurazione di replica in modo da ridurre al minimo la latenza. Per informazioni sull'esecuzione di una migrazione di tipo proof of concept, consulta [Esecuzione di un proof of concept](#).

Argomenti

- [Tipi di latenza CDC](#)
- [Cause comuni della latenza CDC](#)
- [Risoluzione dei problemi di latenza](#)

Tipi di latenza CDC

Questa sezione include i tipi di latenza di replica che possono verificarsi durante la CDC.

Latenza di origine

Il ritardo, in secondi, tra l'ora del commit dell'ultimo evento acquisito dall'endpoint di origine e il timestamp di sistema corrente dell'istanza di replica. È possibile monitorare la latenza tra l'origine dati e l'istanza di replica utilizzando la `CDCLatencySource` CloudWatch metrica. Una metrica `CDCLatencySource` elevata indica che il processo di acquisizione delle modifiche dall'origine è ritardato. Ad esempio, se l'applicazione esegue il commit di un inserimento nell'origine alle 10:00 e AWS DMS utilizza la modifica alle 10:02, la metrica `CDCLatencySource` è 120 secondi.

Per informazioni sulle CloudWatch metriche per, consulta. AWS DMS [Parametri dell'attività di replica](#)

Latenza della destinazione

Il ritardo, in secondi, tra l'ora del commit sull'origine del primo evento in attesa di eseguire il commit sulla destinazione e il timestamp corrente dell'istanza di replica DMS. Puoi monitorare la latenza tra i commit sull'origine dati e sulla destinazione dei dati utilizzando la metrica. CDCLatencyTarget CloudWatch Ciò significa che CDCLatencyTarget include eventuali ritardi nella lettura dall'origine. Di conseguenza, CDCLatencyTarget è sempre maggiore o uguale a CDCLatencySource.

Ad esempio, se l'applicazione esegue il commit di un inserimento nell'origine alle 10:00, AWS DMS lo utilizza alle 10:02 e lo scrive nella destinazione alle 10:05, la metrica CDCLatencyTarget è 300 secondi.

Cause comuni della latenza CDC

Questa sezione include le cause di latenza che la replica potrebbe riscontrare durante la CDC.

Argomenti

- [Risorse degli endpoint](#)
- [Risorse dell'istanza di replica](#)
- [Velocità e larghezza di banda della rete](#)
- [Configurazione di DMS](#)
- [Scenari di replica](#)

Risorse degli endpoint

I seguenti fattori influiscono in modo significativo sulle prestazioni e sulla latenza della replica:

- Configurazioni del database di origine e di destinazione
- Dimensioni istanza
- Datastore di origine o di destinazione con provisioning insufficiente o configurati in modo errato

Per identificare le cause della latenza causata dai problemi degli endpoint per le sorgenti e le destinazioni AWS ospitate, monitora le seguenti metriche: CloudWatch

- FreeMemory

- CPUUtilization
- Metriche di velocità di trasmissione effettiva e I/O, ad esempio WriteIOPS, WriteThroughput o ReadLatency
- Metriche del volume delle transazioni, ad esempio CDCIncomingChanges.

Per informazioni sul monitoraggio CloudWatch delle metriche, consulta [Parametri di AWS Database Migration Service](#)

Risorse dell'istanza di replica

Le risorse dell'istanza di replica sono fondamentali per la replica ed è necessario assicurarsi che non si verifichino colli di bottiglia, in quanto possono portare alla latenza sia sull'origine che sulla destinazione.

Per identificare i colli di bottiglia relativi alle risorse per l'istanza di replica, verifica quanto segue:

- CloudWatch I parametri critici come CPU, memoria, I/O al secondo e storage non presentano picchi o valori costantemente elevati.
- L'istanza di replica è dimensionata in modo appropriato per il carico di lavoro. Per informazioni sulla determinazione della dimensione corretta dell'istanza di replica, consulta [Selezione della dimensione migliore per un'istanza di replica](#).

Velocità e larghezza di banda della rete

La larghezza di banda della rete è un fattore che influisce sulla trasmissione dei dati. Per analizzare le prestazioni di rete della replica, esegui una delle operazioni riportate di seguito:

- Controlla le metriche ReadThroughput e WriteThroughput a livello di istanza. Per informazioni sulle metriche di monitoraggio CloudWatch, consulta [Parametri di AWS Database Migration Service](#)
- Usa l'AMI del supporto di diagnostica AWS DMS. Se l'AMI del supporto di diagnostica non è disponibile nella tua regione, puoi scaricarla da qualsiasi regione supportata e copiarla nella tua regione per eseguire l'analisi della rete. Per informazioni sull'AMI del supporto di diagnostica, consulta [Utilizzo dell'AMI di supporto AWS DMS diagnostico](#).

L'attività di CDC in AWS DMS è a thread singolo per garantire la coerenza dei dati. Di conseguenza, è possibile determinare il volume di dati che la rete è in grado di supportare calcolando la velocità di

trasferimento dei dati a thread singolo. Ad esempio, se l'attività si connette all'origine utilizzando una rete da 100 Mbps (megabit al secondo), la replica ha un'allocazione teorica massima della larghezza di banda di 12,5 MBps (megabyte al secondo). Ciò equivale a 45 gigabit all'ora. Se la velocità di generazione del log delle transazioni sull'origine è superiore a 45 gigabit all'ora, significa che l'attività ha una latenza della CDC. Per una rete a 100 Mbps, queste velocità sono i valori massimi teorici. Altri fattori, come il traffico di rete e il sovraccarico di risorse sull'origine e sulla destinazione, riducono la larghezza di banda effettiva disponibile.

Configurazione di DMS

Questa sezione contiene le configurazioni di replica consigliate che possono aiutare a ridurre la latenza.

- **Impostazioni degli endpoint:** le impostazioni degli endpoint di origine e di destinazione possono causare un calo delle prestazioni dell'istanza di replica. Le impostazioni degli endpoint che attivano funzionalità a uso intensivo di risorse influiscono sulle prestazioni. Ad esempio, per un endpoint Oracle, la disabilitazione LogMiner e l'utilizzo di Binary Reader migliorano le prestazioni, poiché LogMiner richiedono molte risorse. La seguente impostazione migliora le prestazioni di un endpoint Oracle:

```
useLogminerReader=N;useBfile=Y
```

Per ulteriori informazioni sulle impostazioni degli endpoint, consulta la documentazione per il motore dell'endpoint di origine e di destinazione nell'argomento [Utilizzo degli endpoint AWS DMS](#).

- **Impostazioni delle attività:** alcune impostazioni delle attività per uno specifico scenario di replica possono causare un calo delle prestazioni dell'istanza di replica. Ad esempio, AWS DMS utilizza la modalità di applicazione transazionale per impostazione predefinita (`BatchApplyEnabled=false`) per CDC per tutti gli endpoint, ad eccezione di Amazon Redshift. Tuttavia, per le origini con un numero elevato di modifiche, l'impostazione `BatchApplyEnabled` su `true` può migliorare le prestazioni.

Per ulteriori informazioni sulle impostazioni delle attività, consulta [Specificazione delle impostazioni delle attività per le attività del AWS Database Migration Service](#).

- **Posizione iniziale di un'attività di sola CDC:** l'avvio di un'attività di sola CDC da una posizione o da un timestamp precedente comporta l'avvio dell'attività con una maggiore latenza dell'origine CDC. A seconda del volume delle modifiche all'origine, la latenza dell'attività richiede del tempo per la riduzione.

- Impostazioni LOB: i tipi di dati oggetti di grandi dimensioni possono influire sulle prestazioni di replica a causa del modo in cui AWS DMS replica i dati binari di grandi dimensioni. Per ulteriori informazioni, consulta i seguenti argomenti:
 - [Impostazione del supporto LOB per i database di origine in un task AWS DMS](#)
 - [Migrazione di oggetti binari di grandi dimensioni \(LOB\)](#).

Scenari di replica

In questa sezione sono descritti specifici scenari di replica e in che modo possono influire sulla latenza.

Argomenti

- [Interruzione di un'attività per un periodo di tempo esteso](#)
- [Modifiche memorizzate nella cache](#)
- [Replica in più regioni](#)

Interruzione di un'attività per un periodo di tempo esteso

Quando si interrompe un'attività, AWS DMS salva la posizione dell'ultimo log delle transazioni letto dall'origine. Quando si riprende l'attività, DMS tenta di continuare la lettura dalla stessa posizione del log delle transazioni. La ripresa di un'attività dopo diverse ore o giorni causa un aumento della latenza dell'origine CDC fino a quando DMS non finisce di consumare il backlog delle transazioni.

Modifiche memorizzate nella cache

Le modifiche memorizzate nella cache vengono scritte dall'applicazione nell'origine dati durante l'esecuzione della fase di replica di pieno carico di AWS DMS. DMS non applica queste modifiche fino al completamento della fase di pieno carico e all'avvio della fase CDC. Per un'origine con un numero elevato di transazioni, le modifiche memorizzate nella cache richiedono più tempo per essere applicate, quindi la latenza dell'origine aumenta all'inizio della fase CDC. Ti consigliamo di eseguire la fase di pieno carico quando i volumi delle transazioni sono bassi per ridurre al minimo il numero di modifiche memorizzate nella cache.

Replica in più regioni

Il posizionamento degli endpoint DMS o dell'istanza di replica in regioni AWS diverse aumenta la latenza di rete. Di conseguenza aumenta la latenza della replica. Per prestazioni ottimali, posiziona l'endpoint di origine, l'endpoint di destinazione e l'istanza di replica nella stessa regione AWS.

Risoluzione dei problemi di latenza

In questa sezione sono indicate le procedure per la risoluzione dei problemi relativi alla latenza di replica.

Per risolvere i problemi di latenza, esegui questi passaggi:

- Innanzitutto, determina il tipo e la quantità di latenza per l'attività. Controlla la sezione Statistiche della tabella dell'attività nella console DMS o nella CLI. Se i contatori cambiano, la trasmissione dei dati è in corso. Controlla insieme le metriche CDCLatencySource e CDCLatencyTarget per determinare se c'è un collo di bottiglia durante la CDC.
- Se la metrica CDCLatencySource o CDCLatencyTarget riporta valori elevati indica un ostacolo nella replica, quindi controlla quanto segue:
 - Se CDCLatencySource è elevato e CDCLatencyTarget è uguale a CDCLatencySource, indica che c'è un collo di bottiglia nell'endpoint di origine e AWS DMS scrive i dati sulla destinazione senza problemi. Consulta [Risoluzione dei problemi di latenza dell'origine](#) di seguito.
 - Se CDCLatencySource è ridotto e CDCLatencyTarget è elevato, indica che c'è un collo di bottiglia nell'endpoint di destinazione e AWS DMS legge i dati dall'origine senza problemi. Consulta [Risoluzione dei problemi di latenza della destinazione](#) di seguito.
 - Se CDCLatencySource è elevato e CDCLatencyTarget è significativamente superiore a CDCLatencySource, indica problemi sia nella lettura dell'origine che nella scrittura della destinazione. Analizza prima la latenza dell'origine, quindi analizza la latenza di destinazione.

Per informazioni sul monitoraggio delle metriche dell'attività DMS, consulta [Monitoraggio delle attività AWS DMS](#).

Risoluzione dei problemi di latenza dell'origine

Nei seguenti argomenti vengono descritti gli scenari di replica specifici dei tipi di endpoint di origine.

Argomenti

- [Risoluzione dei problemi relativi all'endpoint Oracle](#)
- [Risoluzione dei problemi relativi all'endpoint MySQL](#)
- [Risoluzione dei problemi relativi all'endpoint PostgreSQL](#)
- [Risoluzione dei problemi relativi all'endpoint SQL Server](#)

Risoluzione dei problemi relativi all'endpoint Oracle

In questa sezione vengono descritti gli scenari di replica specifici di Oracle.

Letture dell'origine sospesa

AWS DMS sospende la lettura di un'origine Oracle nei seguenti scenari. Si tratta di un comportamento predefinito. È possibile indagare sulle cause utilizzando il log delle attività. Cerca messaggi simili ai seguenti nel log delle attività. Per informazioni sull'utilizzo del log delle attività, consulta [Visualizzazione e gestione dei log delle attività AWS DMS](#).

- **Messaggio SORTER:** indica che DMS sta memorizzando nella cache le transazioni sull'istanza di replica. Per ulteriori informazioni, consulta la sezione seguente: [Messaggio SORTER nel log delle attività](#).
- **Log delle attività di debug:** se DMS interrompe il processo di lettura, l'attività scrive ripetutamente il seguente messaggio nei log delle attività di debug, senza modificare il campo di contesto o il timestamp:
 - **Binary Reader:**

```
[SOURCE_CAPTURE ]T: Produce CTI event:
context '00000020.f23ec6e5.00000002.000a.00.0000:190805.3477731.16'
xid [00000000001e0018] timestamp '2021-07-19 06:57:55'
thread 2 (oradcdc_oralog.c:817)
```

- **LogMiner:**

```
[SOURCE_CAPTURE ]T: Produce INSERT event:
object id 1309826 context
'000000000F2CECAA010000010005A8F500000275016C0000000000000F2CEC58'
xid [000014e06411d996] timestamp '2021-08-12 09:20:32' thread 1
(oradcdc_reader.c:2269)
```

- **AWS DMS registra il seguente messaggio per ogni nuova operazione del log redo o di archiviazione.**

```
00007298: 2021-08-13T22:00:34 [SOURCE_CAPTURE ]I: Start processing archived
Redo log sequence 14850 thread 2 name XXXXX/XXXXX/ARCHIVELOG/2021_08_14/
thread_2_seq_14850.22977.1080547209 (oradcdc_redo.c:754)
```

Se l'origine presenta nuove operazioni del log redo o di archiviazione e AWS DMS non scrive questi messaggi nel log, significa che l'attività non sta elaborando gli eventi.

Elevata generazione di log redo

Se la tua attività sta elaborando log redo o di archiviazione, ma la latenza dell'origine rimane elevata, prova a identificare la velocità di generazione e i modelli di generazione dei log redo. Se il livello di generazione di log redo è elevato, aumenta la latenza dell'origine perché l'attività legge tutti i log redo e di archiviazione per recuperare le modifiche relative alle tabelle replicate.

Per determinare la frequenza di generazione dei log redo, utilizza le seguenti query.

- Frequenza di generazione di log redo al giorno:

```
select trunc(COMPLETION_TIME,'DD') Day, thread#,
round(sum(BLOCKS*BLOCK_SIZE)/1024/1024/1024) GB,
count(*) Archives_Generated from v$archived_log
where completion_time > sysdate- 1
group by trunc(COMPLETION_TIME,'DD'),thread# order by 1;
```

- Frequenza di generazione di log redo all'ora:

```
Alter session set nls_date_format = 'DD-MON-YYYY HH24:MI:SS';
select trunc(COMPLETION_TIME,'HH') Hour,thread# ,
round(sum(BLOCKS*BLOCK_SIZE)/1024/1024) "REDO PER HOUR (MB)",
count(*) Archives from v$archived_log
where completion_time > sysdate- 1
group by trunc(COMPLETION_TIME,'HH'),thread# order by 1 ;
```

Per risolvere i problemi di latenza in questo scenario, verifica quanto segue:

- Controlla la larghezza di banda della rete e le prestazioni a thread singolo della replica per assicurarti che la rete sottostante sia in grado di supportare la velocità di generazione dei log redo di origine. Per informazioni su come la larghezza di banda della rete può influire sulle prestazioni della replica, consulta [Velocità e larghezza di banda della rete](#) in precedenza.
- Verifica se il log supplementare è configurato al momento. Evita la registrazione aggiuntiva sull'origine, ad esempio abilitando la registrazione di tutte le colonne di una tabella. Per

informazioni sulla configurazione del log supplementare, consulta [Impostazione del log supplementare](#).

- Verifica di utilizzare l'API corretta per leggere i log redo o di archiviazione. È possibile utilizzare Oracle o Binary Reader. LogMiner AWS DMS Mentre LogMiner legge i redo log online e i redo log file archiviati, Binary Reader legge e analizza direttamente i redo log file non elaborati. Di conseguenza, Binary Reader è più performante. Ti consigliamo di utilizzare Binary Reader se la generazione dei log redo supera i 10 GB/ora. Per ulteriori informazioni, consulta [Utilizzo di Oracle LogMiner o AWS DMS Binary Reader for CDC](#).
- Controlla se `ArchivedLogsOnly` è impostato su `Y`. Se questa impostazione dell'endpoint è configurata, AWS DMS legge dai log redo archiviati. Ciò aumenta la latenza dell'origine perché AWS DMS attende che il log redo online venga archiviato prima della lettura. Per [ArchivedLogsOnly](#)ulteriori informazioni, vedere.
- Se l'origine Oracle utilizza Automatic Storage Management (ASM), consulta [Memorizzazione di REDO su Oracle ASM quando si utilizza Oracle come origine per AWS DMS](#) per informazioni su come configurare correttamente il datastore. Puoi ottimizzare ulteriormente le prestazioni di lettura utilizzando l'attributo aggiuntivo di connessione `asmUsePLSQLArray`. Per ulteriori informazioni sull'uso di `asmUsePLSQLArray`, consultare [Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS](#).

Risoluzione dei problemi relativi all'endpoint MySQL

In questa sezione sono descritti gli scenari di replica specifici per MySQL. AWS DMS analizza periodicamente il log binario di MySQL per replicare le modifiche. Questo processo può aumentare la latenza negli scenari riportati di seguito:

Argomenti

- [Transazione di lunga durata sull'origine](#)
- [Carico di lavoro elevato sull'origine](#)
- [Conflitto di log binari](#)

Transazione di lunga durata sull'origine

Poiché MySQL scrive solo transazioni sottoposte al commit nel log binario, le transazioni di lunga durata causano picchi di latenza proporzionali al tempo di esecuzione della query.

Per identificare le transazioni di lunga durata, utilizza la seguente query o il log delle query lente:

```
SHOW FULL PROCESSLIST;
```

Per informazioni sull'utilizzo del log delle query lente, consulta [The Slow Query Log](#) nella [documentazione di MySQL](#).

Per evitare picchi di latenza dovuti alle transazioni di lunga durata, ristruttura le transazioni di origine per ridurre il tempo di esecuzione delle query o aumentare la frequenza di commit.

Carico di lavoro elevato sull'origine

Poiché DMS CDC è a thread singolo, un numero elevato di transazioni può aumentare la latenza dell'origine. Per determinare se la latenza dell'origine è dovuta a un carico di lavoro intenso, confronta il numero e la dimensione dei log binari generati durante il periodo di latenza con i log generati prima della latenza. Per verificare i log binari e lo stato dei thread DMS CDC, utilizza le seguenti query:

```
SHOW BINARY LOGS;  
SHOW PROCESSLIST;
```

Per ulteriori informazioni sugli stati dei thread di dump dei log binari CDC, consulta [Replication Source Thread States](#).

È possibile determinare la latenza confrontando l'ultima posizione del log binario generata sull'origine con l'evento che DMS sta attualmente elaborando. Per identificare il log binario più recente nell'origine, esegui queste operazioni:

- Abilita i log di debug sul componente SOURCE_CAPTURE.
- Recupera il log binario di elaborazione DMS e i dettagli sulla posizione dai log di debug delle attività.
- Utilizza la seguente query per identificare il log binario più recente nell'origine:

```
SHOW MASTER STATUS;
```

Per ottimizzare ulteriormente le prestazioni, modifica `EventsPollInterval`. Per impostazione predefinita, DMS esegue il polling del log binario ogni 5 secondi, ma è possibile migliorare le prestazioni riducendo questo valore. Per ulteriori informazioni sull'impostazione `EventsPollInterval`, consulta [Impostazioni degli endpoint quando si utilizza MySQL come sorgente per AWS DMS](#).

Conflitto di log binari

Quando si migrano più tabelle con una grande quantità di dati, ti consigliamo di suddividere le tabelle in attività separate per MySQL 5.7.2 o versioni successive. Nelle MySQL 5.7.2 e versioni successive, il thread di dump master crea meno conflitti di blocco e migliora la velocità di trasmissione effettiva. Di conseguenza, il thread di dump non blocca più il log binario ogni volta che legge un evento. Ciò significa che più thread di dump possono leggere contemporaneamente il file di log binario. Ciò significa anche che i thread di dump possono leggere il log binario mentre i client scrivono. Per ulteriori informazioni sui thread di dump, consulta [Replication Threads](#) e [MySQL 5.7.2 release notes](#).

Per migliorare le prestazioni della replica per le versioni delle origini MySQL precedenti alla 5.7.2, prova a consolidare le attività con i componenti CDC.

Risoluzione dei problemi relativi all'endpoint PostgreSQL

In questa sezione vengono descritti gli scenari di replica specifici di PostgreSQL.

Argomenti

- [Transazione di lunga durata sull'origine](#)
- [Carico di lavoro elevato sull'origine](#)
- [Velocità di trasmissione effettiva della rete elevata](#)
- [Versare file in Aurora PostgreSQL](#)

Transazione di lunga durata sull'origine

Quando nel database di origine sono presenti transazioni di lunga durata, ad esempio migliaia di inserimenti in una singola transazione, i contatori degli eventi e delle transazioni DMS CDC non aumentano fino al completamento della transazione. Questo ritardo può causare problemi di latenza che è possibile misurare utilizzando la metrica `CDCLatencyTarget`.

Per esaminare le transazioni di lunga durata, effettua una delle operazioni riportate di seguito:

- Usa la vista `pg_replication_slots`. Se il valore `restart_lsn` non si aggiorna, è probabile che PostgreSQL non sia in grado di rilasciare i log WAL (Write Ahead Log) a causa di transazioni attive di lunga durata. Per informazioni sulla vista `pg_replication_slots`, consulta [pg_replication_slots](#) nella [documentazione di PostgreSQL 15.4](#).
- Utilizza la seguente query per ottenere l'elenco di tutte le query attive nel database, insieme alle informazioni correlate:

```
SELECT pid, age(clock_timestamp(), query_start), username, query
FROM pg_stat_activity WHERE query != '<IDLE>'
AND query NOT ILIKE '%pg_stat_activity%'
ORDER BY query_start desc;
```

Nei risultati delle query, il campo `age` mostra la durata attiva di ogni query, che è possibile utilizzare per identificare le query di lunga durata.

Carico di lavoro elevato sull'origine

Se l'origine PostgreSQL ha un carico di lavoro elevato, controlla quanto segue per ridurre la latenza:

- Potresti riscontrare un'elevata latenza quando utilizzi il plug-in `test_decoding` durante la migrazione di un sottoinsieme di tabelle dal database di origine con un valore di transazioni al secondo (TPS) elevato. Questo perché il plug-in `test_decoding` invia tutte le modifiche del database all'istanza di replica, che DMS filtra in base alla mappatura delle tabelle dell'attività. Gli eventi delle tabelle che non fanno parte della mappatura delle tabelle dell'attività possono aumentare la latenza della origine.
- Verifica la velocità di trasmissione effettiva TPS utilizzando uno dei metodi riportati di seguito.
 - Per i sorgenti Aurora PostgreSQL, usa la metrica `CommitThroughput` CloudWatch
 - Per PostgreSQL in esecuzione su Amazon RDS o on-premise, usa la seguente query con un client PSQL versione 11 o successiva (premi **enter** durante la query per ottenere i risultati):

```
SELECT SUM(xact_commit)::numeric as temp_num_tx_ini FROM pg_stat_database; \gset
select pg_sleep(60);
SELECT SUM(xact_commit)::numeric as temp_num_tx_final FROM pg_stat_database; \gset
select (:temp_num_tx_final - :temp_num_tx_ini)/ 60.0 as "Transactions Per Second";
```

- Per ridurre la latenza quando usi il plug-in `test_decoding`, puoi considerare di utilizzare il plug-in `pglogical`. A differenza del plug-in `test_decoding`, il plug-in `pglogical` filtra le modifiche WAL all'origine e invia solo le modifiche pertinenti all'istanza di replica. Per informazioni sull'utilizzo del plug-in `pglogical` con AWS DMS, consulta [Configurazione del plug-in pglogical](#).

Velocità di trasmissione effettiva della rete elevata

La replica potrebbe richiedere un elevato utilizzo della larghezza di banda della rete quando si utilizza il plug-in `test_decoding`, specialmente durante transazioni con volumi elevati. Questo perché il

plug-in `test_decoding` elabora le modifiche e le converte in un formato leggibile dall'uomo più grande del formato binario originale.

Per migliorare le prestazioni, considera di utilizzare `pglogical` che è un plug-in binario. A differenza del plug-in `test_decoding`, il plug-in `pglogical` genera un output in formato binario, con conseguenti modifiche del flusso WAL compresso.

Versare file in Aurora PostgreSQL

Nella versione 13 e successive di PostgreSQL, il parametro determina l'allocazione della memoria per `logical_decoding_work_mem` la decodifica e lo streaming. [Per ulteriori informazioni sul `logical_decoding_work_mem` parametro, vedere Consumo di risorse in PostgreSQL nella documentazione di PostgreSQL 13.13.](#)

La replica logica accumula le modifiche per tutte le transazioni in memoria fino al completamento di tali transazioni. Se la quantità di dati archiviati in tutte le transazioni supera la quantità specificata dal parametro del database `logical_decoding_work_mem`, DMS trasferisce i dati della transazione su disco per liberare memoria per i nuovi dati di decodifica.

Le transazioni a esecuzione prolungata, o molte sottotransazioni, possono comportare un maggiore consumo di memoria di decodifica logica da parte del DMS. Questo maggiore utilizzo della memoria fa sì che DMS crei file di fuoriuscita su disco, il che causa un'elevata latenza del codice sorgente durante la replica.

Per ridurre l'impatto di un aumento del carico di lavoro di origine, procedi come segue:

- Riduci le transazioni di lunga durata.
- Riduci il numero di sottotransazioni.
- Evita di eseguire operazioni che generano una grande quantità di record di log, come l'eliminazione o l'aggiornamento di un'intera tabella in una singola transazione. Esegui invece operazioni in batch più piccoli.

Puoi utilizzare le seguenti CloudWatch metriche per monitorare il carico di lavoro sulla fonte:

- `TransactionLogsDiskUsage`: Il numero di byte attualmente occupati dal WAL logico. Questo valore aumenta in modo monotono se gli slot di replica logica non sono in grado di tenere il passo con il ritmo delle nuove scritture o se transazioni di lunga durata impediscono la raccolta indesiderata di file più vecchi.

- **ReplicationSlotDiskUsage**: la quantità di spazio su disco attualmente utilizzata dagli slot di replica logica.

È possibile ridurre la latenza della sorgente regolando il parametro `logical_decoding_work_mem`. Il valore predefinito per questo parametro è 64 MB. Questo parametro limita la quantità di memoria utilizzata da ogni connessione di replica in streaming logico. Si consiglia di impostare un `logical_decoding_work_mem` valore significativamente più alto rispetto al `work_mem` valore per ridurre la quantità di modifiche decodificate che DMS scrive su disco.

Si consiglia di verificare periodicamente la presenza di file fuoriusciti, in particolare durante i periodi di intensa attività di migrazione o di latenza. Se DMS sta creando un numero significativo di file di spill, significa che la decodifica logica non funziona in modo efficiente, il che può aumentare la latenza. Per mitigare questo problema, aumentate il valore del parametro `logical_decoding_work_mem`.

È possibile controllare l'attuale eccesso di transazioni con la `aurora_stat_file` funzione. Per ulteriori informazioni, consulta [Adjusting working memory for logical decoding](#) nella Amazon Relational Database Service Developer Guide.

Risoluzione dei problemi relativi all'endpoint SQL Server

In questa sezione vengono descritti gli scenari di replica specifici di SQL Server. Per determinare quali modifiche replicare da SQL Server, AWS DMS legge i log delle transazioni ed esegue scansioni periodiche sul database di origine. La latenza della replica in genere deriva dalla limitazione (della larghezza di banda della rete) di SQL Server per queste scansioni a causa dei vincoli delle risorse. Può anche derivare da un aumento significativo del numero di eventi scritti nel log delle transazioni in un breve periodo di tempo.

Argomenti

- [Ricostruzione degli indici](#)
- [Transazioni di grandi dimensioni](#)
- [Intervallo di polling dell'acquisizione MS-CDC non configurato correttamente per Amazon RDS SQL Server](#)
- [Replica di più attività di CDC dallo stesso database di origine](#)

Ricostruzione degli indici

Quando SQL Server ricrea un indice di grandi dimensioni, utilizza una singola transazione. Questo approccio genera molti eventi e può utilizzare una grande quantità di spazio di log se SQL Server ricostruisce più indici contemporaneamente. In tal caso, è possibile aspettarsi brevi picchi nella replica. Se l'origine SQL Server presenta picchi di log elevati, verifica quanto segue:

- Innanzitutto, controlla il periodo di tempo in cui si verificano i picchi di latenza utilizzando le `CDCLatencySource` CloudWatch metriche `CDCLatencySource` and o controllando i messaggi di `Throughput Monitoring` nei log delle attività. Per informazioni sulle metriche per, consulta CloudWatch . AWS DMS [Parametri dell'attività di replica](#)
- Verifica se la dimensione dei log delle transazioni o dei backup dei log attivi è aumentata durante il picco di latenza. Controlla anche se durante quel periodo è stato eseguito un intervento di manutenzione o una ricostruzione. Per informazioni sulla verifica della dimensione del log delle transazioni, consulta [Monitoraggio dell'utilizzo dello spazio dei log](#) nella [documentazione tecnica di SQL Server](#).
- Verifica che il tuo piano di manutenzione segua le best practice di SQL Server. Per informazioni sulle best practice di manutenzione di SQL Server, consulta [Index maintenance strategy](#) nella [documentazione tecnica di SQL Server](#).

Per risolvere i problemi di latenza durante le ricostruzioni degli indici, prova a eseguire queste operazioni:

- Utilizza il modello di ripristino `BULK_LOGGED` per le ricostruzioni offline per ridurre gli eventi che l'attività deve elaborare.
- Se possibile, interrompi l'attività durante la ricostruzione dell'indice. In alternativa, prova a pianificare la ricostruzione dell'indice durante le ore non di punta per mitigare l'impatto di un picco di latenza.
- Prova a identificare i colli di bottiglia delle risorse che rallentano le letture DMS, come la latenza del disco o la velocità di trasmissione effettiva di I/O e risolvi.

Transazioni di grandi dimensioni

Le transazioni con molti eventi o le transazioni di lunga durata fanno aumentare la dimensione del log delle transazioni. Pertanto le letture DMS impiegano più tempo, con conseguente latenza. Questo approccio è simile all'effetto che le ricostruzioni degli indici hanno sulle prestazioni della replica.

Potrebbe essere difficile identificare questo problema se non si conosce il carico di lavoro tipico del database di origine. Per risolvere questo problema, esegui questi passaggi:

- Innanzitutto, identifica l'ora in cui è aumentata la latenza utilizzando le `WriteThroughput` CloudWatch metriche `ReadThroughput` and o controllando i messaggi di `Throughput Monitoring` nei log delle attività.
- Controlla se sono state eseguite query di lunga durata sul database di origine durante il picco di latenza. Per informazioni sulle query di lunga durata, consulta [Troubleshoot slow-running queries in SQL Server](#) nella [documentazione tecnica di SQL Server](#).
- Verifica se la dimensione dei log delle transazioni o dei backup dei log attivi è aumentata. Per ulteriori informazioni, consulta [Monitoraggio dell'utilizzo dello spazio dei log](#) nella [documentazione tecnica di SQL Server](#).

Per risolvere il problema, procedi in uno dei seguenti modi:

- La soluzione migliore è ristrutturare le transazioni sul lato dell'applicazione in modo che vengano completate rapidamente.
- Se non è possibile ristrutturare le transazioni, una soluzione alternativa a breve termine consiste nel verificare eventuali problemi di risorse, ad esempio attese del disco o conflitti di CPU. Se riscontri colli di bottiglia nel database di origine, puoi ridurre la latenza aumentando le risorse del disco, della CPU e della memoria per il database di origine. In tal modo riduci il conflitto per le risorse di sistema, permettendo alle query DMS di essere completate più rapidamente.

Intervallo di polling dell'acquisizione MS-CDC non configurato correttamente per Amazon RDS SQL Server

Un'impostazione errata dell'intervallo di polling per le istanze Amazon RDS può causare un aumento della dimensione del log delle transazioni. Questo avviene perché la replica impedisce il troncamento del log. Sebbene le attività in esecuzione possano continuare la replica con una latenza minima, l'interruzione e la ripresa delle attività o l'avvio di attività di sola CDC possono causare errori. Ciò è dovuto ai timeout che si verificano durante la scansione del log delle transazioni di grandi dimensioni.

Per risolvere il problema relativo a un intervallo di polling configurato in modo errato, esegui queste operazioni:

- Controlla se la dimensione del log delle transazioni attivo sta aumentando e se l'utilizzo del log è vicino al 100%. Per ulteriori informazioni, consulta [Monitoraggio dell'utilizzo dello spazio dei log](#) nella [documentazione tecnica di SQL Server](#).
- Controlla se il troncamento del log viene ritardato con `log_reuse_wait_desc` value pari a REPLICATION. Per ulteriori informazioni, consulta [Log delle transazioni \(SQL Server\)](#) nella [documentazione tecnica di SQL Server](#).

Se riscontri problemi con uno qualsiasi degli elementi dell'elenco precedente, ottimizza l'intervallo di polling dell'acquisizione MS-CDC. Per informazioni sull'ottimizzazione dell'intervallo di polling, consulta [Impostazioni consigliate per l'utilizzo di Amazon RDS for SQL Server come origine per AWS DMS](#).

Replica di più attività di CDC dallo stesso database di origine

Durante la fase di pieno carico, consigliamo di suddividere le tabelle tra le attività per migliorare le prestazioni, separare logicamente le tabelle dipendenti e mitigare l'impatto di un errore dell'attività. Tuttavia, durante la fase CDC, consigliamo di consolidare le attività per ridurre al minimo le scansioni DMS. Durante la fase CDC, ogni attività DMS analizza i log delle transazioni alla ricerca di nuovi eventi più volte ogni minuto. Poiché ogni attività viene eseguita in modo indipendente, ciascuna attività analizza ogni log delle transazioni singolarmente. Questo approccio aumenta l'utilizzo del disco e della CPU nel database SQL Server di origine. Di conseguenza, un elevato numero di attività eseguite in parallelo può far sì che SQL Server limiti le letture DMS, con conseguente aumento della latenza.

Potrebbe essere difficile identificare questo problema se più attività vengono avviate gradualmente. Il sintomo più comune di questo problema è che la maggior parte delle scansioni delle attività inizia a richiedere molto tempo. Ciò comporta una maggiore latenza per le scansioni. SQL Server dà la priorità ad alcune scansioni delle attività, quindi alcune di esse mostrano la latenza normale. Per risolvere questo problema, controlla la metrica `CDCLatencySource` per tutte le attività. Se alcune attività registrano un aumento di `CDCLatencySource`, mentre altre attività indicano un valore basso per `CDCLatencySource`, è probabile che SQL Server stia limitando le letture DMS per alcune attività.

Se SQL Server limita la lettura delle attività durante la fase CDC, consolida le attività per ridurre al minimo il numero di scansioni DMS. Il numero massimo di attività che possono connettersi al database di origine senza creare conflitti dipende da fattori quali la capacità del database di origine, la percentuale di aumento del log delle transazioni o il numero di tabelle. Per determinare il numero

ideale di attività per il tuo scenario di replica, prova la replica in un ambiente di test simile all'ambiente di produzione.

Risoluzione dei problemi di latenza della destinazione

In questa sezione sono illustrati gli scenari che possono contribuire alla latenza della destinazione.

Argomenti

- [Problemi di indicizzazione](#)
- [Messaggio SORTER nel log delle attività](#)
- [Blocco del database](#)
- [Ricerche LOB lente](#)
- [Multi-AZ: registrazione di audit e backup](#)

Problemi di indicizzazione

Durante la fase CDC, AWS DMS replica le modifiche sull'origine eseguendo istruzioni DML (inserimento, aggiornamento ed eliminazione) sulla destinazione. Per le migrazioni eterogenee che utilizzano DMS, le differenze nelle ottimizzazioni degli indici sull'origine e sulla destinazione possono far sì che le scritture sulla destinazione richiedano più tempo. Questo approccio comporta problemi di latenza e prestazioni della destinazione.

Per risolvere i problemi di indicizzazione, procedi come segue. Le procedure per questi passaggi variano a seconda dei diversi motori di database.

- Monitora il tempo di query per il database di destinazione. Il confronto del tempo di esecuzione delle query sulla destinazione e sull'origine può indicare quali indici devono essere ottimizzati.
- Abilita la registrazione per le query a esecuzione lenta.

Per risolvere i problemi di indicizzazione per le repliche di lunga durata, esegui queste operazioni:

- Ottimizza gli indici sui database di origine e di destinazione in modo che il tempo di esecuzione delle query sia simile sull'origine e sulla destinazione.
- Confronta gli indici secondari utilizzati nelle query DML per l'origine e la destinazione. Assicurati che le prestazioni DML sulla destinazione siano paragonabili o migliori delle prestazioni DML sull'origine.

Tieni presente che la procedura per l'ottimizzazione degli indici è specifica del motore di database in uso. Non è disponibile alcuna funzionalità DMS per l'ottimizzazione degli indici di origine e di destinazione.

Messaggio SORTER nel log delle attività

Se un endpoint di destinazione non riesce a tenere il passo con il volume delle modifiche che AWS DMS vi scrive, l'attività memorizza le modifiche nella cache dell'istanza di replica. Se la cache supera la soglia interna, l'attività interrompe la lettura di ulteriori modifiche dall'origine. DMS esegue questa operazione per evitare che l'istanza di replica esaurisca lo spazio di archiviazione o che l'attività si blocchi durante la lettura di un grande volume di eventi in sospeso.

Per risolvere questo problema, controlla se nei CloudWatch registri è presente un messaggio simile a uno dei seguenti:

```
[SORTER ]I: Reading from source is paused. Total disk usage exceeded the limit 90%  
(sorter_transaction.c:110)  
[SORTER ]I: Reading from source is paused. Total storage used by swap files exceeded  
the limit 1048576000 bytes (sorter_transaction.c:110)
```

Se i log contengono un messaggio simile al primo, disabilita qualsiasi registrazione di traccia per l'attività e aumenta lo spazio di archiviazione dell'istanza di replica. Per informazioni sull'aumento dello spazio di archiviazione delle istanze di replica, consulta [Modifica di un'istanza di replica](#).

Se i log contengono un messaggio simile al secondo, esegui queste operazioni:

- Sposta le tabelle con numerose transazioni o operazioni DML di lunga durata in un'attività separata, se non hanno alcuna dipendenza da altre tabelle dell'attività.
- Aumenta le impostazioni `MemoryLimitTotal` e `MemoryKeepTime` per mantenere la transazione in memoria per un periodo più lungo. Ciò non aiuta se la latenza è sostenuta, ma può contribuire a mantenere bassa la latenza durante brevi aumenti di volume transazionale. Per informazioni su queste impostazioni dell'attività, consulta [Impostazioni di ottimizzazione dell'elaborazione delle modifiche](#).
- Valuta se puoi utilizzare l'applicazione in batch per la transazione impostando `BatchApplyEnabled` su `true`. Per informazioni sull'impostazione `BatchApplyEnabled`, consulta [Impostazioni delle attività dei metadati di destinazione](#).

Blocco del database

Se un'applicazione accede a un database utilizzato da AWS DMS come destinazione di replica, l'applicazione può bloccare una tabella a cui DMS sta tentando di accedere. Questo crea un conflitto di blocco. Poiché DMS scrive le modifiche nel database di destinazione nell'ordine in cui sono state applicate nell'origine, il ritardo della scrittura in una tabella dovuti al conflitto di blocco creano ritardi della scrittura in tutte le tabelle.

Per risolvere questo problema, esegui una query sul database di destinazione per verificare se un conflitto di blocco sta bloccando le transazioni di scrittura DMS. Se il database di destinazione blocca le transazioni di scrittura DMS, esegui una o più delle operazioni riportate di seguito:

- Ristruttura le query per eseguire il commit delle modifiche più frequentemente.
- Modifica le impostazioni del timeout di blocco.
- Partiziona le tabelle per ridurre al minimo i conflitti di blocco.

Tieni presente che la procedura per l'ottimizzazione dei conflitti di blocco è specifica del motore di database in uso. Non è disponibile alcuna funzionalità DMS per ottimizzare i conflitti di blocco.

Ricerche LOB lente

Quando AWS DMS replica una colonna di oggetti di grandi dimensioni (LOB), esegue una ricerca sull'origine appena prima di scrivere le modifiche nella destinazione. Questa ricerca normalmente non causa alcuna latenza sulla destinazione, ma se il database di origine ritarda la ricerca a causa del blocco, la latenza della destinazione potrebbe aumentare.

Questo problema è in genere difficile da diagnosticare. Per risolverlo, abilita il debug dettagliato nei log delle attività e confronta i timestamp delle chiamate di ricerca LOB DMS. Per informazioni su come abilitare il debug dettagliato, consulta [Visualizzazione e gestione dei log delle attività AWS DMS](#).

Per risolvere il problema, procedi come segue:

- Migliora le prestazioni delle query SELECT sul database di origine.
- Ottimizza le impostazioni LOB DMS. Per informazioni sull'ottimizzazione delle impostazioni LOB, consulta [Migrazione di oggetti binari di grandi dimensioni \(LOB\)](#).

Multi-AZ: registrazione di audit e backup

Per le destinazioni Amazon RDS, la latenza di destinazione può aumentare nelle seguenti situazioni:

- Backup
- Dopo aver abilitato più zone di disponibilità (multi-AZ)
- Dopo aver abilitato la registrazione del database, ad esempio i log di audit o delle query lente.

Questi problemi sono in genere difficili da diagnosticare. Per risolverli, monitora la latenza per rilevare eventuali picchi periodici durante le finestre di manutenzione di Amazon RDS o i periodi di intenso carico del database.

Per risolvere questi problemi, prova a eseguire queste operazioni:

- Se possibile, durante la migrazione a breve termine, disabilita le multi-AZ, i backup o la registrazione.
- Riprogramma le finestre di manutenzione in periodi di scarsa attività.

Utilizzo degli script di supporto per la diagnostica in AWS DMS

Se riscontri un problema durante l'utilizzo di AWS DMS, il tecnico dell'assistenza potrebbe aver bisogno di ulteriori informazioni sul database di origine o di destinazione. È importante che il Supporto AWS riceva tutte le informazioni necessarie nel più breve tempo possibile. Pertanto, abbiamo sviluppato degli script per eseguire le query di queste informazioni per diversi tra i principali motori di database relazionale.

Se è disponibile uno script di supporto per il tuo database, puoi scaricarlo utilizzando il collegamento nell'argomento dello script corrispondente descritto di seguito. Dopo aver verificato e esaminato lo script (descritto di seguito), puoi eseguirlo secondo la procedura indicata nell'argomento dello script. Una volta completata l'esecuzione dello script, puoi caricarne l'output nel tuo caso del Supporto AWS (nuovamente descritto di seguito).

Prima di eseguire lo script, è possibile rilevare eventuali errori che potrebbero essere stati introdotti durante il download o l'archiviazione dello script di supporto. A tale scopo, confronta il checksum del file di script con il valore fornito da AWS. AWS utilizza l'algoritmo SHA256 per il checksum.

Per verificare il file di script di supporto utilizzando un checksum

1. Apri il file di checksum più recente fornito per verificare gli script di supporto all'indirizzo <https://d2pwp9zz55emqw.cloudfront.net/sha256Check.txt>. Il file può avere un contenuto simile al seguente esempio.

```
MYSQL dfafd0d511477c699f96c64693ad0b1547d47e74d5c5f2f2025b790b1422e3c8
ORACLE 6c41ebcfc99518cfa8a10cb2ce8943b153b2cc7049117183d0b5de3d551bc312
POSTGRES 6ccd274863d14f6f3146fbd8bba43f2d8d4c6a4c25380d7b41c71883aa4f9790
SQL_SERVER 971a6f2c46aec8d083d2b3b6549b1e9990af3a15fe4b922e319f4fdd358debe7
```

2. Esegui il comando di convalida SHA256 per il sistema operativo nella directory che contiene il file di supporto. Ad esempio, sul sistema operativo macOS è possibile eseguire il comando seguente per uno script di supporto Oracle, descritto successivamente in questo argomento.

```
shasum -a 256 awsdms_support_collector_oracle.sql
```

3. Confronta i risultati del comando con il valore mostrato nell'ultimo file `sha256Check.txt` che hai aperto. I due valori devono corrispondere. In caso contrario, contatta il tecnico del supporto per informazioni sulla mancata corrispondenza e su come ottenere un file di script di supporto pulito.

Se disponi di un file di script di supporto pulito, prima di eseguirlo assicurati di leggere e comprendere il codice SQL sia dal punto di vista delle prestazioni che della sicurezza. Se non desideri eseguire codice SQL nello script, puoi commentare o rimuovere l'SQL problematico. Puoi anche contattare il tecnico del supporto per ottenere eventuali soluzioni alternative accettabili.

Una volta completato correttamente, lo script restituisce l'output in un formato HTML leggibile, salvo diversa indicazione. Lo script è progettato per escludere dall'output HTML tutti i dati o i dettagli di sicurezza che possono compromettere l'azienda. Inoltre, non apporta modifiche al database o all'ambiente. Tuttavia, se nell'output HTML sono presenti informazioni che non desideri condividere, sentiti libero di rimuoverle prima di caricare l'output HTML. Se l'output HTML è accettabile, caricalo utilizzando gli allegati nei dettagli del caso del tuo caso di supporto.

Ciascuno dei seguenti argomenti descrive gli script disponibili per un database AWS DMS supportato e in che modo eseguirli. Il tecnico del supporto ti indicherà di usare uno script specifico documentato di seguito.

Argomenti

- [Script di supporto per la diagnostica Oracle](#)
- [Script di supporto per la diagnostica SQL Server](#)
- [Script di supporto diagnostico per database compatibili con MySQL](#)
- [Script di supporto diagnostico PostgreSQL](#)

Script di supporto per la diagnostica Oracle

Di seguito sono riportati gli script di supporto per la diagnostica disponibili per analizzare un database on-premise o Amazon RDS per Oracle nella configurazione di migrazione AWS DMS. Questi script funzionano con un endpoint di origine o di destinazione e sono tutti scritti per essere eseguiti nell'utilità della linea di comando SQL*Plus. Per ulteriori informazioni sull'utilizzo di questa utilità, consulta [A Using SQL Command Line](#) nella documentazione di Oracle.

Prima di eseguire lo script, assicurati che l'account utente in uso disponga delle autorizzazioni necessarie per accedere al database Oracle. Le impostazioni delle autorizzazioni mostrate presuppongono che l'utente sia stato creato come segue.

```
CREATE USER script_user IDENTIFIED BY password;
```

Per un database on-premise, imposta per *script_user* le autorizzazioni minime come illustrato di seguito.

```
GRANT CREATE SESSION TO script_user;  
GRANT SELECT on V$DATABASE to script_user;  
GRANT SELECT on V$VERSION to script_user;  
GRANT SELECT on GV$SGA to script_user;  
GRANT SELECT on GV$INSTANCE to script_user;  
GRANT SELECT on GV$DATAGUARD_CONFIG to script_user;  
GRANT SELECT on GV$LOG to script_user;  
GRANT SELECT on DBA_TABLESPACES to script_user;  
GRANT SELECT on DBA_DATA_FILES to script_user;  
GRANT SELECT on DBA_SEGMENTS to script_user;  
GRANT SELECT on DBA_LOBS to script_user;  
GRANT SELECT on V$ARCHIVED_LOG to script_user;  
GRANT SELECT on DBA_TAB_MODIFICATIONS to script_user;  
GRANT SELECT on DBA_TABLES to script_user;  
GRANT SELECT on DBA_TAB_PARTITIONS to script_user;  
GRANT SELECT on DBA_MVIEWS to script_user;  
GRANT SELECT on DBA_OBJECTS to script_user;
```

```

GRANT SELECT on DBA_TAB_COLUMNS to script_user;
GRANT SELECT on DBA_LOG_GROUPS to script_user;
GRANT SELECT on DBA_LOG_GROUP_COLUMNS to script_user;
GRANT SELECT on V$ARCHIVE_DEST to script_user;
GRANT SELECT on DBA_SYS_PRIVS to script_user;
GRANT SELECT on DBA_TAB_PRIVS to script_user;
GRANT SELECT on DBA_TYPES to script_user;
GRANT SELECT on DBA_CONSTRAINTS to script_user;
GRANT SELECT on V$TRANSACTION to script_user;
GRANT SELECT on GV$ASM_DISK_STAT to script_user;
GRANT SELECT on GV$SESSION to script_user;
GRANT SELECT on GV$SQL to script_user;
GRANT SELECT on DBA_ENCRYPTED_COLUMNS to script_user;
GRANT SELECT on DBA_PDBS to script_user;

GRANT EXECUTE on dbms_utility to script_user;

```

Per un database Amazon RDS, imposta le autorizzazioni minime come illustrato di seguito.

```

GRANT CREATE SESSION TO script_user;
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$DATABASE', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$VERSION', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_$SGA', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_$INSTANCE', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_
$DATAGUARD_CONFIG', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_$LOG', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TABLESPACES', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_DATA_FILES', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_SEGMENTS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_LOBS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$ARCHIVED_LOG', 'script_user', 'SELECT');
exec
  rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_MODIFICATIONS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TABLES', 'script_user', 'SELECT');
exec
  rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_PARTITIONS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_MVIEWS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_OBJECTS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_COLUMNS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_LOG_GROUPS', 'script_user', 'SELECT');
exec
  rdsadmin.rdsadmin_util.grant_sys_object('DBA_LOG_GROUP_COLUMNS', 'script_user', 'SELECT');

```



```
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$ARCHIVE_DEST', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_SYS_PRIVS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TAB_PRIVS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_TYPES', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_CONSTRAINTS', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('V_$TRANSACTION', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_
$ASM_DISK_STAT', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_$SESSION', 'script_user', 'SELECT');
exec rdsadmin.rdsadmin_util.grant_sys_object('GV_$SQL', 'script_user', 'SELECT');
exec
  rdsadmin.rdsadmin_util.grant_sys_object('DBA_ENCRYPTED_COLUMNS', 'script_user', 'SELECT');

exec rdsadmin.rdsadmin_util.grant_sys_object('DBA_PDBS', 'script_user', 'SELECT');

exec rdsadmin.rdsadmin_util.grant_sys_object('DBMS_UTILITY', 'script_user', 'EXECUTE');
```

Di seguito sono riportate le indicazioni per scaricare, rivedere ed eseguire ogni script di supporto SQL*Plus disponibile per Oracle. Viene anche descritto in che modo puoi esaminare e caricare l'output nel tuo caso del Supporto AWS.

Argomenti

- [Script awsdms_support_collector_oracle.sql](#)

Script awsdms_support_collector_oracle.sql

Scarica lo script [awsdms_support_collector_oracle.sql](#).

Questo script raccoglie informazioni sulla configurazione del database Oracle. Ricordati di controllare il checksum dello script e, se il checksum esegue la verifica, esamina il codice SQL contenuto nello script per commentare le parti che non desideri eseguire. Una volta che l'integrità e il contenuto sono validi, puoi eseguire lo script.

Per eseguire lo script e caricare i risultati nel caso di supporto

1. Esegui lo script dall'ambiente di database utilizzando la seguente linea di comando SQL*Plus.

```
SQL> @awsdms_support_collector_oracle.sql
```

<result>

Lo script visualizza una breve descrizione e la richiesta di continuare o interrompere l'esecuzione. Premi [Invio] per continuare.

</result>

2. Alla successiva richiesta, immetti il nome di uno solo degli schemi che vuoi migrare.
3. Alla successiva richiesta, immetti il nome dell'utente (*script_user*) che hai definito per la connessione al database.
4. Alla successiva richiesta, immetti il numero di giorni per i dati che desideri esaminare o accetta il valore predefinito. Lo script quindi raccoglie i dati specificati dal database.

<result>

Una volta completato, lo script visualizza il nome del file HTML di output, ad esempio `dms_support_oracle-2020-06-22-13-20-39-ORCL.html`. Lo script salva questo file nella directory di lavoro.

</result>

5. Esamina il file HTML e rimuovi tutte le informazioni che non desideri condividere. Quando il file HTML è accettabile per la condivisione, caricalo nel tuo caso del Supporto AWS. Per ulteriori informazioni sul caricamento del file, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Script di supporto per la diagnostica SQL Server

Di seguito è riportata una descrizione degli script di supporto per la diagnostica disponibili per analizzare un database on-premise o Amazon RDS per SQL Server nella configurazione di migrazione AWS DMS. Questi script funzionano con un endpoint di origine o di destinazione. Per un database on-premise, esegui questi script nell'utilità della linea di comando `sqlcmd`. Per ulteriori informazioni sull'utilizzo di questa utilità, consulta [sqlcmd - Use the utility](#) nella documentazione di Microsoft.

Non è possibile connettersi a un database Amazon RDS utilizzando l'utilità della linea di comando `sqlcmd`. Esegui questi script usando qualsiasi strumento client che si connetta ad Amazon RDS SQL Server.

Prima di eseguire lo script, assicurati che l'account utente in uso disponga delle autorizzazioni necessarie per accedere al database SQL Server. Sia per un database on-premise che per un database Amazon RDS, puoi utilizzare le stesse autorizzazioni che usi per accedere al database SQL Server senza il ruolo SysAdmin.

Argomenti

- [Impostazione delle autorizzazioni minime per un database SQL Server on-premise](#)
- [Impostazione delle autorizzazioni minime per un database Amazon RDS SQL Server](#)
- [Configurazione della replica continua su un SQL Server autonomo senza il ruolo sysadmin](#)
- [Configurazione della replica continua su SQL Server in un ambiente di gruppo di disponibilità senza il ruolo sysadmin](#)
- [Script di supporto SQL Server](#)

Impostazione delle autorizzazioni minime per un database SQL Server on-premise

Per impostare le autorizzazioni minime per l'esecuzione di un database SQL Server on-premise

1. Crea un nuovo account SQL Server con l'autenticazione tramite password utilizzando SQL Server Management Studio (SSMS), ad esempio *on-prem-user*.
2. Nella sezione Mapping utente di SSMS, scegli i database MSDB e MASTER (che forniscono l'autorizzazione pubblica) e assegna il ruolo DB_OWNER al database in cui desideri eseguire lo script.
3. Apri il menu contestuale (pulsante destro del mouse) del nuovo account, scegli Sicurezza e assegna esplicitamente il privilegio Connect SQL.
4. Esegui i seguenti comandi per l'assegnazione.

```
GRANT VIEW SERVER STATE TO on-prem-user;  
USE MSDB;  
GRANT SELECT ON MSDB.DBO.BACKUPSET TO on-prem-user;  
GRANT SELECT ON MSDB.DBO.BACKUPMEDIAFAMILY TO on-prem-user;  
GRANT SELECT ON MSDB.DBO.BACKUPFILE TO on-prem-user;
```

Impostazione delle autorizzazioni minime per un database Amazon RDS SQL Server

Per impostare le autorizzazioni minime per un database Amazon RDS SQL Server

1. Crea un nuovo account SQL Server con l'autenticazione tramite password utilizzando SQL Server Management Studio (SSMS), ad esempio *rds-user*.
2. Nella sezione Mapping utente di SSMS, scegli il database MSDB (che fornisce l'autorizzazione pubblica) e assegna il ruolo DB_OWNER al database in cui desideri eseguire lo script.

3. Apri il menu contestuale (pulsante destro del mouse) del nuovo account, scegli Sicurezza e assegna esplicitamente il privilegio Connect SQL.
4. Esegui i seguenti comandi per l'assegnazione.

```
GRANT VIEW SERVER STATE TO rds-user;  
USE MSDB;  
GRANT SELECT ON MSDB.DBO.BACKUPSET TO rds-user;  
GRANT SELECT ON MSDB.DBO.BACKUPMEDIAFAMILY TO rds-user;  
GRANT SELECT ON MSDB.DBO.BACKUPFILE TO rds-user;
```

Configurazione della replica continua su un SQL Server autonomo senza il ruolo sysadmin

In questa sezione viene descritto come configurare la replica continua per un'origine database SQL Server indipendente che non richieda all'account utente di disporre di privilegi sysadmin.

Note

Dopo aver eseguito i passaggi indicati in questa sezione, l'utente DMS non sysadmin disporrà delle autorizzazioni necessarie per:

- Leggere le modifiche dal file di log delle transazioni online
- Accedere al disco per leggere le modifiche dai file di backup del log delle transazioni
- Aggiungere o modificare la pubblicazione utilizzata da DMS
- Aggiungere articoli alla pubblicazione

1. Configura Microsoft SQL Server per la replica come descritto in [Acquisizione delle modifiche ai dati per SQL Server autogestito on-premise o su Amazon EC2](#).
2. Abilita la replica MS-REPLICATION sul database di origine. È possibile abilitare la replica manualmente oppure eseguendo l'attività una sola volta come utente sysadmin.
3. Crea lo schema awsdms nel database di origine utilizzando lo script seguente:

```
use master  
go  
create schema awsdms  
go
```

```
-- Create the table valued function [awsdms].[split_partition_list] on the Master
database, as follows:
USE [master]
GO

set ansi_nulls on
go

set quoted_identifier on
go

if (object_id('[awsdms].[split_partition_list]','TF')) is not null

drop function [awsdms].[split_partition_list];

go

create function [awsdms].[split_partition_list]

(

@plist varchar(8000), --A delimited list of partitions

@dlim nvarchar(1) --Delimiting character

)

returns @partitionsTable table --Table holding the BIGINT values of the string
fragments

(

pid bigint primary key

)

as

begin

declare @partition_id bigint;
```

```
declare @dml_pos integer;

declare @dml_len integer;

set @dml_len = len(@dml);

while (charindex(@dml,@plist)>0)

begin

set @dml_pos = charindex(@dml,@plist);

set @partition_id = cast( ltrim(rtrim(substring(@plist,1,@dml_pos-1))) as bigint);

insert into @partitionsTable (pid) values (@partition_id)

set @plist = substring(@plist,@dml_pos+@dml_len,len(@plist));

end

set @partition_id = cast (ltrim(rtrim(@plist)) as bigint);

insert into @partitionsTable (pid) values ( @partition_id );

return

end

GO
```

4. Crea la procedura [awsdms].[rtm_dump_dblog] nel database master utilizzando lo script seguente:

```
use [MASTER]

go

if (object_id('[awsdms].[rtm_dump_dblog]','P')) is not null drop procedure
[awsdms].[rtm_dump_dblog];
go

set ansi_nulls on
```

```
go

set quoted_identifier on
GO

CREATE procedure [awsdms].[rtm_dump_dblog]

(

@start_lsn varchar(32),

@seqno integer,

@filename varchar(260),

@partition_list varchar(8000), – A comma delimited list: P1,P2,... Pn

@programmed_filtering integer,

@minPartition bigint,

@maxPartition bigint

)

as begin

declare @start_lsn_cmp varchar(32); – Stands against the GT comparator

SET NOCOUNT ON – – Disable "rows affected display"

set @start_lsn_cmp = @start_lsn;

if (@start_lsn_cmp) is null

set @start_lsn_cmp = '00000000:00000000:0000';

if (@partition_list is null)

begin

RAISERROR ('Null partition list waspassed',16,1);
```

```
return

end

if (@start_lsn) is not null

set @start_lsn = '0x'+@start_lsn;

if (@programmed_filtering=0)

SELECT

[Current LSN],

[operation],

[Context],

[Transaction ID],

[Transaction Name],

[Begin Time],

[End Time],

[Flag Bits],

[PartitionID],

[Page ID],

[Slot ID],

[RowLog Contents 0],

[Log Record],

[RowLog Contents 1]

FROM
```



```
fn_dump_dblog (
@start_lsn, NULL, N'DISK', @seqno, @filename,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default)
where [Current LSN] collate SQL_Latin1_General_CP1_CI_AS > @start_lsn_cmp collate
SQL_Latin1_General_CP1_CI_AS
and
(
( [operation] in ('LOP_BEGIN_XACT', 'LOP_COMMIT_XACT', 'LOP_ABORT_XACT') )
or
( [operation] in ('LOP_INSERT_ROWS', 'LOP_DELETE_ROWS', 'LOP_MODIFY_ROW') )
and
( ( [context] in ('LCX_HEAP', 'LCX_CLUSTERED', 'LCX_MARK_AS_GHOST') ) or ([context] =
'LCX_TEXT_MIX' and (datalength([RowLog Contents 0]) in (0,1))))
and [PartitionID] in ( select * from master.awsdms.split_partition_list
(@partition_list, ', '))
```

```
)  
  
or  
  
([operation] = 'LOP_HOBT_DDL')  
  
)  
  
else  
  
SELECT  
  
[Current LSN],  
  
[operation],  
  
[Context],  
  
[Transaction ID],  
  
[Transaction Name],  
  
[Begin Time],  
  
[End Time],  
  
[Flag Bits],  
  
[PartitionID],  
  
[Page ID],  
  
[Slot ID],  
  
[RowLog Contents 0],  
  
[Log Record],  
  
[RowLog Contents 1] – After Image  
  
FROM
```

```
fn_dump_dblog (
@start_lsn, NULL, N'DISK', @seqno, @filename,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default,
default, default, default, default, default, default, default)
where [Current LSN] collate SQL_Latin1_General_CP1_CI_AS > @start_lsn_cmp collate
SQL_Latin1_General_CP1_CI_AS
and
(
( [operation] in ('LOP_BEGIN_XACT','LOP_COMMIT_XACT','LOP_ABORT_XACT') )
or
( [operation] in ('LOP_INSERT_ROWS','LOP_DELETE_ROWS','LOP_MODIFY_ROW')
and
( ( [context] in ('LCX_HEAP','LCX_CLUSTERED','LCX_MARK_AS_GHOST') ) or ([context] =
'LCX_TEXT_MIX' and (datalength([RowLog Contents 0]) in (0,1))))
and ([PartitionID] is not null) and ([PartitionID] >= @minPartition and
[PartitionID]<=@maxPartition)
)
```

```
or

([operation] = 'LOP_HOBT_DDL')

)

SET NOCOUNT OFF – Re-enable "rows affected display"

end

GO
```

5. Crea il certificato nel database master utilizzando lo script seguente:

```
Use [master]
Go

CREATE CERTIFICATE [awsdms_rtm_dump_dblog_cert] ENCRYPTION BY PASSWORD =
  N'@5trongpassword'

WITH SUBJECT = N'Certificate for FN_DUMP_DBLOG Permissions';
```

6. Crea l'accesso del certificato utilizzando lo script seguente:

```
Use [master]
Go

CREATE LOGIN awsdms_rtm_dump_dblog_login FROM CERTIFICATE
  [awsdms_rtm_dump_dblog_cert];
```

7. Aggiungi l'accesso al ruolo del server sysadmin utilizzando lo script seguente:

```
ALTER SERVER ROLE [sysadmin] ADD MEMBER [awsdms_rtm_dump_dblog_login];
```

8. Aggiungi la firma a [master].[awsdms].[rtm_dump_dblog] con il certificato utilizzando lo script seguente:

```
Use [master]
GO
ADD SIGNATURE
```

```
TO [master].[awsdms].[rtm_dump_dblog] BY CERTIFICATE [awsdms_rtm_dump_dblog_cert]
WITH PASSWORD = '@5trongpassword';
```

Note

Se la stored procedure viene ricreata, è necessario aggiungere nuovamente la firma.

9. Crea [awsdms].[rtm_position_1st_timestamp] sul database master utilizzando lo script seguente:

```
use [master]
if object_id('[awsdms].[rtm_position_1st_timestamp]','P') is not null
DROP PROCEDURE [awsdms].[rtm_position_1st_timestamp];
go
create procedure [awsdms].[rtm_position_1st_timestamp]
(
  @dbname          sysname,      -- Database name
  @seqno          integer,      -- Backup set sequence/position number
  @filename       varchar(260), -- The backup filename
  @1stTimeStamp   varchar(40)   -- The timestamp to position by
)
as begin

SET NOCOUNT ON      -- Disable "rows affected display"

declare @firstMatching table
(
  cLsn varchar(32),
  bTim datetime
)

declare @sql nvarchar(4000)
declare @nl          char(2)
declare @tb          char(2)
declare @fnameVar   nvarchar(254) = 'NULL'

set @nl = char(10); -- New line
set @tb = char(9)   -- Tab separator

if (@filename is not null)
set @fnameVar = '''+@filename +''''
```


12. Aggiungi l'accesso al ruolo sysadmin utilizzando lo script seguente:

```
ALTER SERVER ROLE [sysadmin] ADD MEMBER [awsdms_rtm_position_1st_timestamp_login];
```


13. Aggiungi la firma a [master].[awsdms].[rtm_position_1st_timestamp] con il certificato utilizzando lo script seguente:

```
Use [master]
GO
ADD SIGNATURE
TO [master].[awsdms].[rtm_position_1st_timestamp]
BY CERTIFICATE [awsdms_rtm_position_1st_timestamp_cert]
WITH PASSWORD = '@5trongpassword';
```

14. Fornisci all'utente DMS l'accesso in esecuzione alla nuova stored procedure utilizzando lo script seguente:

```
use master
go
GRANT execute on [awsdms].[rtm_position_1st_timestamp] to dms_user;
```

15. Crea un utente con le autorizzazioni e i ruoli descritti di seguito in ciascuno dei seguenti database:

 Note

È necessario creare l'account utente dmsnosysadmin con lo stesso SID per ogni replica. La seguente query SQL può verificare il valore SID dell'account dmsnosysadmin per ogni replica. Per ulteriori informazioni sulla creazione di un utente, consulta [CREATE USER \(Transact-SQL\)](#) nella [documentazione di Microsoft SQL Server](#). Per ulteriori informazioni sulla creazione di account utente SQL per il database Azure SQL, consulta [Active geo-replication](#).

```
use master
go
grant select on sys.fn_dblog to [DMS_user]
grant view any definition to [DMS_user]
grant view server state to [DMS_user]-(should be granted to the login).
grant execute on sp_repldone to [DMS_user]
```

```
grant execute on sp_replincrementlsn to [DMS_user]
grant execute on sp_addpublication to [DMS_user]
grant execute on sp_addarticle to [DMS_user]
grant execute on sp_articlefilter to [DMS_user]
grant select on [awsdms].[split_partition_list] to [DMS_user]
grant execute on [awsdms].[rtm_dump_dblog] to [DMS_user]
```

```
use MSDB
go
grant select on msdb.dbo.backupset to [DMS_user]
grant select on msdb.dbo.backupmediafamily to [DMS_user]
grant select on msdb.dbo.backupfile to [DMS_user]
```

Nel database di origine esegui lo script seguente:

```
EXEC sp_addrolemember N'db_owner', N'DMS_user'
use Source_DB
go
```

16. Infine, aggiungi un attributo aggiuntivo di connessione all'endpoint SQL Server di origine:

```
enableNonSysadminWrapper=true;
```

Configurazione della replica continua su SQL Server in un ambiente di gruppo di disponibilità senza il ruolo sysadmin

In questa sezione viene descritto come configurare la replica continua per un'origine database SQL Server in un ambiente del gruppo di disponibilità che non richieda all'account utente di disporre di privilegi sysadmin.

Note


Dopo aver eseguito i passaggi indicati in questa sezione, l'utente DMS non sysadmin disporrà delle autorizzazioni necessarie per:

- Leggere le modifiche dal file di log delle transazioni online
- Accedere al disco per leggere le modifiche dai file di backup del log delle transazioni
- Aggiungere o modificare la pubblicazione utilizzata da DMS

- Aggiungere articoli alla pubblicazione

Per configurare la replica continua senza utilizzare l'utente sysadmin in un ambiente di gruppo di disponibilità

1. Configura Microsoft SQL Server per la replica come descritto in [Acquisizione delle modifiche ai dati per SQL Server autogestito on-premise o su Amazon EC2](#).
2. Abilita la replica MS-REPLICATION sul database di origine. È possibile abilitare la replica manualmente oppure eseguendo l'attività una sola volta come utente sysadmin.

 Note

È necessario configurare il distributore della replica MS-REPLICATION come locale o in modo da consentire l'accesso a utenti non sysadmin tramite il server collegato e associato.

3. Se l'opzione di endpoint Usa esclusivamente sp_repldone in un singola attività è abilitata, interrompi il processo di lettura dei log della replica MS-REPLICATION.
4. Per ogni replica completa le seguenti operazioni:
 1. Crea lo schema [awsdms][awsdms] nel database master:

```
CREATE SCHEMA [awsdms]
```

2. Crea la funzione dei valori di tabella [awsdms].[split_partition_list] nel database master:

```
USE [master]
GO

SET ansi_nulls on
GO

SET quoted_identifier on
GO

IF (object_id('[awsdms].[split_partition_list]','TF')) is not null
    DROP FUNCTION [awsdms].[split_partition_list];
GO
```

```

CREATE FUNCTION [awsdms].[split_partition_list]
(
    @plist varchar(8000),    --A delimited list of partitions
    @dlm nvarchar(1)       --Delimiting character
)
RETURNS @partitionsTable table --Table holding the BIGINT values of the string
    fragments
(
    pid bigint primary key
)
AS
BEGIN
    DECLARE @partition_id bigint;
    DECLARE @dlm_pos integer;
    DECLARE @dlm_len integer;
    SET @dlm_len = len(@dlm);
    WHILE (charindex(@dlm,@plist)>0)
    BEGIN
        SET @dlm_pos = charindex(@dlm,@plist);
        SET @partition_id = cast( ltrim(rtrim(substring(@plist,1,@dlm_pos-1))) as
bigint);
        INSERT into @partitionsTable (pid) values (@partition_id)
        SET @plist = substring(@plist,@dlm_pos+@dlm_len,len(@plist));
    END
    SET @partition_id = cast (ltrim(rtrim(@plist)) as bigint);
    INSERT into @partitionsTable (pid) values ( @partition_id );
    RETURN
END
GO

```

3. Crea la procedura [awsdms].[rtm_dump_dblog] nel database master:

```

USE [MASTER]
GO

IF (object_id('[awsdms].[rtm_dump_dblog]','P')) is not null
    DROP PROCEDURE [awsdms].[rtm_dump_dblog];
GO

SET ansi_nulls on
GO

SET quoted_identifier on

```

```
GO

CREATE PROCEDURE [awsdms].[rtm_dump_dblog]
(
    @start_lsn          varchar(32),
    @seqno              integer,
    @filename           varchar(260),
    @partition_list     varchar(8000), -- A comma delimited list: P1,P2,... Pn
    @programmed_filtering integer,
    @minPartition       bigint,
    @maxPartition       bigint
)
AS
BEGIN

    DECLARE @start_lsn_cmp varchar(32); -- Stands against the GT comparator

    SET NOCOUNT ON -- Disable "rows affected display"

    SET @start_lsn_cmp = @start_lsn;
    IF (@start_lsn_cmp) is null
        SET @start_lsn_cmp = '00000000:00000000:0000';

    IF (@partition_list is null)
        BEGIN
            RAISERROR ('Null partition list was passed',16,1);
            return
            --set @partition_list = '0,';    -- A dummy which is never matched
        END

    IF (@start_lsn) is not null
        SET @start_lsn = '0x'+@start_lsn;

    IF (@programmed_filtering=0)
        SELECT
            [Current LSN],
            [operation],
            [Context],
            [Transaction ID],
            [Transaction Name],
            [Begin Time],
            [End Time],
            [Flag Bits],
            [PartitionID],
```

```

[Page ID],
[Slot ID],
[RowLog Contents 0],
[Log Record],
[RowLog Contents 1] -- After Image
FROM
fn_dump_dblog (
    @start_lsn, NULL, N'DISK', @seqno, @filename,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default)
WHERE
    [Current LSN] collate SQL_Latin1_General_CP1_CI_AS > @start_lsn_cmp collate
SQL_Latin1_General_CP1_CI_AS -- This aims for implementing FN_DBLOG based on GT
comparator.
AND
(
    ( [operation] in ('LOP_BEGIN_XACT', 'LOP_COMMIT_XACT', 'LOP_ABORT_XACT') )
    OR
    ( [operation] in ('LOP_INSERT_ROWS', 'LOP_DELETE_ROWS', 'LOP_MODIFY_ROW')
    AND
        ( ( [context] in ('LCX_HEAP', 'LCX_CLUSTERED', 'LCX_MARK_AS_GHOST') )
or ([context] = 'LCX_TEXT_MIX') )
        AND
            [PartitionID] in ( select * from master.awsdfs.split_partition_list
(@partition_list, ','))
        )
    OR
    ([operation] = 'LOP_HOBT_DDL')
)
ELSE
SELECT
    [Current LSN],
    [operation],
    [Context],
    [Transaction ID],
    [Transaction Name],
    [Begin Time],

```

```

[End Time],
[Flag Bits],
[PartitionID],
[Page ID],
[Slot ID],
[RowLog Contents 0],
[Log Record],
[RowLog Contents 1] -- After Image
FROM
fn_dump_dblog (
    @start_lsn, NULL, N'DISK', @seqno, @filename,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default,
    default, default, default, default, default, default, default, default)
WHERE [Current LSN] collate SQL_Latin1_General_CP1_CI_AS > @start_lsn_cmp
collate SQL_Latin1_General_CP1_CI_AS -- This aims for implementing FN_DBLOG
based on GT comparator.
AND
(
    ( [operation] in ('LOP_BEGIN_XACT','LOP_COMMIT_XACT','LOP_ABORT_XACT') )
    OR
    ( [operation] in ('LOP_INSERT_ROWS','LOP_DELETE_ROWS','LOP_MODIFY_ROW')
    AND
        ( ( [context] in ('LCX_HEAP','LCX_CLUSTERED','LCX_MARK_AS_GHOST') )
or ([context] = 'LCX_TEXT_MIX') )
        AND (([PartitionID] is not null) and ([PartitionID] >= @minPartition and
[PartitionID]<=@maxPartition)
    )
    OR
    ([operation] = 'LOP_HOBT_DDL')
)
SET NOCOUNT OFF -- Re-enable "rows affected display"
END
GO

```

4. Crea un certificato nel database master:

```
USE [master]
```

```
GO
CREATE CERTIFICATE [awsdms_rtm_dump_dblog_cert]
    ENCRYPTION BY PASSWORD = N'@hardpassword1'
    WITH SUBJECT = N'Certificate for FN_DUMP_DBLOG Permissions'
```

5. Crea un accesso del certificato:

```
USE [master]
GO
CREATE LOGIN awsdms_rtm_dump_dblog_login FROM CERTIFICATE
    [awsdms_rtm_dump_dblog_cert];
```

6. Aggiungi l'accesso al ruolo del server sysadmin:

```
ALTER SERVER ROLE [sysadmin] ADD MEMBER [awsdms_rtm_dump_dblog_login];
```

7. Aggiungi la firma alla procedura [master].[awsdms].[rtm_dump_dblog] con il certificato:

```
USE [master]
GO

ADD SIGNATURE
    TO [master].[awsdms].[rtm_dump_dblog]
    BY CERTIFICATE [awsdms_rtm_dump_dblog_cert]
    WITH PASSWORD = '@hardpassword1';
```

Note

Se la stored procedure viene ricreata, è necessario aggiungere nuovamente la firma.

8. Crea la procedura [awsdms].[rtm_position_1st_timestamp] nel database master:

```
USE [master]
IF object_id('[awsdms].[rtm_position_1st_timestamp]','P') is not null
    DROP PROCEDURE [awsdms].[rtm_position_1st_timestamp];
GO
CREATE PROCEDURE [awsdms].[rtm_position_1st_timestamp]
(
    @dbname          sysname,          -- Database name
    @seqno           integer,         -- Backup set sequence/position number
    within file
    @filename        varchar(260),    -- The backup filename
```



```
SET NOCOUNT OFF      -- Re-enable "rows affected display"

END
GO
```

9. Crea un certificato nel database master:

```
USE [master]
GO
CREATE CERTIFICATE [awsdms_rtm_position_1st_timestamp_cert]
    ENCRYPTION BY PASSWORD = N'@hardpassword1'
    WITH SUBJECT = N'Certificate for FN_POSITION_1st_TIMESTAMP Permissions';
```

10. Crea un accesso del certificato:

```
USE [master]
GO
CREATE LOGIN awsdms_rtm_position_1st_timestamp_login FROM CERTIFICATE
    [awsdms_rtm_position_1st_timestamp_cert];
```

11. Aggiungi l'accesso al ruolo del server sysadmin:

```
ALTER SERVER ROLE [sysadmin] ADD MEMBER
    [awsdms_rtm_position_1st_timestamp_login];
```

12. Aggiungi la firma alla procedura [master].[awsdms].[rtm_position_1st_timestamp] con il certificato:

```
USE [master]
GO
ADD SIGNATURE
    TO [master].[awsdms].[rtm_position_1st_timestamp]
    BY CERTIFICATE [awsdms_rtm_position_1st_timestamp_cert]
    WITH PASSWORD = '@hardpassword1';
```

Note

Se la stored procedure viene ricreata, è necessario aggiungere nuovamente la firma.

13. Crea un utente con le autorizzazioni e i ruoli descritti di seguito in ciascuno dei seguenti database:

Note

È necessario creare l'account utente dmsnosysadmin con lo stesso SID per ogni replica. La seguente query SQL può verificare il valore SID dell'account dmsnosysadmin per ogni replica. Per ulteriori informazioni sulla creazione di un utente, consulta [CREATE USER \(Transact-SQL\)](#) nella [documentazione di Microsoft SQL Server](#). Per ulteriori informazioni sulla creazione di account utente SQL per il database Azure SQL, consulta [Active geo-replication](#).

```
SELECT @@servername servername, name, sid, create_date, modify_date
FROM sys.server_principals
WHERE name = 'dmsnosysadmin';
```

14 Fornisci le autorizzazioni del database master per ogni replica:

```
USE master
GO

GRANT select on sys.fn_dblog to dmsnosysadmin;
GRANT view any definition to dmsnosysadmin;
GRANT view server state to dmsnosysadmin -- (should be granted to the login).
GRANT execute on sp_repldone to dmsnosysadmin;
GRANT execute on sp_replincrementlsn to dmsnosysadmin;
GRANT execute on sp_addpublication to dmsnosysadmin;
GRANT execute on sp_addarticle to dmsnosysadmin;
GRANT execute on sp_articlefilter to dmsnosysadmin;
GRANT select on [awsdms].[split_partition_list] to dmsnosysadmin;
GRANT execute on [awsdms].[rtm_dump_dblog] to dmsnosysadmin;
GRANT execute on [awsdms].[rtm_position_1st_timestamp] to dmsnosysadmin;
```

15 Fornisci le autorizzazioni del database msdb per ogni replica:

```
USE msdb
GO

GRANT select on msdb.dbo.backupset to dmsnosysadmin
GRANT select on msdb.dbo.backupmediafamily to dmsnosysadmin
GRANT select on msdb.dbo.backupfile to dmsnosysadmin
```

16 Aggiungi il ruolo `db_owner` a `dmsnosysadmin` nel database di origine. Dal momento che il database è sincronizzato, è possibile aggiungere il ruolo solo nella replica primaria.

```
use <source DB>
GO
EXEC sp_addrolemember N'db_owner', N'dmsnosysadmin'
```

Script di supporto SQL Server

Negli argomenti seguenti viene descritto come scaricare, rivedere ed eseguire ogni script di supporto disponibile per SQL Server. Viene anche illustrato come esaminare e caricare l'output dello script nel caso del Supporto AWS.

Argomenti

- [Script `awsdms_support_collector_sql_server.sql`](#)

Script `awsdms_support_collector_sql_server.sql`

Scarica lo script [awsdms_support_collector_sql_server.sql](#).

Note

Esegui questo script di supporto per la diagnostica SQL Server solo su SQL Server 2014 e versioni successive.

Questo script raccoglie informazioni sulla configurazione del database SQL Server. Ricordati di controllare il checksum dello script e, se il checksum esegue la verifica, esamina il codice SQL contenuto nello script per commentare le parti che non desideri eseguire. Una volta che l'integrità e il contenuto sono validi, puoi eseguire lo script.

Per eseguire lo script per un database SQL Server on-premise

1. Esegui lo script utilizzando la linea di comando `sqlcmd` seguente.

```
sqlcmd -Uon-prem-user -Ppassword -SDMS-SQL17AG-N1 -y 0
-iC:\Users\admin\awsdms_support_collector_sql_server.sql -oC:\Users\admin
\DMS_Support_Report_SQLServer.html -dsqlserverdb01
```

I parametri del comando `sqlcmd` specificati sono:

- `-U`: nome dell'utente del database.
 - `-P`: password dell'utente del database.
 - `-S`: nome del server di database SQL Server.
 - `-y`: larghezza massima delle colonne di output dell'utilità `sqlcmd`. Il valore 0 specifica colonne con larghezza illimitata.
 - `-i`: percorso dello script di supporto da eseguire, in questo caso `awsdms_support_collector_sql_server.sql`.
 - `-o`: percorso del file HTML di output, con il nome file che hai specificato, contenente le informazioni di configurazione del database raccolte.
 - `-d`: nome del database SQL Server.
2. Una volta completato lo script, esamina il file HTML di output e rimuovi tutte le informazioni che non desideri condividere. Quando il file HTML è accettabile per la condivisione, caricalo nel tuo caso del Supporto AWS. Per ulteriori informazioni sul caricamento del file, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Con Amazon RDS per SQL Server, non è possibile connettersi tramite l'utilità della linea di comando `sqlcmd`, quindi utilizza la procedura seguente.

Per eseguire lo script per un database RDS SQL Server

1. Esegui lo script utilizzando qualsiasi strumento client che ti consenta di connetterti a RDS SQL Server come utente `Master` e salvare l'output come file HTML.
2. Esamina il file HTML di output e rimuovi tutte le informazioni che non desideri condividere. Quando il file HTML è accettabile per la condivisione, caricalo nel tuo caso del Supporto AWS. Per ulteriori informazioni sul caricamento del file, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Script di supporto diagnostico per database compatibili con MySQL

Di seguito sono riportati gli script di supporto diagnostico disponibili per analizzare un database on-premise o compatibile con Amazon RDS per MySQL nella configurazione di migrazione AWS DMS. Questi script funzionano con un endpoint di origine o di destinazione. Gli script sono tutti scritti per essere eseguiti sulla linea di comando MySQL SQL.

Per informazioni sull'installazione del client MySQL, consulta [Installing MySQL Shell](#) nella documentazione di MySQL. Per informazioni sull'utilizzo del client di MySQL, consulta [Using MySQL Shell Commands](#) nella documentazione di MySQL.

Prima di eseguire uno script, assicurati che l'account utente in uso disponga delle autorizzazioni necessarie per accedere al database compatibile con MySQL. Utilizza la procedura seguente per creare un account utente e fornire le autorizzazioni minime necessarie per eseguire lo script.

Per configurare un account utente con le autorizzazioni minime per eseguire gli script

1. Crea l'utente per eseguire gli script.

```
create user 'username'@'hostname' identified by password;
```

2. Assegna il comando select ai database per analizzarli.

```
grant select on database-name.* to username;  
grant replication client on *.* to username;
```

- 3.

```
grant execute on procedure mysql.rds_show_configuration to username;
```

Negli argomenti seguenti viene descritto come scaricare, rivedere ed eseguire ogni script di supporto disponibile per un database compatibile con MySQL. Viene anche illustrato come esaminare e caricare l'output dello script nel caso del Supporto AWS.

Argomenti

- [Script awsdms_support_collector_MySQL.sql](#)

Script awsdms_support_collector_MySQL.sql

Scarica lo script [awsdms_support_collector_MySQL.sql](#).

Questo script raccoglie informazioni sulla configurazione del database compatibile con MySQL. Ricordati di controllare il checksum dello script e, se il checksum esegue la verifica, esamina il codice SQL contenuto nello script per commentare le parti che non desideri eseguire. Una volta che l'integrità e il contenuto sono validi, puoi eseguire lo script.

Esegui lo script dopo la connessione all'ambiente del database tramite la linea di comando.

Per eseguire lo script e caricare i risultati nel caso di supporto

1. Connettiti al database utilizzando il comando `mysql` seguente.

```
mysql -h hostname -P port -u username database-name
```

2. Esegui lo script utilizzando il comando `mysql source` seguente.

```
mysql> source awsdms_support_collector_MySQL_compatible_DB.sql
```

Esamina il report generato e rimuovi tutte le informazioni che desideri condividere. Quando il contenuto è accettabile per la condivisione, carica il file nel tuo caso del Supporto AWS. Per ulteriori informazioni sul caricamento del file, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Note

- Se disponi già di un account utente con i privilegi richiesti descritti in [Script di supporto diagnostico per database compatibili con MySQL](#), puoi utilizzarlo per eseguire lo script.
- Ricordati di connetterti al database prima di eseguire lo script.
- Lo script genera l'output in formato testo.
- Tenendo presenti le best practice di sicurezza, se si crea un nuovo account utente solo per eseguire questo script di supporto diagnostico MySQL, si consiglia di eliminare questo account utente dopo il completamento dell'esecuzione dello script.

Script di supporto diagnostico PostgreSQL

Di seguito sono riportati gli script di supporto diagnostico disponibili per analizzare qualsiasi RDBMS PostgreSQL (on-premise, Amazon RDS o Aurora PostgreSQL) nella tua configurazione di migrazione AWS DMS. Questi script funzionano con un endpoint di origine o di destinazione. Gli script sono tutti scritti per essere eseguiti nell'utilità della linea di comando `psql`.

Prima di eseguire questi script, assicurati che l'account utente in uso disponga delle seguenti autorizzazioni necessarie per accedere a qualsiasi RDBMS PostgreSQL:

- PostgreSQL 10.x o versione successiva: un account utente con autorizzazione di esecuzione per la funzione `pg_catalog.pg_ls_waldir`.
- PostgreSQL 9.x o versioni precedenti: un account utente con autorizzazioni predefinite.

Si consiglia di utilizzare un account esistente con le autorizzazioni appropriate per eseguire questi script.

Se devi creare un nuovo account utente o fornire le autorizzazioni a un account esistente per eseguire questi script, puoi usare i seguenti comandi SQL per qualsiasi RDBMS PostgreSQL basato sulla versione PostgreSQL.

Per fornire all'account le autorizzazioni per eseguire questi script per un database PostgreSQL 10.x o versioni successive

- Esegui una di queste operazioni:
 - Per un nuovo account utente, esegui quanto segue.

```
CREATE USER script_user WITH PASSWORD 'password';  
GRANT EXECUTE ON FUNCTION pg_catalog.pg_ls_waldir TO script_user;
```

- Per un account utente esistente, esegui quanto segue.

```
GRANT EXECUTE ON FUNCTION pg_catalog.pg_ls_waldir TO script_user;
```

Per fornire all'account le autorizzazioni per eseguire questi script per un database PostgreSQL 9.x o versioni precedenti

- Esegui una di queste operazioni:
 - Per un nuovo account utente, esegui il comando seguente con le autorizzazioni predefinite.

```
CREATE USER script_user WITH PASSWORD password;
```

- Per un account utente esistente, utilizza le autorizzazioni esistenti.

Note

Questi script non supportano determinate funzionalità relative alla ricerca della dimensione del WAL per database PostgreSQL 9.x e versioni precedenti. Per ulteriori informazioni, contatta il Supporto AWS.

I seguenti argomenti descrivono come scaricare, rivedere ed eseguire ogni script di supporto disponibile per PostgreSQL. Descrivono inoltre come rivedere e caricare l'output dello script nel caso del Supporto AWS.

Argomenti

- [Script `awsdms_support_collector_postgres.sql`](#)

Script `awsdms_support_collector_postgres.sql`

Scarica lo script [awsdms_support_collector_postgres.sql](#).

Questo script raccoglie informazioni sulla configurazione del database PostgreSQL. Ricordati di verificare il checksum dello script. Se il checksum lo verifica, esamina il codice SQL contenuto nello script per commentare il codice che desideri eseguire. Una volta che l'integrità e il contenuto sono validi, puoi eseguire lo script.

Note

È possibile eseguire questo script con la versione 10 o successiva del client `psql`.

È possibile utilizzare le seguenti procedure per eseguire lo script dall'ambiente di database o dalla linea di comando. In entrambi i casi, puoi caricare il file per il Supporto AWS in un secondo momento.

Per eseguire lo script e caricare i risultati nel caso di supporto

1. Esegui una di queste operazioni:

- Esegui lo script dall'ambiente di database utilizzando la seguente linea di comando `psql`.

```
dbname=# \i awsdms_support_collector_postgres.sql
```

Alla successiva richiesta, immetti il nome di uno solo degli schemi che vuoi migrare.

Alla successiva richiesta, immetti il nome dell'utente (*script_user*) che hai definito per la connessione al database.

- Esegui lo script seguente direttamente dalla linea di comando. Questa opzione evita qualsiasi richiesta prima dell'esecuzione dello script.

```
psql -h database-hostname -p port -U script_user -d database-name -f  
awsdms_support_collector_postgres.sql
```

2. Esamina il file HTML di output e rimuovi tutte le informazioni che non desideri condividere. Quando il file HTML è accettabile per la condivisione, caricalo nel tuo caso del Supporto AWS. Per ulteriori informazioni sul caricamento del file, consulta [Utilizzo degli script di supporto per la diagnostica in AWS DMS](#).

Utilizzo dell'AMI di supporto AWS DMS diagnostico

Se si verifica un problema relativo alla rete quando si lavora con AWS DMS, il tecnico dell'assistenza potrebbe aver bisogno di ulteriori informazioni sulla configurazione di rete. Vogliamo assicurarci che AWS Support riceva quante più informazioni richieste possibile nel più breve tempo possibile. Pertanto, abbiamo sviluppato un'AMI Amazon EC2 preconfigurata con strumenti di diagnostica per AWS DMS testare il tuo ambiente di rete.

I test diagnostici installati sull'Amazon Machine Image (AMI) sono:

- Virtual Private Cloud (VPC)
- Perdita di pacchetti di rete
- Latenza di rete
- Dimensione dell'unità di trasmissione massima (MTU)

Argomenti

- [Avvia una nuova AWS DMS istanza diagnostica Amazon EC2](#)
- [Creazione di un ruolo IAM](#)
- [Esecuzione dei test diagnostici](#)
- [Fasi successive](#)

- [ID AMI per regione](#)

Note

Se riscontri problemi di prestazioni con l'origine Oracle, puoi valutare le prestazioni di lettura dei log redo o di archiviazione di Oracle per trovare i modi per migliorare le prestazioni. Per ulteriori informazioni, consulta [Valutazione delle prestazioni di lettura dei log redo o di archiviazione di Oracle](#).

Avvia una nuova AWS DMS istanza diagnostica Amazon EC2

In questa sezione viene avviata una nuova istanza Amazon EC2. Per ulteriori informazioni sull'avvio di un'istanza Amazon EC2, consulta [Tutorial: Nozioni di base sulle istanze Amazon EC2 Linux](#) nella [Guida per l'utente di Amazon EC2 per istanze Linux](#).

Avvia un'istanza Amazon EC2 con le seguenti impostazioni:

- Per Immagini di applicazioni e sistema operativo (Amazon Machine Image) cerca l'AMI DMS-DIAG-AMI. Se hai effettuato l'accesso alla console, puoi cercare l'AMI con [questa query](#). Per l'ID AMI dell'AMI di AWS diagnostica nella tua regione, consulta [ID AMI per regione](#) quanto segue.
- Per Tipo di istanza si consiglia di scegliere t2.micro.
- Per Impostazioni di rete scegli lo stesso VPC utilizzato dall'istanza di replica.

Una volta che l'istanza è attiva, connettiti all'istanza. Per ulteriori informazioni sulla connessione a un'istanza Amazon EC2 Linux, consulta [Connessione all'istanza di Linux](#).

Creazione di un ruolo IAM

Se desideri eseguire i test diagnostici sulla tua istanza di replica utilizzando le autorizzazioni minime richieste, crea un ruolo IAM che usi la seguente policy di autorizzazioni:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
```

```
        "Effect": "Allow",
        "Action": [
            "dms:DescribeEndpoints",
            "dms:DescribeTableStatistics",
            "dms:DescribeReplicationInstances",
            "dms:DescribeReplicationTasks",
            "secretsmanager:GetSecretValue"
        ],
        "Resource": "*"
    }
]
```

Associa il ruolo a un nuovo utente IAM. Per informazioni sulla creazione dei ruoli IAM, delle policy e degli utenti, consulta le sezioni seguenti nella [Guida per l'utente di IAM](#):

- [Nozioni di base su IAM](#)
- [Creazione di ruoli IAM](#)
- [Creazione di policy IAM](#)

Esecuzione dei test diagnostici

Dopo aver creato un'istanza Amazon EC2 e aver stabilito la connessione, procedi come segue per eseguire i test diagnostici sull'istanza di replica.

1. Configura la AWS CLI:

```
$ aws configure
```

Fornisci le credenziali di accesso per l'account AWS utente che desideri utilizzare per eseguire i test diagnostici. Fornisci la regione per il VPC e l'istanza di replica.

2. Visualizza le AWS DMS attività disponibili nella tua regione. Sostituisci la regione di esempio con la tua regione.

```
$ dms-report -r us-east-1 -l
```

Questo comando mostra lo stato delle attività.


```

#####
#
#
#   AWS DMS Diagnostic
#   Date: 07-13-2022
#
#
#   aws region: us-east-2
#
#
#####
==== DMS DIAG Info ====
Public IP: 3.22.100.10
Private IP: 172.30.0.240
Instance ID: i-04829b2beb8214602
Instance MAC: 02:58:04:b5:52:28
Instance Type: t2.micro
Instance Sec Group: DMS-EC2-sec-group
Instance AWS Region: us-east-2
Instance VPC Id: vpc-08ba020355d8a952e

==== Network Packet Check ====
1.) Check DMS EC2 MetaData service
>>>>Result: 10 packets transmitted, 10 packets received, 0% packet loss
    Looks good with no issue. <<<<<

2.) Check Source endpoint (dms-ec2-postgres-dev-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: 10 packets transmitted, 10 packets received, 0% packet loss
    Looks good with no issue. <<<<<

3.) Check Target endpoint (rds-postgres-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: 10 packets transmitted, 10 packets received, 0% packet loss
    Looks good with no issue. <<<<<

==== End network packet check ====

==== Network Latency Check ====
1.) Check DMS MetaData Service
>>>>Result: round-trip min/avg/max = 0.4/0.4/0.5 ms
    Looks good with no issue. <<<<<

2.) Check Source endpoint (dms-ec2-postgres-dev-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: round-trip min/avg/max = 1.0/1.1/1.2 ms
    Looks good with no issue. <<<<<

3.) Check Target endpoint (rds-postgres-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: round-trip min/avg/max = 1.4/1.4/1.5 ms
    Looks good with no issue. <<<<<

==== End network latency check ====

==== Network MTU Check ====
1.) Check DMS MetaData Service
>>>>Result: MTU setting looks good. Local MTU (9001) matches remote MTU (9001) <<<<<

2.) Check Source endpoint (dms-ec2-postgres-dev-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: MTU setting looks good. Local MTU (9001) matches remote MTU (9001) <<<<<

3.) Check Target endpoint (rds-postgres-instance-1.cucdvzaur7nk.us-east-2.rds.amazonaws.com:5432)
>>>>Result: MTU setting looks good. Local MTU (9001) matches remote MTU (9001) <<<<<

==== End network MTU check ====

```

Perform AMI Diag EC2 VPC Check**Perform Network Packet Test****Returns Test Results and Recommendation****Perform Network Latency Test****Perform Network Maximum Transmission Unit (MTU) Check**

Fasi successive

Nelle seguenti sezioni sono riportate le informazioni sulla risoluzione dei problemi in base ai risultati dei test di diagnostica di rete:

Test del VPC

Questo test verifica che l'istanza Amazon EC2 di diagnostica si trovi nello stesso VPC dell'istanza di replica. Se l'istanza Amazon EC2 di diagnostica non si trova nello stesso VPC dell'istanza di replica, terminala e creala nuovamente nel VPC corretto. Non puoi modificare il VPC di un'istanza Amazon EC2 dopo averlo creato.

Test di perdita di pacchetti di rete

Questo test invia 10 pacchetti ai seguenti endpoint e verifica l'eventuale perdita di pacchetti:

- Il servizio di metadati AWS DMS Amazon EC2 sulla porta 80
- L'endpoint di origine
- L'endpoint di destinazione

Tutti i pacchetti devono arrivare correttamente. In caso di perdita di pacchetti, rivolgiti a un tecnico della rete per determinare il problema e trovare una soluzione.

Test di latenza di rete

Questo test invia 10 pacchetti agli stessi endpoint del test precedente e verifica la latenza dei pacchetti. Tutti i pacchetti devono avere una latenza inferiore a 100 millisecondi. Se alcuni pacchetti hanno una latenza superiore a 100 millisecondi, contatta un tecnico della rete per determinare il problema e trovare una soluzione.

Test di dimensione dell'unità di trasmissione massima (MTU)

Questo test rileva la dimensione della MTU utilizzando lo strumento Traceroute sugli stessi endpoint del test precedente. Tutti i pacchetti del test devono avere la stessa dimensione della MTU. Se alcuni pacchetti hanno una dimensione della MTU diversa, contatta uno specialista di sistema per determinare il problema e trovare una soluzione.

ID AMI per regione

Per visualizzare un elenco delle AMI di diagnostica DMS disponibili nella tua AWS regione, esegui il seguente esempio di CLI AWS .

```
aws ec2 describe-images --owners 343299325021 --filters "Name=name, Values=DMS-DIAG*"
--query "sort_by(Images, &CreationDate)[-1].[Name, ImageId, CreationDate]" --output
text
```

Se l'output non mostra risultati, significa che l'AMI DMS Diagnostic non è disponibile nella tua AWS regione. La soluzione alternativa consiste nel seguire i passaggi seguenti per copiare l'AMI diagnostica da un'altra regione. Per ulteriori informazioni, consulta [Copiare un AMI](#).

- Avvia un'istanza nella regione disponibile.
- Crea l'immagine. L'immagine sarà di tua proprietà.
- Copia l'AMI nella tua regione, ad esempio la regione del Medio Oriente (Emirati Arabi Uniti).
- Avvia l'istanza nella tua regione locale.

Riferimento AWS DMS

In questa sezione di riferimento sono fornite ulteriori informazioni che potrebbero essere necessarie quando si utilizza AWS Database Migration Service (AWS DMS), tra cui le informazioni di conversione dei tipi di dati.

AWS DMS mantiene i tipi di dati quando esegui una migrazione omogenea del database in cui sia l'origine che la destinazione utilizzano lo stesso tipo di motore. Quando esegui una migrazione eterogeneo, ovvero da un tipo di motore di database a un altro, i tipi di dati vengono convertiti in un tipo intermedio. Per vedere come i tipi di dati vengono visualizzati sul database di destinazione, consulta le tabelle dei tipi di dati per i motori di database di origine e di destinazione.

Ricorda alcuni aspetti importanti dei tipi di dati durante la migrazione di un database:

- Il tipo di dati FLOAT è intrinsecamente un algoritmo di approssimazione. Quando inserisci un valore specifico in FLOAT, può essere rappresentato in maniera diversa nel database. Questa differenza è dovuta al fatto che FLOAT non è un tipo di dati esatto, ad esempio un tipo di dati decimale, come NUMBER o NUMBER(p,s). Pertanto, il valore interno di FLOAT archiviato nel database può variare rispetto al valore inserito. Pertanto, questo valore migrato di un FLOAT potrebbe non corrispondere esattamente al valore nel database di origine.

Per ulteriori informazioni su questo problema, consulta i seguenti articoli:

- [Virgola mobile IEEE](#) in Wikipedia
- [IEEE floating-point representation](#) in Microsoft Learn
- [Why floating-point numbers may lose precision](#) in Microsoft Learn

Argomenti


- [Tipi di dati per AWS Database Migration Service](#)

Tipi di dati per AWS Database Migration Service

AWS Database Migration Service utilizza i tipi di dati integrati per eseguire la migrazione da un tipo di motore di database di origine a uno di destinazione. La tabella seguente mostra i tipi di dati integrati e le relative descrizioni.

Tipi di dati AWS DMS	Descrizione
STRING	Una stringa di caratteri.
WSTRING	Una stringa di caratteri a doppio byte.
BOOLEAN	Un valore booleano.
BYTE	Un valore di dati binari.
DATE	Un valore di data: anno, mese, giorno.
TIME	Una valore di ora: ora, minuti, secondi.
DATETIME	Un valore di timestamp: anno, mese, giorno, ora, minuto, secondo, secondi frazionati. I secondi frazionati hanno una scala massima di 9 cifre. È supportato il seguente formato: YYYY:MM:DD HH:MM:SS.F(9). Per Amazon S3 Select e Amazon S3 Glacier Select, il formato del tipo di dati DATETIME è diverso. Per ulteriori informazioni, consulta la descrizione del tipo di dati timestamp primitivo in Tipi di dati nella Guida per l'utente di Amazon Simple Storage Service.
INT1	Intero con segno da un byte.
INT2	Intero con segno da due byte.
INT4	Intero con segno da quattro byte.
INT8	Intero con segno da otto byte.
NUMERIC	Valore numerico esatto con precisione e scala fisse.
REAL4	Valore in virgola mobile a precisione singola.
REAL8	Valore in virgola mobile a precisione doppia.

Tipi di dati AWS DMS	Descrizione
UINT1	Intero senza segno da un byte.
UINT2	Intero senza segno da due byte.
UINT4	Intero senza segno da quattro byte.
UINT8	Intero senza segno da otto byte.
BLOB	Oggetto binario di grandi dimensioni.
CLOB	Oggetto carattere di grandi dimensioni.
NCLOB	Oggetto carattere nativo di grandi dimensioni.

 Note

AWS DMS non è in grado di eseguire la migrazione di nessun tipo di dati LOB verso endpoint Apache Kafka.

AWS Note di rilascio DMS

Di seguito, puoi trovare le note di rilascio per le versioni correnti e precedenti di AWS Database Migration Service (AWS DMS).

AWS DMS non fa distinzione tra versioni principali e secondarie quando si abilita l'aggiornamento automatico della versione per l'istanza di replica. DMS aggiorna automaticamente la versione dell'istanza di replica durante la finestra di manutenzione se la versione è obsoleta.

Tieni presente che per aggiornare manualmente la versione dell'istanza di replica (utilizzando l'API o la CLI) dalla versione 3.4.x alla 3.5.x, devi impostare il parametro su `AllowMajorVersionUpgrade true`. Per informazioni sul `AllowMajorVersionUpgrade` parametro, [ModifyReplicationInstance](#) consultate la documentazione dell'API DMS.

Note

L'attuale versione predefinita del motore per AWS DMS è la 3.5.1.

La tabella seguente mostra le seguenti date per le versioni DMS attive:

- Data di rilascio della versione
- La data dopo la quale non è possibile creare nuove istanze con la versione
- La data in cui DMS aggiorna automaticamente le istanze di quella versione (la data EOL)

Versione	Data di rilascio	Nessuna data di nuova istanza	Data di fine vita
3.5.3	17 maggio 2024	31 agosto 2025	31 ottobre 2025
3.5.2	29 ottobre 2023	30 marzo 2025	29 aprile 2025
3.5.1	30 giugno 2023	30 novembre 2024	30 gennaio 2025
3.4.7	31 maggio 2022	30 luglio 2024	29 agosto 2024
3.4.6	30 novembre 2021	26 maggio 2024	27 giugno 2024

AWS Note di rilascio di Database Migration Service 3.5.3

AWS DMS Nuove funzionalità nella versione 3.5.3

Nuova caratteristica o miglioramento	Descrizione
Endpoint sorgente PostgreSQL migliorato per il supporto di Babelfish	AWS DMS ha migliorato il suo endpoint sorgente PostgreSQL per supportare i tipi di dati Babelfish. Per ulteriori informazioni, consulta Utilizzo di un database PostgreSQL come origine AWS DMS .
Supporto per S3 Parquet come sorgente	AWS DMS supporta S3 Parquet come sorgente. Per ulteriori informazioni, consulta Utilizzo di Amazon S3 come sorgente per AWS DMS
Supporto per PostgreSQL 16.x	AWS DMS supporta PostgreSQL versione 16.x. Per ulteriori informazioni, consulta Utilizzo di un database PostgreSQL come origine AWS DMS e Utilizzo di un database PostgreSQL come destinazione per AWS Database Migration Service .
Throughput migliorato per le migrazioni a pieno carico da Oracle ad Amazon Redshift	AWS DMS Serverless offre prestazioni di throughput notevolmente migliorate per le migrazioni a pieno carico da Oracle ad Amazon Redshift. Per ulteriori informazioni, consulta Throughput migliorato per le migrazioni a pieno carico da Oracle ad Amazon Redshift .

AWS DMS la versione 3.5.3 include i seguenti problemi risolti:

Problemi risolti nella versione DMS 3.5.3 del 17 maggio 2024

Problema risolto	Descrizione
Funzione di override della convalida dei dati	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale DMS non rispettava il filtraggio dell'origine quando un'azione della regola era impostata nelle mappature delle tabelle. <code>override-validation-function</code>
Errori CDC di origine MySQL	È stato risolto un problema relativo a MySQL come origine a causa del quale la migrazione CDC non funzionava con la codifica UTF16.

Problema risolto	Descrizione
Differenze nella convalida dei dati e nella collazione	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale DMS non applicava correttamente l'impostazione dell' <code>HandleCollationDiff</code> attività quando veniva utilizzato il filtraggio delle colonne.
Sospensione dell'attività di convalida dei dati.	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale l'attività DMS si bloccava con un errore «targetis null».
Fallimenti delle attività nella replica da PostgreSQL a PostgreSQL.	È stato risolto un problema per le migrazioni da PostgreSQL a PostgreSQL a causa del quale un'attività DMS non funzionava durante l'inserimento di dati LOB nella destinazione durante la replica CDC.
Perdita di dati con PostgreSQL come fonte	È stato risolto un problema relativo a PostgreSQL come fonte in cui si verificava la perdita di dati in determinati scenari limite.
Errori CDC di origine MySQL 5.5	È stato risolto un problema relativo a MySQL come origine a causa del quale la replica CDC non funzionava con MySQL versione 5.5.
Problema relativo alla tabella IOT di origine Oracle.	È stato risolto un problema relativo a Oracle come origine a causa del quale DMS non replicava correttamente UPDATE le istruzioni per le tabelle IOT con la registrazione supplementare abilitata su tutte le colonne.
Fonte MySQL (LOBs)	È stato risolto un problema relativo alle migrazioni da MySQL a Redshift a causa del fallimento dell'attività DMS a causa dei LOB che superavano la dimensione massima consentita da Redshift.
Problema di convalida con <code>SkipLobColumns</code>	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale l'attività DMS non funzionava <code>SkipLobColumns = true</code> quando una chiave primaria si trovava nell'ultima colonna della tabella di origine.

Problema risolto	Descrizione
Salta la convalida in cui si trova la chiave univoca null	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale DMS non saltava correttamente le righe con chiavi univoche nulle.
Miglioramenti alla convalida dei dati per l'operatore Oracle. COLLATE	È stato risolto un problema relativo alla funzionalità di convalida dei dati che impediva la convalida con un errore di sintassi nelle versioni di Oracle precedenti alla 12.2.
Gestione degli errori durante il caricamento completo	È stato risolto un problema per PostgreSQL come destinazione in cui l'attività si bloccava durante la fase di caricamento completo dopo un errore di tabella causato da dati non validi.
Rivalidazione delle attività di sola convalida CDC	È stata migliorata la funzionalità di convalida dei dati per consentire la riconvalida di un'attività di sola convalida CDC.
S3 come problema obiettivo CdcMaxBatchInterval Out of Memory	Risolto un problema relativo a S3 come destinazione a causa del quale l'attività DMS avrebbe avuto esito negativo se la condizione di memoria esaurita era impostata. CdcMaxBatchInterval
Driver di origine Oracle	È stato aggiornato il driver sorgente DMS Oracle dalla v12.2 alla v19.18.
Avviso di troncamento LOB con sorgente SQL Server	Registrazione migliorata per SQL Server come sorgente per mostrare avvisi sul troncamento del LOB durante il CDC.
Miglioramenti apportati al lettore binario di Oracle	Il lettore binario sorgente Oracle è stato migliorato per supportare quanto segue: <ul style="list-style-type: none">• Piattaforma Big Endian• Suggerimenti DML paralleli con compressione HCC• Compressioni Oracle avanzate con Golden Gate abilitate

AWS Note di rilascio di Database Migration Service 3.5.2

AWS DMS Nuove funzionalità nella versione 3.5.2

Nuova caratteristica o miglioramento	Descrizione
Convalida dei dati Redshift	AWS DMS ora supporta la convalida dei dati nei target Redshift.
Supporto per Microsoft SQL Server versione 2022 come origine e destinazione.	AWS DMS ora supporta l'utilizzo di Microsoft SQL Server versione 2022 come origine e destinazione.
IBM Db2 LUW come destinazione	AWS DMS ora supporta IBM Db2 LUW come destinazione. Utilizzando AWS DMS, ora puoi eseguire migrazioni in tempo reale da IBM Db2 LUW a IBM Db2 LUW.

AWS DMS la versione 3.5.2 include i seguenti problemi risolti:

Problemi risolti nella versione di manutenzione di DMS 3.5.2 del 29 aprile 2024

Problema risolto	Descrizione
IBM Db2 target segmentato o a pieno carico	È stato aggiunto il supporto per il pieno carico segmentato con IBM Db2 come destinazione.
Amazon Timestream come impostazioni di destinazione	È stata migliorata la gestione delle impostazioni di timestamp non valide e delle operazioni di tabella non supportate per Timestream come destinazione.
Arresto anomalo dell'attività con filtro a colonne	È stato risolto un problema a causa del quale un'attività si bloccava durante l'utilizzo di un filtro su una colonna che DMS aggiungeva dinamicamente utilizzando una regola di trasformazione.
Registrazione della lettura del file di scambio delle transazioni	È stata aggiunta la registrazione per mostrare quando DMS sta leggendo i file di scambio delle transazioni.

Problema risolto	Descrizione
S3 come obiettivo con CdcInsertsAndUpdates	Risolto un problema relativo a S3 come bersaglio a causa del quale un'attività si bloccava quando è in corso <code>true</code> e <code>PreserveTransactions</code> quando <code>CdcInsertsAndUpdates</code> è <code>true</code>
Operatori negativi del filtro di origine	È stato risolto un problema per cui l'operatore del filtro di origine, impostato su un operatore negativo, aveva un comportamento errato se sulla stessa colonna era definita una regola di trasformazione.
È stata aggiunta la registrazione per quando DMS sospende la lettura dalla fonte	Registrazione migliorata per mostrare quando DMS sospende temporaneamente la lettura dalla fonte per migliorare le prestazioni.
Filtri di origine con caratteri sfuggiti	È stato risolto un problema relativo ai filtri di origine in cui DMS applica i caratteri di escape alle tabelle appena create durante CDC.
PostgreSQL come destinazione, eliminazioni replicate in modo errato	È stato risolto un problema per PostgreSQL come destinazione in cui DMS replica le eliminazioni come valori nulli.
Miglioramenti alla registrazione di Oracle as a source	Registrazione avanzata per Oracle come fonte per rimuovere codici di errore estranei.
Registrazione migliorata delle limitazioni XMLTYPE	Registrazione migliorata per Oracle come fonte per mostrare la mancanza di supporto da parte di DMS per la modalità LOB completa per il tipo di dati. XMLTYPE
Perdita di dati MySQL	È stato risolto un problema per MySQL come destinazione in cui i metadati delle colonne danneggiati potevano causare arresti anomali delle attività o perdita di dati.
Filtro applicato a una nuova colonna	È stato risolto un problema durante il caricamento completo in cui DMS ignorava un filtro aggiunto da una regola di trasformazione a una nuova colonna.

Problema risolto	Descrizione
S3 come obiettivo: problema di convalida	Risolto un problema relativo a S3 come destinazione a causa del quale la convalida dei dati non riusciva durante la migrazione di più tabelle con definizioni di partizionamento di convalida diverse.
Arresto anomalo dell'attività solo CDC	Risolto un problema relativo alle attività riservate ai soli CDC in cui l'attività si bloccava quando lo era. <code>TaskRecoveryTableEnabled true</code>
Collazioni incompatibili tra MySQL e MariaDB	È stato risolto un problema per le migrazioni da MySQL a MariaDB in cui DMS non migra le tabelle MySQL v8 con regole di confronto. <code>tf8mb4_0900_ai_ci</code>
L'attività si blocca con <code>BatchApplyEnabled</code>	È stato risolto un problema relativo alla funzionalità di applicazioni in batch a causa del quale l'attività non riusciva in determinate condizioni.
Caratteri non UTF-8 in Amazon DocumentDB	È stato aggiunto il supporto per caratteri non UTF-8 per gli endpoint Amazon DocumentDB.
Arresto anomalo dell'attività Batch Apply	È stato risolto un problema relativo alla funzionalità Batch Apply a causa del quale l'attività DMS si bloccava durante la replica di transazioni di grandi dimensioni.
Gestione del rollback delle transazioni Db2	È stato risolto un problema relativo a Db2 come origine in cui DMS replicava un INSERT file sulla destinazione, nonostante fosse ripristinato sull'origine.
Convalida con filtri di origine	È stato risolto un problema per cui la convalida non rispettava i filtri di origine.

AWS Note di rilascio di Database Migration Service 3.5.1

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS Database Migration Service (AWS DMS) versione 3.5.1.

Nuova caratteristica o miglioramento	Descrizione
Supporto per PostgreSQL 15.x	AWS DMS la versione 3.5.1 supporta PostgreSQL versione 15.x. Per ulteriori informazioni, consulta Utilizzo di PostgreSQL come origine e Utilizzo di PostgreSQL come destinazione .
Supporto per i cluster elastici Amazon DocumentDB con raccolte partizionate	AWS DMS la versione 3.5.1 supporta Amazon DocumentDB Elastic Clusters con raccolte ripartite. Per ulteriori informazioni, consulta Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service .
Redshift serverless come destinazione	Supporto per l'utilizzo di Amazon Redshift serverless come endpoint di destinazione. Per ulteriori informazioni, consulta Utilizzo di un database Amazon Redshift come destinazione per AWS Database Migration Service .
Impostazioni degli endpoint Babelfish	Impostazioni avanzate degli endpoint di destinazione PostgreSQL per fornire supporto per Babelfish. Per ulteriori informazioni, consulta Utilizzo di un database PostgreSQL come destinazione per AWS Database Migration Service .
Transazioni aperte per un'origine Oracle	AWS DMS 3.5.1 migliora la metodologia di gestione delle transazioni aperte quando si avvia un'attività solo CDC dalla posizione iniziale per una fonte Oracle. Per ulteriori informazioni, consulta <code>OpenTransactionWindow</code> nella sezione Impostazioni degli endpoint quando si utilizza Oracle come fonte per AWS DMS .
Amazon Timestream come obiettivo	Supporto per l'utilizzo di Amazon Timestream come endpoint di destinazione. Per ulteriori informazioni, consulta Utilizzo di Amazon Timestream come destinazione per AWS Database Migration Service .

AWS DMS la versione 3.5.1 include i seguenti problemi risolti:

Problema risolto	Descrizione
Oracle come fonte: aumento delle sessioni inattive	È stato risolto un problema relativo alla fonte Oracle a causa del quale le attività riservate ai soli CDC avevano sessioni inattive in continua crescita, con la seguente eccezione: <code>ORA-00020: maximum number of processes exceeded on the source database</code>
Replica delle modifiche UPDATE in DocumentDB	È stato risolto un problema per DocumentDB come destinazione in cui le istruzioni UPDATE non venivano replicate correttamente in alcuni scenari.
Attività di sola convalida	Migliore gestione degli errori per consentire alla funzionalità di convalida dei dati di fallire correttamente l'operazione quando la convalida dei dati è disabilitata per le attività di sola convalida.
Replica Redshift dopo la cessazione della connes sione	È stato risolto un problema per il target Redshift a causa del quale l'attività DMS non tentava di applicare nuovamente le modifiche sulla destinazione quando la destinazione era <code>ParallelApplyThreads</code> impostata su un valore maggiore di zero dopo l'interruzione della connessione, con conseguente perdita di dati.
Replica da testo a testo medio in MySQL	È stato risolto un problema relativo alla replica da MySQL a MySQL di tipi di dati <code>mediumtext</code> con modalità Full-LOB.
L'attività CDC non si replica con <code>rotated secret</code>	È stato risolto un problema per le attività DMS con <code>BatchApplyEnabled</code> impostazione <code>true</code> in cui DMS interrompeva la replica dei dati dopo che Secrets Manager aveva ruotato la password.
Problema di segmentaz ione di MongoDB/D ocumentDB	È stato risolto un problema relativo alla fonte MongoDB/DocDB in cui la segmentazione degli intervalli non funzionava correttamente quando la colonna della chiave primaria conteneva un valore elevato.
Convalida dei dati Oracle di valori numerici non associati	È stato risolto un problema per Oracle Target a causa del quale DMS riconosceva un valore di tipo NUMERIC di dati non associato durante la convalida dei dati. STRING

Problema risolto	Descrizione
Convalida dei dati di SQL Server	È stato risolto un problema relativo agli endpoint di SQL Server in cui la convalida dei dati DMS generava un'istruzione SQL non valida.
Segmentazione automatica MongoDB	È stata migliorata la funzionalità di partizionamento automatico dei dati durante la migrazione di documenti in parallelo da MongoDB come origine.
Formato Amazon S3 Apache Parquet	È stato risolto un problema a causa del quale i file Apache Parquet scritti su S3 come destinazione potevano essere visualizzati con Python con Apache Arrow C++.
PostgreSQL come gestione DDL di origine	È stato risolto un problema relativo all'origine PostgreSQL a causa del quale le operazioni DDL non supportate non venivano ignorate correttamente.
Errore dei dati timestamp tz PostgreSQL	È stato risolto un problema relativo alle migrazioni da PostgreSQL a PostgreSQL a causa del quale il timestamp con i dati del fuso orario non veniva migrato correttamente con la funzionalità di applicazione in batch abilitata durante la CDC.
Errore di convalida da Oracle a PostgreSQL	È stato risolto un problema relativo alle migrazioni da Oracle a PostgreSQL a causa del quale la convalida dei dati non riusciva per il tipo di dati NUMERIC (38,30).
Errore del tipo di dati esteso Oracle	È stato risolto un problema relativo all'origine Oracle a causa del quale il tipo di dati varchar esteso veniva troncato.
Combinazione degli operatori di filtro	È stato risolto un problema relativo alla funzionalità di filtro delle colonne a causa del quale l'operatore di colonna nullo non poteva essere combinato con altri tipi di operatori.
Latenza CDC derivante da una registrazione eccessiva	È stato risolto un problema relativo all'origine PostgreSQL a causa del quale l'eccessiva registrazione degli avvisi del plug-in pglogical causava la latenza del CDC di origine.

Problema risolto	Descrizione
Gestione della replica bidirezionale di Crea tabella con DDL	È stato risolto un problema relativo alla replica bidirezionale da PostgreSQL a PostgreSQL a causa del quale la modifica Crea tabella con DDL non veniva replicata correttamente.
Errore CDC durante l'utilizzo dei filtri	È stato risolto un problema relativo alla funzionalità di filtro a causa del quale la replica CDC non riusciva.
Convalida del nome host dell'autorità di certificazione per gli endpoint Kafka	È stata migliorata la funzionalità degli endpoint Kafka aggiungendo l'opzione per disabilitare la convalida del nome host dell'autorità di certificazione (<code>SslEndpointIdentificationAlgorithm</code>).
Convalida LUW IBM Db2	È stato risolto un problema a causa del quale i tipi di dati di origine, timestamp e ora di Db2 LUW non venivano gestiti correttamente durante la convalida dei dati.
Convalida S3	È stato risolto un problema relativo alle migrazioni da Db2 LUW a S3 in cui la funzionalità di convalida non gestiva correttamente il tipo di dati timestamp(0).
Errore di riavvio dell'attività DMS	È stato risolto un problema con il codice sorgente PostgreSQL a causa AWS DMS del quale l'attività non riusciva a riavviarsi e non poteva consumare eventi relazionali quando si utilizzava il plug-in pglogical.
Convalida di SQL Server del tipo di dati HIERARCHY	È stato risolto un problema relativo all'origine SQL Server a causa del quale la convalida del tipo di dati HIERARCHY non riusciva.
Stringhe SQL Server con caratteri di controllo	È stato risolto un problema relativo all'origine SQL Server a causa del quale le stringhe con caratteri di controllo non venivano replicate correttamente.
Redshift con Secrets Manager	È stato risolto un problema relativo alla destinazione Redshift a causa del quale il test dell'endpoint non riusciva quando si utilizzava Secrets Manager.

Problema risolto	Descrizione
Incoerenza delle impostazioni ParallelLoadThreads MySQL	È stato risolto un problema relativo alla destinazione MySQL a causa del quale l'impostazione ParallelLoadThreads non veniva mantenuta correttamente dopo le modifiche alle impostazioni delle attività.
Errore nella mappatura del tipo di dati da PostgreSQL a Oracle	È stato risolto un problema relativo alle migrazioni da PostgreSQL a Oracle a causa del quale l'attività non riusciva durante la replica dal tipo di dati TEXT al tipo di dati VARCHAR2(2000).
Convalida dei dati da Oracle a PostgreSQL	È stato risolto un problema relativo alle migrazioni da Oracle a PostgreSQL in cui la convalida dei dati restituiva falsi positivi quando i caratteri NULL venivano replicati come caratteri SPACE.
Origine SQL Server in configurazione AlwaysOn	È stato risolto un problema relativo all'origine di SQL Server nella AlwaysOn configurazione a causa del quale l'AWS DMS attività non riusciva se il nome della replica non corrispondeva esattamente al nome effettivo del server.
Errore nel test degli endpoint dell'origine Oracle	È stato risolto un problema con Oracle Source a causa del quale il test di connessione dell'AWS DMS endpoint non riusciva a causa di privilegi insufficienti durante il recupero dell'ID di sessione (SID) Oracle.
CDC non seleziona nuove tabelle	È stato risolto un problema relativo alle attività di sola CDC per cui in alcuni casi le tabelle create nell'origine dopo l'avvio dell'attività non venivano replicate.
Transazioni aperte in Oracle come origine	È stata migliorata la metodologia di gestione delle transazioni aperte quando si avvia un'attività di sola CDC dalla posizione iniziale di un'origine Oracle.

Problema risolto	Descrizione
Problema di dati mancanti	È stato risolto un problema relativo ai dati mancanti quando si riprendeva un'attività se questa veniva interrotta dopo l'applicazione delle modifiche memorizzate nella cache (opzione <code>StopTaskCACHEDCHANGESAPPLIED</code> impostata su <code>true</code>). Questo problema può verificarsi raramente se AWS DMS persistono le modifiche memorizzate nella cache al disco dell'istanza di AWS DMS replica a causa di un elevato volume di modifiche sull'origine.
Problema di convalida dei dati sul tipo di dati esteso	È stato risolto un problema relativo alla convalida dei dati da PostgreSQL a Oracle a causa del quale la convalida non riusciva per i tipi di dati estesi.
Problema di convalida dei dati per la codifica incoerente dei caratteri	È stato risolto un problema relativo alla convalida dei dati da SQL Server a PostgreSQL a causa del quale la convalida non riusciva quando la codifica dei caratteri non era coerente tra origine e destinazione.
Problema di convalida dei dati ORA-01455	È stato risolto un problema a causa del quale si verificava un errore ORA-01455 durante la convalida quando un <code>integer</code> PostgreSQL era mappato a un <code>number(10)</code> Oracle.
Supporto IDENTITY di SQL Server	È stato risolto un problema relativo alla replica dei dati da SQL Server a SQL Server a causa del quale la migrazione delle colonne di identità non riusciva quando la colonna di destinazione aveva la proprietà IDENTITY.
Problema del set di caratteri con le istruzioni ALTER	È stato risolto un problema relativo alla AWS DMS replica da MySQL a MySQL che modificava il set di caratteri in UTF16 durante la migrazione di un'istruzione durante il CDC. ALTER
Supporto dei tipi di dati spaziali da PostgreSQL a Redshift	È stato aggiunto il supporto per il tipo di dati <code>spatial</code> durante la migrazione da PostgreSQL ad Amazon Redshift.
Compressione GZIP di file .parquet	È stato risolto un problema che impediva la generazione di file.parquet con compressione GZIP con S3 come destinazione AWS DMS .

Problema risolto	Descrizione
Migrazione dell'origine MongoDB/DocDB	Risolto un problema AWS DMS che impediva la migrazione di alcune partizioni da una fonte MongoDB.
Problema relativo alle statistiche delle tabelle	È stato risolto un problema che impediva la visualizzazione delle statistiche delle tabelle quando almeno una delle attività sull'istanza di replica conteneva più di 1001 tabelle.
Tabella sospesa per IBM Db2 LUW 10.1.0 e versioni precedenti	È stato risolto un problema relativo a Db2 LUW come origine in cui la migrazione delle tabelle era sospesa con l'errore TYPESTRIN GUNITS is not valid quando la versione del database di origine era 10.1.0 o precedente.
Problema di partizionamento di MongoDB	È stato risolto un problema relativo a MongoDB/DocDB in cui mancavano uno o più segmenti della partizione di origine.
Problema di partizionamento di MongoDB	Risolve un problema per cui la segmentazione basata su una colonna con il tipo NumberLong () falliva a causa di un bug di conversione dei tipi.
Problema di partizionamento di MongoDB	Prestazioni di segmentazione automatica migliorate per set di dati di grandi dimensioni con MongoDB come origine.
Versione del driver MongoDB	È stato effettuato il downgrade del driver MongoDB alla versione 1.20.0 per continuare a supportare le versioni 3.6 e precedenti di MongoDB.
Tipo di dati timestamp Amazon S3 Apache Parquet	È stato risolto un problema per Amazon S3 Parquet Target. AWS DMS ora imposta il parametro di formato in isAdjustedToUTC modo true che corrisponda al comportamento delle versioni precedenti di AWS DMS.
Comando di copia di Amazon Redshift come destinazione	È stato risolto un problema relativo ad Amazon Redshift come destinazione a causa del quale il comando di copia non funzionava per le tabelle di grandi dimensioni durante la copia di dati da Amazon S3 ad Amazon Redshift.

Problema risolto	Descrizione
Tipi di dati geometrici PostgreSQL	È stato risolto un problema relativo alle migrazioni da PostgreSQL a PostgreSQL a causa del quale la migrazione non riusciva su tipi di dati geometrici di grandi dimensioni.
XML da Oracle a PostgreSQL	È stato risolto un problema a causa del quale la migrazione aggiungeva uno spazio in XML durante la replica da Oracle a PostgreSQL.
Aggiornamento del checkpoint di destinazione nei motori supportati	AWS DMS ora aggiorna il checkpoint di destinazione nella <code>awsdms_txn_state</code> tabella del database di destinazione.
Record MongoDB/DocDB inviati alla raccolta sbagliata	È stato risolto un problema relativo a MongoDB/DocDB a causa del quale i dati venivano inviati alla raccolta di destinazione sbagliata.
Oracle Source: nuova selezione di tabelle con impostazione dell'EscapeCharacter endpoint	AWS DMS È stato risolto un problema relativo a Oracle Source a causa del quale venivano recuperate nuove tabelle per la replica solo quando l'attività veniva interrotta e ripresa mentre era impostata l'EscapeCharacter endpoint.
Checkpoint di ripristino del CDC	È stata corretta un'incongruenza nel checkpoint di ripristino CDC osservata tra il datastore di destinazione e la console AWS DMS .
Attività di sola convalida CDC	È stato risolto un problema relativo alle attività di sola convalida CDC per le quali non veniva restituito l'esito negativo anche se tutte le tabelle dell'attività riscontravano errori.
Problemi di comportamento di convalida con connessione all'origine o alla destinazione	È stato risolto un problema relativo alla convalida dei dati che AWS DMS causava la sospensione delle tabelle sull'origine o sulla destinazione in caso di interruzione della connessione.

Problema risolto	Descrizione
Falsi positivi di convalida dei dati da Oracle a PostgreSQL	È stato risolto un problema con la convalida dei dati da Oracle a PostgreSQL a causa del quale venivano segnalati falsi positivi. AWS DMS perché le differenze nella rappresentazione dei caratteri NULL di origine sulla destinazione non venivano prese in considerazione con tipi di dati basati su testo diversi da VARCHAR.
Troncamento dei dati da Oracle a PostgreSQL	È stato risolto un problema relativo all'origine Oracle e alla destinazione PostgreSQL a causa del quale AWS DMS troncava i dati delle colonne NVARCHAR con l'impostazione Oracle <code>NLS_NCHAR_CHARACTERSET</code> configurata su <code>AL16UTF16</code> .
Errori di convalida dei dati	È stato risolto un problema relativo alla convalida dei dati a causa del quale <code>unable to create where filter clause</code> generava un errore quando venivano utilizzati il filtro di origine e una regola di trasformazione per l'aggiunta di colonne.
Gestione degli errori relativi a Redshift come destinazione	È stato risolto un problema relativo a Redshift come destinazione per cui la gestione degli errori non funzionava come configurato quando l'attività di CDC aveva l'impostazione dell'attività <code>ParallelApplyThreads</code> configurata su un valore maggiore di zero.
Errore di comunicazione relativo a Oracle come origine	È stato risolto un problema relativo a Oracle come origine per cui l'attività rimaneva nello stato <code>RUNNING</code> , ma non era in grado di migrare alcun dato dopo un errore di comunicazione.
Tabella CDC sospesa con i filtri di colonna	È stato risolto un problema relativo alle attività di pieno carico e CDC in cui una tabella veniva sospesa durante la fase CDC quando venivano applicati i filtri di colonna.
Errore di convalida dei dati di S3 come destinazione per i caratteri speciali	È stato risolto un problema relativo alla convalida dei dati di destinazione S3 a causa del quale l'attività avrebbe avuto esito negativo se il nome della tabella includeva un carattere speciale diverso dal carattere di sottolineatura.

Problema risolto	Descrizione
Errore di pieno carico e CDC di MongoDB come origine	È stato risolto un problema relativo a MongoDB come origine a causa del quale un'attività di pieno carico e CDC non funzionava durante la gestione degli eventi della cache con la migrazione di una raccolta di grandi dimensioni.
Problema di aggiornamento con <code>BatchApplyEnabled</code> impostato su <code>true</code>	È stato risolto un problema per cui, in alcuni casi, un' <code>BatchApplyEnabled</code> attività con l'impostazione dell'attività impostata su <code>true</code> non funzionava dopo la migrazione dalla AWS DMS versione 3.4.6 alla 3.5.1.
Origine SQL Server AlwaysOn con regole di confronto con distinzione tra maiuscole e minuscole	È stato risolto un problema con SQL Server AlwaysOn come origine a causa del quale un'attività avrebbe avuto esito negativo con regole di confronto con distinzione tra maiuscole e minuscole.
Sospensione dell'attività con MySQL come origine	È stato risolto un problema relativo a MySQL come origine in cui un'attività si bloccava invece di restituire esito negativo quando l'origine non era configurata correttamente.
Errore dell'attività di pieno carico di S3 come origine	È stato risolto un problema con S3 come origine a causa del quale un'attività non riusciva al ripristino dopo l'aggiornamento dalla AWS DMS versione 3.4.6 o 3.4.7 alla versione 3.5.1.
PostgreSQL come origine con <code>CapturedDDL</code> impostato su <code>false</code>	È stato risolto un problema relativo a PostgreSQL come origine a causa del quale le DDL non venivano gestite correttamente con l'impostazione dell'endpoint <code>CaptureDDLs</code> configurata su <code>false</code> .
Arresto anomalo dell'attività Oracle come origine durante la ripresa	È stato risolto un problema relativo a Oracle come origine a causa del quale si verificava l'arresto anomalo di un'attività al momento della ripresa a causa di dati errati nel nome della colonna.
Errore di ricerca LOB con MySQL come origine	È stato risolto un problema relativo a MySQL come origine a causa del quale una ricerca LOB non riusciva quando l'impostazione dell'attività <code>ParallelApplyThreads</code> era configurata su un valore maggiore di zero.

Problema risolto	Descrizione
Errore LSN illogico relativo a SQL Server come origine	È stato risolto un problema con SQL Server come origine a causa del quale un'attività non riusciva con un <code>illogical LSN sequencing state error</code> errore dopo l'aggiornamento dalla versione 3.4.7 alla versione 3.5.1. AWS DMS
PostgreSQL come origine con <code>pglogical</code>	È stato risolto un problema relativo a PostgreSQL come origine a causa del quale un'attività che utilizzava il plug-in <code>pglogical</code> restituiva a esito negativo quando l'attività veniva interrotta, una tabella veniva rimossa dalle regole di selezione, l'attività veniva ripresa e venivano apportate modifiche alla tabella rimossa.
Checkpoint di ripristino errato di Aurora MySQL	È stato risolto un problema relativo ad Aurora MySQL come origine a causa del quale veniva salvato un checkpoint di ripristino errato a seguito di un failover di Aurora o dell'arresto e dell'avvio dell'origine Aurora.
Arresto anomalo dell'attività di SQL Server come origine	È stato risolto un problema relativo a SQL Server come origine a causa del quale veniva eseguito l'arresto anomalo di un'attività quando <code>SafeguardPolicy</code> era impostato su <code>RELY_ON_SQL_SERVER_REPLICATION_AGENT</code> .
Casting errato del tipo di dati con MySQL come destinazione	È stato risolto un problema relativo a MySQL come destinazione a causa del quale la replica CDC non riusciva per l'errato casting del tipo di dati nella fase di applicazione in batch.
Errore dell'attività con <code>CaptureDDLs</code> impostato su <code>false</code> per PostgreSQL come origine	È stato risolto un problema relativo a PostgreSQL come origine a causa del quale un'attività non riusciva perché DDL veniva trattato come DML quando l'impostazione dell'endpoint <code>CaptureDDLs</code> era configurata su <code>false</code> .
Arresto anomalo della raccolta vuota di MongoDB	È stato risolto un problema relativo a MongoDB come origine a causa del quale si verificava l'arresto anomalo dell'attività per una raccolta vuota.

Problema risolto	Descrizione
Arresto anomalo dell'attività pieno carico per Redshift come destinazione	È stato risolto un problema relativo a Redshift a causa del quale si verificava l'arresto anomalo di un'attività durante la fase di pieno carico quando la tabella di controllo del checkpoint di ripristino era abilitata.
Nessun trasferimento di dati da S3 a S3	È stato risolto un problema relativo alla replica da S3 a S3 che impediva la replica dei dati AWS DMS se non fosse stato specificato <code>bucketFolder</code> .
Latenza CDC con GlueCatalogGeneration impostato su true	È stato risolto un problema relativo a S3 come destinazione a causa del quale si verificava una latenza eccessiva quando <code>GlueCatalogGeneration</code> era impostato su <code>true</code> .
Troncamento dei dati per Oracle come destinazione	È stato risolto un problema con Oracle come destinazione in cui i dati nelle colonne VARCHAR2 AWS DMS venivano troncati.
Comportamento dei caratteri jolly di sottolineatura per PostgreSQL	È stato risolto un problema relativo a PostgreSQL come origine a causa del quale il comportamento del carattere jolly "_" nelle regole di selezione non funzionava come documentato.
Problema di intestazione WAL vuota per PostgreSQL come origine	È stato risolto un problema relativo a PostgreSQL come origine a causa del quale l'attività non riusciva per un'intestazione WAL vuota ricevuta dallo slot di replica.
MySQL o MariaDB come origine con log binari compressi	Risolto un problema per MySQL e MariaDB come fonti in cui non veniva emesso un messaggio di errore corretto quando veniva rilevata la compressione BINLOG. AWS DMS
Caratteri speciali di convalida dei dati S3	È stata migliorata la convalida dei dati S3 per gestire i caratteri speciali nelle colonne di chiave primarie e non primarie.
Voci fuorvianti del log delle attività con Redshift come destinazione	È stato risolto un problema relativo a Redshift come destinazione a causa del quale nel log delle attività erano presenti voci fuorvianti che riportavano gli errori delle istruzioni di applicazione in batch su UPDATES e DELETES.

Problema risolto	Descrizione
Arresto anomalo dell'attività di migrazione da SQL Server a S3	È stato risolto un problema relativo alle migrazioni da SQL Server a S3 a causa del quale si verificava l'arresto anomalo dell'attività durante l'applicazione delle modifiche memorizzate nella cache.
Dati mancanti per gli errori di applicazione in batch	È stato risolto un problema relativo alla funzionalità di applicazione in batch a causa del quale un errore nell'applicazione di un batch causava la perdita di dati.

AWS Note sulla versione beta di Database Migration Service 3.5.0

Important

AWS DMS 3.5.0 è una versione beta del motore di istanze di replica. AWS DMS supporta questa versione come tutte le versioni precedenti. Tuttavia, consigliamo di testare la versione AWS DMS 3.5.0 Beta prima di utilizzarla per scopi di produzione.

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti nella versione 3.5.0 Beta di AWS Database Migration Service (AWS DMS).

Nuova caratteristica o miglioramento	Descrizione
Time Travel per Oracle e Microsoft SQL Server	Ora puoi utilizzare Time Travel in tutte le AWS regioni con endpoint di origine Oracle, Microsoft SQL Server e PostgreSQL supportati da DMS e endpoint di destinazione PostgreSQL e MySQL supportati da DMS.
Convalida S3	AWS DMS ora supporta la convalida dei dati replicati negli endpoint di destinazione Amazon S3. Per informazioni sulla convalida dei dati di destinazione di Amazon S3, consulta Convalida dei dati di destinazione Amazon S3 .
Integrazione del catalogo Glue	AWS Glue è un servizio che fornisce modi semplici per classificare i dati e consiste in un repository di metadati noto come. AWS

Nuova caratteristica o miglioramento	Descrizione
	<p>Glue Data Catalog Ora puoi integrare un endpoint AWS Glue Data Catalog di destinazione Amazon S3 e interrogare i dati Amazon S3 tramite altri servizi AWS come Amazon Athena. Per ulteriori informazioni, consulta Utilizzo di AWS Glue Data Catalog con una destinazione Amazon S3 per AWS DMS.</p>
<p>Applicazione in parallelo per DocumentDB come destinazione</p>	<p>Utilizzando DocumentDB come destinazione con nuove impostazioni delle ParallelApply* attività, AWS DMS ora supporta un massimo di 5000 record al secondo durante la replica CDC. Per ulteriori informazioni, consulta Utilizzo di Amazon DocumentDB come destinazione per AWS Database Migration Service.</p>
<p>Registrazione incentrata sul cliente</p>	<p>Ora è possibile esaminare e gestire i registri delle attività in modo più efficace con la versione 3.5.0. AWS DMS Per informazioni sulla visualizzazione e la gestione dei registri delle attività AWS DMS, vedere. Visualizzazione e gestione dei log delle attività AWS DMS</p>
<p>Meccanismo SASL_PLAIN per endpoint di destinazione Kafka</p>	<p>È ora possibile utilizzare l'autenticazione SASL_PLAIN per supportare gli endpoint di destinazione Kafka MSK.</p>
<p>Replica delle transazioni XA in MySQL</p>	<p>Ora puoi utilizzare le transazioni XA nell'origine MySQL DMS. Prima di DMS 3.5.0, le modifiche DML applicate come parte delle transazioni XA non venivano replicate correttamente.</p>
<p>Tipi di dati estesi Oracle</p>	<p>AWS DMS ora supporta la replica di tipi di dati estesi nella versione Oracle 12.2 e successive.</p>
<p>Ambiente Db2 LUW PureScale</p>	<p>AWS DMS ora supporta la replica da un ambiente Db2 LUW. PureScale Questa funzionalità è supportata solo utilizzando l'opzione Inizia a elaborare le modifiche dalla posizione della modifica di origine.</p>

Nuova caratteristica o miglioramento	Descrizione
Origine SQL Server con opzione READ_COMMITTED_SNAPSHOT	Quando si utilizza un database di origine di Microsoft SQL Server con l'opzione READ_COMMITTED_SNAPSHOT impostata su TRUE, è possibile replicare correttamente le modifiche DML impostando l'attributo force DataRow Lookup connection.

AWS DMS 3.5.0 include i seguenti problemi risolti:

Problemi risolti nella AWS DMS versione 3.5.0 lanciata il 17 marzo 2023

Argomento	Risoluzione	
Oracle: confronto di caso speciale per una stringa convertita da valore numerico	È stato risolto un problema relativo all'origine Oracle a causa del quale le regole di filtro non funzionavano come previsto per una colonna numerica quando per la stessa colonna era prevista la trasformazione del tipo di dati in stringa.	
Miglioramenti di SQL Server AG on-premise	Migliore efficienza della gestione delle connessioni con SQL Server Source nella AlwaysOn configurazione eliminando le connessioni non necessarie alle repliche non utilizzate dal DMS.	
Conversione interna di HIERARCHYID per SQL Server	È stato risolto un problema relativo all'origine SQL Server in cui il tipo di dati HIERARCHYID veniva replicato come VARCHAR(250) anziché HIERARCHYID nella destinazione SQL Server.	
Correzione dell'attività di spostamento per la destinazione S3	Risolto il problema per cui lo spostamento di un'attività con una destinazione S3 richiedeva molto tempo, risultava bloccato o mai completato.	
Meccanismo SASL Plain di Kafka	È stato introdotto il supporto per il metodo di autenticazione SASL Plain per l'endpoint di destinazione Kafka MSK.	

Argomento	Risoluzione
Caricamento/Applicazione in parallelo non riesce a causa del parametro <code>_type</code> con Opensearch 2.x	È stato risolto un problema per la destinazione Opensearch 2.x in cui il caricamento o l'applicazione in parallelo non funzionava a causa della mancanza del supporto per il parametro <code>_type</code> .
Supporto per il filtro di mappatura delle tabelle con operatori misti	È stata rimossa una limitazione in base alla quale era possibile applicare un solo filtro su una colonna.
Endpoint S3, Kinesis, Kafka: migrazione delle colonne LOB basata su modifica nella fase CDC	È stato risolto il problema relativo alle destinazioni Kinesis, Kafka e S3 a causa del quale i dati delle colonne LOB aggiunte durante la CDC non venivano replicati.
Aggiornamento del driver MongoDB	È stato aggiornato il driver MongoDB alla v1.23.2.
Aggiornamento del driver Kafka	È stato aggiornato il driver Kafka da 1.5.3 a 1.9.2.
L'impostazione dell'endpoint S3 non funzionava correttamente	È stato risolto un problema relativo alla destinazione S3 per cui l'impostazione dell'endpoint <code>AddTrailingPaddingCharacter</code> non funzionava quando i dati contenevano il carattere specificato come delimitatore per la destinazione S3.
Arresto anomalo dell'attività di destinazione Kinesis	È stato risolto un problema relativo alla destinazione Kinesis a causa del quale si verificava l'arresto anomalo di un'attività quando il valore PK era vuoto e il debug dettagliato era abilitato.

Argomento	Risoluzione	
I nomi delle colonne delle destinazioni S3 spostati di una posizione	È stato risolto il problema relativo alla destinazione S3 in cui i nomi delle colonne venivano spostati di una posizione quando <code>AddColumnName</code> era impostato su <code>true</code> e <code>TimestampColumnName</code> era impostato su <code>""</code> .	
Registrazione migliorata per gli avvisi di troncamento LOB	Registrazione degli avvisi migliorata per il troncamento LOB dell'origine SQL Server in modo da includere l'istruzione <code>select</code> utilizzata per recuperare il LOB.	
Aggiunto un errore irreversibile per evitare arresti anomali dell'attività DMS se la password TDE è sbagliata.	È stato introdotto un messaggio di errore significativo ed è stato eliminato il problema di arresto anomalo dell'attività in situazioni in cui l'attività DMS non riusciva senza alcun messaggio di errore a causa di una password TDE errata per Oracle come origine.	
Migrazione di DDL CTAS (Create Table As Selected) PostgreSQL consentita durante la CDC.	Sono state rimosse le limitazioni per cui DMS non era in grado di replicare le DDL CTAS (Create Table As Selected) PostgreSQL durante la CDC.	
Risolto l'arresto anomalo dell'attività <code>pg_logical</code> quando le colonne della tabella venivano eliminate nel CDC.	È stato risolto il problema relativo all'origine PostgreSQL con destinazione S3 a causa del quale le colonne erano disallineate nella destinazione quando il supporto per i LOB era disabilitato e i LOB erano presenti.	
Risolta la perdita di memoria nella gestione delle connessioni MySQL	È stato risolto il problema relativo all'origine MySQL a causa del quale il consumo di memoria delle attività aumentava continuamente.	


Argomento	Risoluzione
Impostazione dell'endpoint di origine Oracle: <code>ConvertTimestampWithZoneToUTC</code>	Imposta questo attributo su <code>true</code> per convertire in UTC il valore del timestamp delle colonne "TIMESTAMP WITH TIME ZONE" e "TIMESTAMP WITH LOCAL TIME ZONE". Per impostazione predefinita, il valore di questo attributo è "false" e i dati vengono replicati utilizzando il fuso orario del database di origine.
Origine Oracle: <code>DataTruncationErrorPolicy</code> per <code>SUSPEND_TABLE</code> non funziona	È stato risolto il problema relativo all'origine Oracle con destinazione S3 a causa del quale le tabelle non venivano sospese mentre l'impostazione dell'attività <code>DataTruncationErrorPolicy</code> era impostata su <code>SUSPEND_TABLE</code> .
SQL Server non riesce su schemi/tabelle lunghi durante la creazione di una clausola di query	È stato risolto il problema relativo all'origine SQL Server a causa del quale l'attività non riusciva o non rispondeva quando la regola di selezione conteneva un elenco di tabelle separate da virgole.
Autenticazione di Secrets Manager con endpoint MongoDB	È stato risolto il problema relativo agli endpoint MongoDB e DocumentDB a causa del quale l'autenticazione basata su Secrets Manager non funzionava.
DMS tronca i dati durante la CDC per una colonna <code>varchar multibyte</code> quando <code>NLS_NCHAR_CHARACTERSET</code> è impostato su UTF8	È stato risolto il problema relativo all'origine Oracle con destinazione Oracle a causa del quale i dati venivano troncati per le colonne <code>VARCHAR multibyte</code> con <code>NLS_NCHAR_CHARACTERSET</code> impostato su UTF8.
<code>filterTransactionsOfUser</code> ECA per Oracle LogMiner	È stato aggiunto un attributo di connessione aggiuntivo (ECA) <code>filterTransactionsOfUser</code> per consentire a DMS di ignorare le transazioni di un utente specifico durante la replica da Oracle utilizzando LogMiner.

Argomento	Risoluzione
Errore ripristinabile dell'impostazione SQL Server quando Isn non è presente nel backup	Risolto il problema relativo a SQL Server a causa del quale un'attività non restituiva esito negativo se mancava un LSN.

AWS Note di rilascio di Database Migration Service 3.4.7

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti nella versione 3.4.7 di AWS Database Migration Service (AWS DMS).

Nuova caratteristica o miglioramento	Descrizione
Supporto per Babelfish come destinazione	<p>AWS DMS ora supporta Babelfish come bersaglio. Utilizzando AWS DMS, ora puoi migrare i dati in tempo reale da qualsiasi fonte AWS DMS supportata a Babelfish, con tempi di inattività minimi.</p> <p>Per ulteriori informazioni, consulta Uso di Babelfish come destinazioni per AWS Database Migration Service.</p>
Supporto per i database IBM Db2 z/OS come origine per solo pieno carico	<p>AWS DMS ora supporta i database IBM Db2 z/OS come fonte. Utilizzando AWS DMS, ora è possibile eseguire migrazioni in tempo reale dai mainframe Db2 verso qualsiasi destinazione supportata. AWS DMS</p> <p>Per ulteriori informazioni, consulta Utilizzo dei database IBM Db2 for z/OS come origine per AWS DMS.</p>
Supporto per la replica di lettura SQL Server come origine	<p>AWS DMS ora supporta la replica di lettura di SQL Server come origine. Utilizzando AWS DMS, ora è possibile eseguire migrazioni in tempo reale dalla replica di lettura di SQL Server verso qualsiasi AWS DMS destinazione supportata.</p>

Nuova caratteristica o miglioramento	Descrizione
	<p>Per ulteriori informazioni, consulta Utilizzo di un database Microsoft SQL Server come origine per AWS DMS.</p>
Supporta EventBridge eventi DMS	<p>AWS DMS supporta la gestione delle sottoscrizioni agli eventi utilizzando EventBridge per gli eventi DMS.</p> <p>Per ulteriori informazioni, consulta Utilizzo degli eventi e delle notifiche Amazon EventBridge in AWS Database Migration Service.</p>
Supporto per gli endpoint VPC di origine e di destinazione	<p>AWS DMS ora supporta gli endpoint Amazon Virtual Private Cloud (VPC) come sorgenti e destinazioni. AWS DMS ora possono connettersi a qualsiasi AWS servizio con endpoint VPC quando nel VPC sono definiti percorsi esplicitamente definiti verso i servizi. AWS DMS</p> <div data-bbox="544 909 1507 1367" style="border: 1px solid #0070C0; border-radius: 10px; padding: 10px;"><p> Note</p><p>Gli aggiornamenti alle AWS DMS versioni 3.4.7 e successivi e richiedono prima la configurazione per l'utilizzo degli endpoint VPC o per AWS DMS l'utilizzo di route pubbliche . Questo requisito si applica agli endpoint di origine e destinazione per Amazon S3, Amazon Kinesis AWS Secrets Manager Data Streams, Amazon DynamoDB, Amazon Redshift e Amazon Service. OpenSearch</p></div> <p>Per ulteriori informazioni, consulta Configurazione degli endpoint VPC come endpoint di origine e di destinazione AWS DMS.</p>
La nuova versione di PostgreSQL	<p>PostgreSQL versione 14.x è ora supportato come origine e destinazione.</p>

Nuova caratteristica o miglioramento	Descrizione
Supporto per Aurora serverless v2 come destinazione	<p>AWS DMS ora supporta Aurora Serverless v2 come destinazione. Utilizzando AWS DMS, ora puoi eseguire migrazioni in tempo reale verso Aurora Serverless v2.</p> <p>Per informazioni sulle destinazioni supportate AWS DMS , consulta. Destinazioni per la migrazione dei dati</p>
Nuove versioni di IBM Db2 per LUW	<p>AWS DMS ora supporta IBM Db2 for LUW versioni 11.5.6 e 11.5.7 come sorgente. Utilizzando AWS DMS, ora puoi eseguire migrazioni in tempo reale dalle versioni più recenti di IBM DB2 for LUW.</p> <p>Per informazioni sulle AWS DMS fonti, vedere. Origini per la migrazione dei dati</p> <p>Per informazioni sugli AWS DMS obiettivi supportati, vedere Destinazioni per la migrazione dei dati.</p>

AWS DMS 3.4.7 include il seguente comportamento nuovo o modificato e i problemi risolti:

- Ora puoi utilizzare un formato di data dalla definizione della tabella per analizzare una stringa di dati in un oggetto data quando usi Amazon S3 come origine.
- Sono disponibili nuovi contatori delle statistiche delle tabelle: `AppliedInserts`, `AppliedDdls`, `AppliedDeletes` e `AppliedUpdates`.
- È ora possibile scegliere il tipo di mappatura predefinito da utilizzare OpenSearch come destinazione.
- La nuova impostazione degli endpoint `TrimSpaceInChar` per le origini Oracle, PostgreSQL e SQLServer consente di specificare se tagliare i dati nei tipi di dati CHAR e NCHAR.
- La nuova impostazione degli endpoint `ExpectedBucketOwner` per Amazon S3 impedisce lo sniping quando si utilizza S3 come origine o destinazione.
- Per RDS SQL Server, Azure SQL Server e SQL Server autogestito, DMS ora offre la configurazione automatica dell'acquisizione MS-CDC su tutte le tabelle selezionate per un'attività di migrazione con o senza una CHIAVE PRIMARIA o con un indice univoco, considerando la priorità

di abilitazione per la replica MS-REPLICATION sulle tabelle SQL Server autogestite con CHIAVE PRIMARIA.

- È stato aggiunto il supporto per la replica delle operazioni DDL di partizioni e sottopartizioni Oracle durante le migrazioni omogenee di Oracle.
- È stato risolto un problema a causa del quale si verificava l'arresto anomalo di un'attività di convalida dei dati con una chiave primaria composta con Oracle come origine e destinazione.
- È stato risolto un problema relativo al casting corretto di un tipo di carattere variabile su un booleano mentre la colonna di destinazione era già creata come booleana con Redshift come destinazione.
- È stato risolto un problema che causava il troncamento dei dati per i tipi di dati `varchar` migrati come `varchar(255)` a causa di un problema ODBC noto con PostgreSQL come destinazione.
- È stato risolto un problema per cui Parallel Hint per l'operazione DELETE non veniva rispettato con `BatchApplyEnabled` impostato su `true` e `BatchApplyPreserveTransaction` impostato su `false` con Oracle come destinazione.
- La nuova impostazione degli endpoint `AddTrailingPaddingCharacter` per Amazon S3 aggiunge il padding ai dati di stringa quando si utilizza S3 come destinazione.
- La nuova impostazione delle attività `max_statement_timeout_seconds` estende il timeout predefinito delle query sugli endpoint. Questa impostazione è attualmente usata dalle query sui metadati degli endpoint MySQL.
- Con PostgreSQL come destinazione, è stato risolto un problema a causa del quale un'attività di CDC non utilizzava correttamente le impostazioni dell'attività di gestione degli errori.
- È stato risolto un problema a causa del quale DMS non era in grado di identificare correttamente la modalità Redis per un'istanza Redis Enterprise.
- È stato esteso il supporto dell'attributo aggiuntivo di connessione `includeOpForFullLoad` per il formato parquet di destinazione S3.
- È stata introdotta la nuova impostazione degli endpoint PostgreSQL `migrateBooleanAsBoolean`. Quando questa impostazione è configurata su `true` per una migrazione da PostgreSQL a Redshift, un booleano verrà migrato come `varchar(1)`. Quando è impostata su `false`, un booleano viene migrato come `varchar(15)`, che è il comportamento predefinito.
- È stato risolto un problema relativo alla migrazione con datatype `date time` con l'origine SQL Server. Questa correzione risolve il problema dell'inserimento di `Null` quando la precisione è espressa in millisecondi.

- Per l'origine PostgreSQL con PGLOGICAL, è stato risolto un problema relativo alla migrazione durante l'utilizzo di pglogical e alla rimozione di un campo dalla tabella di origine durante la fase CDC, in cui il valore dopo la rimozione del campo non veniva migrato nella tabella di destinazione.
- È stato risolto un problema relativo alla migrazione di SQL Server Loopback con la replica bidirezionale che generava record ripetuti.
- È stato aggiunto il nuovo attributo aggiuntivo di connessione `mapBooleanAsBoolean` per PostgreSQL come origine. Utilizzando questo attributo di connessione aggiuntivo, puoi sovrascrivere la mappatura del tipo di dati predefinito di un booleano PostgreSQL con un tipo di dati booleano. RedShift
- È stato risolto un problema relativo alla migrazione a causa del quale quando si utilizzava SQL Server come origine `ALTER DECIMAL/NUMERIC SCALE` non si replicava sulle destinazioni.
- È stato risolto un problema di relativo a SQL Server 2005.
- A partire dal 17 ottobre 2022, DMS 3.4.7 ora supporta le classi di istanze Amazon EC2 di sesta generazione per le istanze di replica.
- A partire dal 25 novembre 2022, con DMS 3.4.7 puoi convertire schemi di database e oggetti di codice utilizzando la conversione dello schema DMS e individuare nel tuo ambiente di rete i database che sono buoni candidati per la migrazione utilizzando DMS Fleet Advisor.
- A partire dal 25 novembre 2022, DMS Studio è stato ritirato.
- A partire dal 31 gennaio 2023, la conversione dello schema DMS supporta Aurora MySQL e Aurora PostgreSQL come fornitore di dati di destinazione.
- A partire dal 6 marzo 2023, con DMS Fleet Advisor puoi generare raccomandazioni sulle destinazioni con la giusta dimensione per i tuoi database di origine.
- A partire dal 6 marzo 2023, AWS DMS supporta la policy AWS gestita che consente la pubblicazione di punti dati metrici su Amazon CloudWatch.

Sono stati risolti i problemi della versione di manutenzione di DMS 3.4.7 del 5 maggio 2023

Argomento	Risoluzione
Errore relativo all'attività di origine PostgreSQL	È stato risolto un problema relativo all'origine PostgreSQL a causa del quale le attività non andavano a buon fine quando si superava il numero massimo consentito di operazioni DDL in un singolo evento.

Argomento	Risoluzione	
Falsi positivi per la convalida dei dati di origine PostgreSQL	È stato risolto un problema relativo all'origine PostgreSQL con destinazione Oracle a causa del quale il casting errato del campo timestamp provocava errori di convalida dei dati falsi positivi.	
Gestione degli errori relativi all'origine MySQL	È stato risolto un problema relativo a un'origine MySQL a causa del quale l'attività DMS non restituiva esito negativo quando il log BIN successivo non era disponibile.	
Registrazione di ROTATE_EVENT dell'origine MySQL	Registrazione migliorata per ROTATE_EVENT dell'origine MySQL, incluso il nome del log BIN letto.	
Problema di timeout della convalida dei dati	È stato risolto un problema relativo alla funzionalità di convalida dei dati a causa del quale l'impostazione degli endpoint <code>executeTimeout</code> non veniva rispettata per le query relative alla convalida dei dati.	
Problema di pieno carico parallelo per la destinazione PostgreSQL	È stato risolto un problema per la destinazione PostgreSQL a causa del quale il pieno carico segmentato (parallelo) non funzionava a causa di un errore di "connessione interrotta".	
Problema di spostamento dell'attività DMS	È stato risolto un problema relativo alla destinazione S3 a causa del quale un'operazione di spostamento di un'attività DMS richiedeva molto tempo o non veniva mai completata.	
Problema relativo ai record duplicati dell'origine PostgreSQL	È stato risolto un problema relativo all'origine PostgreSQL a causa del quale un'attività DMS generava errori relativi ai duplicati sulla destinazione dopo l'interruzione e la ripresa di un'attività.	

Argomento	Risoluzione
Falsi positivi per la convalida dei dati della destinazione Oracle	È stato risolto un problema relativo alla destinazione Oracle a causa del quale la convalida dei dati restituiva errori falsi positivi dovuti alla replica errata del fuso orario per i campi del timestamp.

Sono stati risolti i problemi della versione di manutenzione di DMS 3.4.7 del 22 febbraio 2023

Argomento	Risoluzione
Repliche di SQL Server AG come origine	È stato aggiunto il supporto per il codice sorgente di SQL Server nella AlwaysOn configurazione in cui la porta TCP del listener differiva dalla porta TCP di replica.
Perdita di dati con Amazon Redshift come destinazione	È stato risolto un problema relativo alla destinazione Redshift a causa del quale, in alcuni rari casi, un riavvio imprevisto di Redshift poteva causare la perdita di dati sulla destinazione.
Supporto per la protezione dell'origine SQL Server	È stato risolto un problema relativo all'origine SQL Server a causa del quale l'attività DMS poteva non riuscire con un errore che indicava l'impossibilità di leggere i backup del log delle transazioni quando veniva specificata l'impostazione degli endpoint "SafeguardPolicy": "EXCLUSIVE_AUTOMATIC_TRUNCATION" .
Errore dell'attività di convalida dei dati per Oracle come origine	È stato risolto un problema relativo all'origine Oracle a causa del quale l'attività DMS poteva non riuscire durante la convalida dei dati perché i valori della chiave primaria venivano identificati in modo errato.
Problema dei dati dell'immagine precedente Kinesis	È stato risolto un problema per le destinazioni di streaming (Kinesis, Kafka) a causa del quale l'imposta

Argomento	Risoluzione
	zione delle attività "EnableBeforeImage" funzionava solo per i tipi di dati carattere.
File di log Time Travel	È stato risolto un problema relativo alla funzionalità Time Travel a causa del quale DMS creava file di log Time Travel a zero byte quando l'origine era inattiva.

Sono stati risolti i problemi della versione di manutenzione di DMS 3.4.7 del 16 dicembre 2022

Argomento	Risoluzione
BatchApplyAbilitato	È stato risolto un problema di registrazione eccessiva quando BatchApplyEnabled è impostato su True.
Nuova impostazione dell'endpoint MongoDB: Timeout FullLoad NoCursor	L' FullLoadNoCursorTimeout impostazione dell'endpoint MongoDB NoCursorTimeout specifica il cursore a pieno caricamento. NoCursorTimeout è un'impostazione di connessione MongoDB che impedisce al server di chiudere il cursore se inattivo.
MongoDB: funzione di filtro per la segmentazione con colonna singola	La nuova funzione di filtro migliora le prestazioni per la migrazione dei database MongoDB utilizzando una singola colonna per la segmentazione.
Da MongoDB a Redshift	Durante la migrazione da MongoDB a Redshift, se la raccolta MongoDB include un tipo di dati binario, è stato risolto un problema a causa del quale DMS non creava la tabella di destinazione su Redshift.
Nuovo attributo di connessione SocketTimeout MongoDB MS	Il nuovo attributo di connessione extra SocketTimeout MongoDB MS configura il timeout di connessione per i client MongoDB in unità di millisecondi. Se il valore è minore o uguale a zero, viene utilizzato il client MongoDB predefinito.

Argomento	Risoluzione
Risolto il problema che causava l'arresto anomalo di un'attività Amazon Kinesis	Durante la migrazione al flusso di dati Amazon Kinesis come destinazione, è stato risolto un problema di gestione dei valori null quando nella tabella non è presente una chiave primaria.
Convalida dei dati Oracle NULL PK/UK supportata	È stata rimossa la limitazione secondo cui la convalida dei dati dei valori NULL PK/UK non era supportata.
Da Oracle ad Amazon S3	Durante la migrazione da Oracle ad Amazon S3, è stato risolto un problema a causa del quale alcuni record venivano migrati erroneamente come NULL.
Oracle Standby	Quando si utilizza Oracle Standby come origine, è stata aggiunta la possibilità per DMS di gestire le transazioni aperte.
Migrazione da Oracle a Oracle con il tipo di dati spaziali SDO_GEOMETRY	Durante la migrazione da Oracle a Oracle, è stato risolto un problema a causa del quale l'attività non riusciva se nella tabella era presente una colonna SDO_GEOMETRY nella DDL.
Oracle come origine	È stato risolto un problema a causa del quale quando si utilizzava Oracle come origine DMS saltava occasionalmente un numero di sequenza di log redo di Oracle.
Oracle come origine: log redo online e di archiviazione mancanti	È stato risolto un problema a causa del quale quando si utilizzava Oracle come origine l'operazione DMS non riusciva se mancavano i log di archiviazione.
DMS occasionalmente ignora il log redo Oracle Standby	È stato risolto un problema a causa del quale quando si utilizzava Oracle come origine DMS saltava occasionalmente un numero di sequenza di log redo di Oracle.

Argomento	Risoluzione
I tipi di dati spaziali da Oracle a Oracle non vengono replicati durante la CDC	È stato risolto un problema a causa del quale con la replica da Oracle a Oracle, i tipi di dati spaziali non venivano replicati durante la CDC.
Oracle come destinazione	È stato risolto un problema a causa del quale quando si utilizzava Oracle come destinazione, l'applicazione di destinazione non riusciva con l'errore ORA-01747.
Amazon S3: corretta la perdita di dati nelle tabelle di ricaricamento	È stato risolto un problema a causa del quale quando si utilizzava Amazon S3 come destinazione, un'operazione di ricaricamento delle tabelle non generava file CDC.
Inizializzazione del contesto SQL Server Always On nel caso in cui il server principale è utilizzato come origine	Quando si utilizzava SQL Server Always On come origine, è stato risolto un problema che impediva l'inizializzazione dei gruppi di disponibilità (AG) se l'origine è primaria ed è impostata su true. AlwaysOnSharedSync edBackupsEnabled
Impostazione degli endpoint di SQL Server aggiornata	Quando un endpoint di origine è SQL Server Always On Availability Group ed è una replica secondaria, è stato risolto un problema per cui l'attività di replica non riusciva se AlwaysOnSharedSynchedBackupsIsEnabled impostata su True.
PostgreSQL come origine	È stato risolto un problema a causa del quale CDC non riusciva a migrare le operazioni di eliminazione/aggiornamento sul sorgente PostgreSQL, introdotto nella versione 3.4.7 nel supporto di Boolean. mapBooleanAs

AWS Note di rilascio di Database Migration Service 3.4.6

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti nella versione 3.4.6 di AWS Database Migration Service (AWS DMS).

Nuova caratteristica o miglioramento	Descrizione
AWS DMS Viaggio nel tempo	<p>AWS DMS introduce Time Travel, una funzionalità che garantisce ai clienti flessibilità nelle funzionalità di registrazione e migliora l'esperienza di risoluzione dei problemi. Con Time Travel, puoi archiviare e crittografare AWS DMS i log utilizzando Amazon S3 e visualizzare, scaricare e offuscare i log entro un determinato periodo di tempo.</p>
Supporto per l'istanza gestita SQL di Microsoft Azure come origine	<p>AWS DMS ora supporta Microsoft Azure SQL Managed Instance come origine. Utilizzando AWS DMS, ora puoi eseguire migrazioni in tempo reale da Microsoft Azure SQL Managed Instance verso qualsiasi destinazione AWS DMS supportata.</p> <p>Per informazioni sulle AWS DMS fonti, vedere. Origini per la migrazione dei dati</p> <p>Per informazioni sugli AWS DMS obiettivi supportati, vedere Destinazioni per la migrazione dei dati.</p>
Supporto di Google Cloud SQL per MySQL come origine	<p>AWS DMS ora supporta Google Cloud SQL for MySQL come sorgente. Utilizzando AWS DMS, ora puoi eseguire migrazioni live da Google Cloud SQL for MySQL verso qualsiasi destinazione supportata. AWS DMS</p> <p>Per informazioni sulle AWS DMS fonti, consulta. Origini per la migrazione dei dati</p> <p>Per informazioni sugli AWS DMS obiettivi supportati, vedere Destinazioni per la migrazione dei dati.</p>

Nuova caratteristica o miglioramento	Descrizione
Supporto del caricamento parallelo per dati partizionati su S3	AWS DMS ora supporta il caricamento parallelo per i dati partizionati su Amazon S3, migliorando i tempi di caricamento per la migrazione dei dati partizionati dai dati di origine del motore di database supportato ad Amazon S3. Questa funzionalità crea sottocartelle Amazon S3 per ogni partizione della tabella nell'origine del database, permettendo ad AWS DMS di eseguire processi paralleli per popolare ogni sottocartella.
Supporto di più argomenti di destinazione di Apache Kafka in un'unica attività	AWS DMS ora supporta i target multiargomento di Apache Kafka con un'unica attività. Utilizzando AWS DMS, ora è possibile replicare più schemi da un singolo database su diversi argomenti di destinazione di Apache Kafka utilizzando la stessa attività. Ciò elimina la necessità di creare più attività separate in situazioni in cui è necessario migrare molte tabelle dello stesso database di origine su argomenti di destinazione Kafka diversi.

I problemi risolti nella versione AWS DMS 3.4.6 includono quanto segue:

- È stato risolto un problema a causa del quale le colonne delle istruzioni UPDATE venivano popolate in colonne errate se la colonna della chiave primaria non era la prima colonna con Amazon S3 come destinazione con formato CSV.
- È stato risolto un problema per cui AWS DMS le attività potevano bloccarsi quando si utilizzava il plug-in pglogical con NULL valori in BYTEA colonne in modalità LOB limitata quando si utilizzava PostgreSQL come sorgente.
- È stato risolto un problema per cui AWS DMS le attività potevano bloccarsi quando veniva eliminato un gran numero di tabelle di origine quando si utilizzava PostgreSQL come sorgente.
- È stato migliorato il partizionamento delle cartelle basato sulla data di Amazon S3 introducendo la nuova impostazione Amazon S3 DatePartitionTimezone per consentire il partizionamento in date non UTC.
- È supportata la mappatura tra i tipi di dati `TIMESTAMP WITH TIME ZONE` dalle origini a `TIMESTAMPTZ` con Redshift come destinazione.

- Sono state migliorate le prestazioni del CDC per le attività senza regole di selezione dei caratteri jolly con MongoDB o Amazon DocumentDB come origine.
- È stato risolto un problema a causa del quale i nomi degli schemi con caratteri jolly e caratteri di sottolineatura e lunghezza inferiore a 8 non venivano acquisiti dalle attività AWS DMS con Db2 LUW come origine.
- È stato risolto un problema a causa del quale AWS DMS le istanze esaurivano la memoria con grandi volumi di dati quando si utilizzava OpenSearch Service come destinazione.
- Sono state migliorate le prestazioni di convalida dei dati supportando le attività di sola convalida pieno carico.
- È stato risolto un problema che impediva la ripresa AWS DMS delle attività dopo il failover forzato quando si utilizzava Sybase come fonte.
- È stato risolto un problema a causa del quale l'avviso veniva AWS DMS inviato in modo errato. `Invalid BC timestamp was encountered in column`

I problemi risolti nella versione di manutenzione di DMS 3.4.6 includono i seguenti:

- È stato risolto un problema di arresto anomalo di un'attività quando la modalità di applicazione in blocco è abilitata con Oracle come origine e destinazione.
- È stato risolto un problema che impediva a un'attività di pieno carico di utilizzare correttamente l'impostazione degli endpoint `ExecuteTimeout` con PostgreSQL come origine.
- È stato risolto un problema relativo alla migrazione delle colonne del tipo di dati array quando l'attività è impostata sulla modalità LOB limitata con PostgreSQL come origine.
- È stato risolto un problema relativo alla migrazione dei timestamp con fuso orario precedente al 1970-01-01 con PostgreSQL come origine.
- È stato risolto un problema a causa del quale DMS trattava una stringa vuota come nulla durante la replica con SQL Server come origine e destinazione.
- È stato risolto un problema in modo da rispettare le impostazioni degli endpoint di timeout di lettura e scrittura della sessione con MySQL come origine e destinazione.
- È stato risolto un problema a causa del quale un'attività di CDC DMS scaricava i file relativi al pieno carico con Amazon S3 come origine.
- È stato risolto un problema di arresto anomalo del log quando `CdcInsertsAndUpdates` e `PreserveTransactions` erano entrambi impostati su `true` con Amazon S3 come destinazione.

- È stato risolto un problema a causa del quale un'attività si bloccava quando la ParallelApply funzione* è abilitata, ma alcune tabelle non hanno una chiave primaria predefinita quando si utilizza Amazon Kinesis Data Streams come origine.
- È stato risolto un problema per cui non veniva fornito un errore per errore StreamArn quando si utilizzava Amazon Kinesis Data Streams come fonte.
- È stato risolto un problema per cui un valore di chiave primaria come stringa vuota causava l'arresto anomalo di un'attività quando veniva utilizzata OpenSearch come destinazione.
- È stato risolto un problema a causa del quale veniva utilizzato troppo spazio su disco per la convalida dei dati.

Sono stati risolti i problemi della versione di manutenzione di DMS 3.4.6 del 13 dicembre 2022

Argomento	Risoluzione
Driver ODBC SAP ASE	È stato risolto un problema relativo a SAP ASE come origine in modo che il driver ODBC potesse supportare i set di caratteri.
Bug della chiave primaria datetime di SQL Server per la ricerca lob	È stato risolto un problema relativo a SQL Server come origine a causa del quale la ricerca LOB non funzionava correttamente, quando la chiave primaria aveva un tipo di dati datetime, con precisione in millisecondi.
Da SQL Server a Redshift: "datetime Offset" mappato a "timestampz"	Per le migrazioni da SQL Server a Redshift, è stata migliorata la mappatura in modo che il formato "datetimeoffset" di SQL Server sia mappato al formato "timestampz" di Redshift.
Convalida dei dati: SkipLobColumns è vera	È stato risolto un problema per cui l'attività DMS si bloccava quando SkipLobColumns era True, c'è un LOB nell'origine, la chiave primaria si trova nell'ultima colonna e una differenza di dati veniva rilevata dalla convalida.
Convalida dei dati con MySQL come origine	È stato risolto un problema relativo a MySQL come origine con la convalida dei dati abilitata, a causa del quale si verificava un arresto anomalo dell'attività DMS

Argomento	Risoluzione
	durante l'utilizzo di una tabella con una chiave univoca composta con valori nulli.
MySQL come origine	È stato risolto un problema relativo a MySQL come origine, a causa del quale una tabella veniva sospesa con l'errore di overflow quando le colonne venivano modificate per aggiungere precisione.
Aggiornamento del driver ODBC MySQL a 8.0.23	È stato risolto un problema relativo a MySQL come origine, a causa del quale la collazione "utf8mb4_0900_bin" era incompatibile con il driver mysql utilizzato da DMS.
MySQL: supporto delle modifiche DDL per le tabelle partizionate	È stata introdotta una nuova skipTableSuspension ForPartitionDdl impostazione dell'endpoint MySQL per consentire all'utente di saltare la sospensione della tabella per le modifiche DDL delle partizioni durante il CDC, in modo che DMS possa ora supportare le modifiche DDL per le tabelle MySQL partizionate.
Migrazione da MongoDB a Redshift	È stato risolto un problema relativo alle migrazioni da MongoDB a Redshift, a causa del quale DMS non riusciva a creare la tabella di destinazione su Redshift se la raccolta MongoDB aveva un tipo di dati binario.
Destinazione Redshift: errore di segmentazione di Time Travel nell'applicazione in blocco	È stato risolto un problema relativo a Redshift come target, a causa del quale l'attività DMS si bloccava con BatchApplyEnabled set to true.
Redshift come destinazione	È stato risolto un problema relativo a Redshift come destinazione, a causa del quale, con parallel-load impostato su type=partitions-auto, i segmenti paralleli scrivevano file CSV in blocco nella stessa directory della tabella e interferivano tra loro.

Argomento	Risoluzione
Redshift come destinazione	È stato risolto un problema relativo a Redshift come destinazione, a causa del quale durante la CDC la colonna di destinazione era di tipo booleano mentre l'origine era di tipo carattere variabile.
Redshift come destinazione	È stato migliorato il log delle attività per identificare una modifica DDL che non riesce a replicarsi su Redshift come destinazione.
Convalida dei dati con PostgreSQL	È stato risolto un problema di convalida con PostgreSQL, a causa del quale la convalida non riusciva quando erano presenti tipi di dati booleani.
PostgreSQL come origine	È stato risolto un problema relativo a PostgreSQL come sorgente, in modo che il caricamento completo <code>ExecuteTimeout</code> utilizzasse il campo negli attributi di connessione aggiuntivi.
PostgreSQL come origine	È stato risolto un problema relativo a PostgreSQL come origine, a causa del quale un'attività non andava a buon fine se stava leggendo LSN superiori all'LSN di ripristino dell'attività richiesta per più di 60 minuti, a indicare che c'è un problema con lo slot di replica utilizzato.
PostgreSQL come origine: timestamp prima del 01/01/1970	È stato risolto un problema relativo a PostgreSQL come origine, a causa del quale i timestamp precedenti al 01/01/1970 non venivano migrati correttamente durante la CDC.
PostgreSQL come origine	È stato risolto un problema relativo a PostgreSQL come origine, a causa del quale DMS troncava i valori dei tipi di dati con caratteri variabili durante la CDC.

Argomento	Risoluzione
PostgreSQL come origine: ripresa dell'attività interrotta	È stato risolto un problema relativo a PostgreSQL come origine, a causa del quale la ripresa di una ripetizione dell'attività precedentemente interrotta comportava la mancata esecuzione di una o più transazioni durante la CDC.
Amazon S3 come destinazione	È stato risolto un problema per S3 come destinazione, in cui l'intestazione del file CSV risultante era disattivata di una colonna quando era vera ed era «». AddColumn Name TimestampColumnName
Amazon S3 come origine: comportamento di utilizzo della memoria in fase di pieno carico per l'attività	È stato risolto un problema relativo a S3 come origine, a causa del quale un'attività DMS con pieno carico rilasciava la memoria utilizzata solo dopo che l'intera tabella era stata caricata nel database di destinazione.
Amazon S3 come operazione di ricarica della tabella di destinazione	È stato risolto un problema relativo a S3 come destinazione, a causa del quale un'operazione di ricaricamento della tabella non consentiva la generazione di file CDC.

AWS Note di rilascio di Database Migration Service 3.4.5

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti nella versione 3.4.5 di AWS Database Migration Service (AWS DMS).

Nuova caratteristica o miglioramento	Descrizione
Supporto per Redis come destinazione	AWS DMS ora supporta Redis come destinazione. Utilizzando AWS DMS, ora puoi migrare i dati in tempo reale da qualsiasi fonte AWS DMS supportata a un data store Redis, con tempi di inattività

Nuova caratteristica o miglioramento	Descrizione
	à minimi. Per informazioni sugli AWS DMS obiettivi, consulta. Destinazioni per la migrazione dei dati
Supporto per MongoDB 4.2 e 4.4 come origine	AWS DMS ora supporta MongoDB 4.2 e 4.4 come sorgenti. Utilizzando AWS DMS, ora puoi migrare i dati dai cluster MongoDB 4.2 e 4.4 verso qualsiasi AWS DMS destinazione supportata, incluso Amazon DocumentDB (con compatibilità con MongoDB), con tempi di inattività minimi. Per Origini per la migrazione dei dati informazioni sulle fonti, consulta. AWS DMS
Supporto per più database con MongoDB come origine	AWS DMS ora supporta la migrazione di più database in un'unica attività utilizzando MongoDB come fonte. Utilizzando AWS DMS, ora puoi raggruppare più database di un cluster MongoDB e migrarli utilizzando un'unica attività di migrazione del database. Puoi migrare verso qualsiasi destinazione AWS DMS supportata, incluso Amazon DocumentDB (con compatibilità MongoDB), con tempi di inattività minimi.
Supporto per la segmentazione automatica con MongoDB o Amazon DocumentDB (compatibile con MongoDB) come origine	AWS DMS ora supporta la segmentazione automatica utilizzando MongoDB o Amazon DocumentDB come fonte. Utilizzando AWS DMS, è possibile configurare le attività di migrazione del database per segmentare automaticamente la raccolta di un cluster MongoDB o DocumentDB. Puoi quindi migrare i segmenti in parallelo verso qualsiasi destinazione AWS DMS supportata, incluso Amazon DocumentDB, con tempi di inattività minimi.
Miglioramento delle prestazioni del pieno carico di Amazon Redshift	AWS DMS ora supporta l'uso di thread paralleli quando si utilizza Amazon Redshift come destinazione a pieno carico. Sfruttando le impostazioni delle attività multithread a pieno carico, puoi migliorare le prestazioni della migrazione iniziale da qualsiasi fonte AWS DMS supportata ad Amazon Redshift. Per informazioni sugli AWS DMS obiettivi, consulta. Destinazioni per la migrazione dei dati

I problemi risolti nella versione AWS DMS 3.4.5 includono quanto segue:

- È stato risolto un problema a causa del quale i dati potevano potenzialmente mancare o essere duplicati dopo la ripresa, quando si utilizzava PostgreSQL come origine con un'elevata concorrenza delle transazioni.
- È stato risolto un problema a causa del quale le attività di migrazione del database non riuscivano con l'errore `Could not find relation id...` quando si utilizzava PostgreSQL come origine, con il plugin `pglogical` abilitato.
- È stato risolto un problema a causa del quale le colonne `VARCHAR` non venivano replicate correttamente quando si utilizzava PostgreSQL come origine e Oracle come destinazione.
- È stato risolto un problema a causa del quale le operazioni di eliminazione non venivano acquisite correttamente quando la chiave primaria non era la prima colonna nella definizione della tabella con PostgreSQL come origine.
- È stato risolto un problema a causa del quale le attività di migrazione del database non ricevevano gli aggiornamenti LOB in un'impostazione speciale dei metadati con MySQL come origine.
- È stato risolto un problema a causa del quale le colonne `TIMESTAMP` venivano trattate come `DATETIME` in modalità LOB completa con MySQL versione 8 come origine.
- È stato risolto un problema a causa del quale le attività di migrazione del database non riuscivano durante l'analisi dei record `NULL DATETIME` con MySQL 5.6.4 e versioni successive come origine.
- È stato risolto un problema a causa del quale le attività di migrazione del database si bloccavano dopo aver riscontrato l'errore `Thread is exiting` con Amazon Redshift come destinazione e l'applicazione parallela.
- È stato risolto un problema a causa del quale i dati potevano andare persi quando le attività di migrazione del database si disconnettevano da un endpoint di destinazione Amazon Redshift durante la CDC con applicazione in batch.
- Sono state migliorate le prestazioni del pieno carico tramite chiamata `ACCEPTINVCHARS` con Amazon Redshift come destinazione.
- È stato risolto un problema a causa del quale i record duplicati venivano replicati quando si tornava dalla modalità `one-by-one` di applicazione parallela utilizzando Amazon Redshift come destinazione.
- È stato risolto un problema a causa del quale le attività di migrazione del database non passavano dalla proprietà degli oggetti Amazon S3 a quella del proprietario del bucket `cannedAclForObjects=bucket_owner_full_control` con Amazon S3 come destinazione.
- Migliorato AWS DMS supportando più destinazioni di archiviazione con `ECA additionalArchivedLogDestId` quando si utilizza Oracle come fonte.

- È stato risolto un problema a causa del quale le attività di migrazione del database non riuscivano con l'errore `OCI_INVALID_HANDLE` durante l'aggiornamento di una colonna LOB in modalità LOB completa.
- È stato risolto un problema a causa del quale le colonne `NVARCHAR2` non venivano migrate correttamente durante la CDC con Oracle come origine.
- AWS DMS Migliorato grazie all'attivazione `SafeguardPolicy` quando si utilizza RDS per SQL Server come origine.
- È stato risolto un problema a causa del quale le attività di migrazione del database restituivano un errore in `rdsadmin` con un'origine SQL Server non RDS.
- È stato risolto un problema a causa del quale la convalida dei dati non riusciva con `UUID` come chiave primaria in un'impostazione di partizione con SQL Server come origine.
- È stato risolto un problema a causa del quale le attività di pieno carico e CDC non riuscivano se il LSN richiesto non veniva trovato nel log del database con `Db2 LUW` come origine.
- Migliorato AWS DMS supportando timestamp CDC personalizzati quando si utilizza MongoDB come sorgente.
- È stato risolto un problema a causa del quale le attività di migrazione del database si bloccavano quando venivano arrestate, con MongoDB come origine, e il driver MongoDB restituiva errori su `endSessions`.
- È stato risolto un problema che AWS DMS impediva l'aggiornamento dei campi non primari quando si utilizzava DynamoDB come destinazione.
- È stato risolto un problema a causa del quale la convalida dei dati segnalava false corrispondenze positive sulle colonne `CLOB` e `NCLOB`.
- È stato risolto un problema a causa del quale la convalida dei dati non riusciva sui record contenenti solo spazi bianchi con Oracle come origine.
- È stato risolto un problema a causa del quale si verificava l'arresto anomalo delle attività di migrazione del database quando si troncava una tabella partizionata.
- È stato risolto un problema a causa del quale le attività di migrazione del database non riuscivano durante la creazione della tabella di controllo `awsdms_apply_exceptions`.
- È stato esteso il supporto del plug-in di autenticazione `caching_sha2_password` con MySQL versione 8.

AWS Note di rilascio di Database Migration Service 3.4.4

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.4.4.

Nuova caratteristica o miglioramento	Descrizione
Supporto per la crittografia TLS e l'autenticazione TLS o SASL con Kafka come destinazione	AWS DMS ora supporta la crittografia TLS e l'autenticazione TLS o SASL utilizzando Amazon MSK e il cluster Kafka locale come destinazione. Per ulteriori informazioni sull'utilizzo della crittografia e dell'autenticazione per gli endpoint Kafka, consulta Connessione a Kafka utilizzando Transport Layer Security (TLS) .

I problemi risolti nella versione 3.4.4 includono quanto segue: AWS DMS

- AWS DMS Registrazione migliorata degli errori delle attività quando si utilizzano gli endpoint Oracle.
- L'esecuzione migliorata delle AWS DMS attività continua l'elaborazione quando gli endpoint Oracle Source cambiano ruolo dopo il failover di Oracle Data Guard.
- È stata migliorata la gestione degli errori che considera ORA-12561 come un errore recuperabile quando si utilizzano gli endpoint Oracle.
- È stato risolto un problema a causa del quale le colonne EMPTY_BLOB() e EMPTY_CLOB() venivano migrate come nulle con Oracle come origine.
- È stato risolto un problema per cui AWS DMS le attività non riuscivano ad aggiornare i record dopo l'aggiunta di modifiche DDL alle colonne quando si utilizzava SQL Server come origine.
- È stata migliorata la migrazione di PostgreSQL come origine con il supporto del tipo di dati `TIMESTAMP WITH TIME ZONE`.
- È stato risolto un problema a causa del quale l'impostazione `afterConnectScript` non funzionava durante un pieno carico con PostgreSQL come destinazione.
- È stata introdotta una nuova impostazione `mapUnboundedNumericAsString` per gestire meglio il tipo di data `NUMERIC` senza precisione e scala quando si utilizzano gli endpoint PostgreSQL.
- È stato risolto un problema per cui AWS DMS le attività fallivano con «0 righe interessate» dopo l'interruzione e la ripresa dell'attività quando si utilizzava PostgreSQL come sorgente.

- È stato risolto un problema che AWS DMS impediva la migrazione del tipo di `TIMESTAMP` dati con il BC suffisso quando si utilizza PostgreSQL come origine.
- È stato risolto un problema che AWS DMS impediva la migrazione del `TIMESTAMP` valore «±infinity» quando si utilizza PostgreSQL come sorgente.
- È stato risolto un problema a causa del quale le stringhe vuote venivano trattate come `NULL` con S3 come origine e con l'impostazione `csvNullValue` configurata su altri valori.
- È stato migliorato l'attributo aggiuntivo di connessione `timestampColumnName` in un pieno carico con CDC in modo da renderlo ordinabile durante la CDC con S3 come destinazione.
- È stata migliorata la gestione dei tipi di dati binari in formato esadecimale, ad esempio `BYTE`, `BINARY` e `BLOB`, con S3 come origine.
- È stato risolto un problema a causa del quale i record eliminati venivano migrati con caratteri speciali con S3 come destinazione.
- È stato risolto un problema relativo alla gestione dei valori di chiave vuoti con Amazon DocumentDB (compatibile con MongoDB) come destinazione.
- È stato risolto un problema che AWS DMS impediva la replica `NumberDecimal Decimal128` delle colonne quando si utilizzava MongoDB o Amazon DocumentDB (con compatibilità con MongoDB) come sorgente.
- È stato risolto un problema che consentiva alle attività di CDC di riprovare in caso di failover con MongoDB o Amazon DocumentDB (compatibile con MongoDB) come origine.
- È stata aggiunta un'opzione per rimuovere il prefisso esadecimale «0x» dai valori RAW dei tipi di dati quando si utilizza Kinesis, Kafka o come destinazione. OpenSearch
- È stato risolto un problema a causa del quale la convalida non riusciva su colonne di caratteri a lunghezza fissa con Db2 LUW come origine.
- È stato risolto un problema a causa del quale la convalida non riusciva quando il tipo di dati di origine o il tipo di dati di destinazione era `FLOAT` o `DOUBLE`.
- È stato risolto un problema a causa del quale la convalida dei caratteri `NULL` non riusciva con Oracle come origine.
- È stato risolto un problema a causa del quale la convalida delle colonne XML non riusciva con Oracle come origine.
- È stato risolto un problema a causa del quale AWS DMS le attività si bloccavano quando erano presenti colonne annullabili nelle chiavi composite che utilizzavano MySQL come sorgente.

- È stato risolto un problema che AWS DMS non riusciva a convalidare entrambe UNIQUEIDENTIFIER le colonne dagli endpoint di origine di SQL Server e le colonne UUID dagli endpoint di destinazione PostgreSQL.
- È stato risolto un problema a causa del quale un'attività di CDC non utilizzava una definizione di tabella di origine aggiornata dopo la modifica.
- È stato migliorato il AWS DMS failover per considerare gli errori delle attività causati da un nome utente o una password non validi come errori recuperabili.
- È stato risolto un problema per cui AWS DMS le attività fallivano a causa della mancanza di LSN quando si utilizzava RDS per SQL Server come origine.

AWS Note di rilascio di Database Migration Service 3.4.3

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.4.3.

Nuova caratteristica o miglioramento	Descrizione
Nuova versione di Amazon DocumentDB	Amazon DocumentDB versione 4.0 è ora supportato come origine.
Nuova versione di MariaDB	MariaDB versione 10.4 è ora supportato come origine e destinazione.
Support per AWS Secrets Manager l'integrazione	È possibile archiviare in modo sicuro i dettagli di connessione al database (credenziali utente) per gli endpoint supportati in AWS Secrets Manager. È quindi possibile inviare il segreto corrispondente anziché le credenziali in testo semplice AWS DMS quando si crea o si modifica un endpoint. AWS DMS quindi si connette ai database degli endpoint utilizzando il segreto. Per ulteriori informazioni sulla creazione di segreti per gli AWS DMS endpoint, consulta Utilizzo dei segreti per accedere agli endpoint AWS Database Migration Service

Nuova caratteristica o miglioramento	Descrizione
Opzioni più ampie per le istanze di replica C5 e R5	È ora possibile creare le seguenti dimensioni più grandi per l'istanza di replica: dimensioni C5 fino a 96 vCPU e 192 GiB di memoria e dimensioni R5 fino a 96 vCPU e 768 GiB di memoria.
Miglioramento delle prestazioni di Amazon Redshift	AWS DMS ora supporta l'applicazione parallela quando si utilizza Redshift come obiettivo per migliorare le prestazioni della replica in corso. Per ulteriori informazioni, consulta Impostazioni delle attività multithread per Amazon Redshift .

I problemi risolti nella versione AWS DMS 3.4.3 includono quanto segue:

- È stato risolto un problema per cui il timestamp di commit diventava "1970-01-01 00:00:00" per gli eventi differiti con Db2 LUW come origine.
- È stato risolto un problema a causa del quale AWS DMS le attività non funzionavano con una NVARCHAR colonna come chiave primaria quando si utilizzava SQL Server come origine con la modalità Full LOB.
- È stato risolto un problema di record mancanti durante la fase di modifiche memorizzate nella cache con SQL Server come origine.
- È stato risolto un problema a causa del quale i record venivano ignorati dopo la ripresa AWS DMS delle attività quando si utilizzava RDS per SQL Server come origine.
- È stato risolto un problema a causa del quale il componente di registrazione AWS DMS ASSERTION generava log di grandi dimensioni per SQL Server.
- È stato risolto un problema a causa del quale la convalida dei dati non riusciva durante la fase CDC per l'overflow dell'analisi delle colonne con MySQL come origine.
- È stato risolto un problema a causa del quale AWS DMS le attività si bloccavano a causa di un errore di segmentazione durante la convalida dei dati quando si utilizzava PostgreSQL come destinazione.
- È stato risolto un problema a causa del quale la convalida dei dati non riusciva sul tipo di dati DOUBLE durante la CDC con PostgreSQL come origine e destinazione.
- È stato risolto un problema a causa del quale i record inseriti dal comando copy non venivano replicati correttamente con PostgreSQL come origine e Redshift come destinazione.

- È stato risolto un problema di perdita di dati durante la fase di modifiche memorizzate nella cache con PostgreSQL come origine.
- È stato risolto un problema a causa del quale si verificava la perdita di dati o la duplicazione dei record con PostgreSQL come origine.
- È stato risolto un problema a causa del quale gli schemi con casi misti non venivano migrati usando pglogical con PostgreSQL come origine.
- È stato risolto un problema a causa del quale l'ultimo messaggio di errore non conteneva l'errore ORA con Oracle come origine.
- È stato risolto un problema per cui AWS DMS le attività non riuscivano a creare istruzioni UPDATE quando si utilizzava Oracle come destinazione.
- È stato risolto un problema per cui AWS DMS le attività non replicavano i dati quando si utilizzava Oracle 12.2 come origine con la configurazione ASM e Pluggable Database.
- È stata migliorata l'analisi dei record preservando la conformità delle quote a RFC 4180 con S3 come origine.
- È stata migliorata la gestione di `timestampColumnName` in modo che la colonna di pieno carico sia ordinabile con quella del CDC.
- Introducendo una nuova impostazione dell'`endpointMessageMaxBytes`, è stato risolto un problema a causa del quale AWS DMS le attività non funzionavano quando erano presenti elementi LOB di dimensioni superiori a 1 MB.
- È stato risolto un problema per cui AWS DMS le attività si bloccavano a causa di un errore di segmentazione quando si utilizzava Redshift come destinazione.
- Registrazione degli errori migliorata per la connessione di test Redshift.
- È stato risolto un problema AWS DMS che impediva il trasferimento di tutti i documenti da MongoDB a DocumentDB durante il caricamento completo.
- È stato risolto un problema per cui AWS DMS le attività segnalavano un errore irreversibile quando nessuna tabella era inclusa nelle regole di mappatura delle tabelle.
- È stato risolto un problema a causa del quale gli schemi e le tabelle creati prima del riavvio delle attività AWS DMS non si replicavano sulla destinazione con MySQL come origine.
- È stato risolto un problema a causa del quale il carattere jolly di escape `[_]` non eseguiva l'escape del carattere jolly `"_"` nella regola di esclusione con MySQL come origine.
- È stato risolto un problema a causa del quale la colonna del tipo di dati UNSIGNED BIGINT non veniva replicata correttamente con MySQL come origine.

AWS Note di rilascio di Database Migration Service 3.4.2

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.4.2.

Nuova caratteristica o miglioramento	Descrizione
<p>Supporto per la connessione privata di Amazon Virtual Private Cloud (Amazon VPC) AWS al Database Migration Service (DMS) senza richiedere un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione AWS Direct Connect</p>	<p>Ora puoi connetterti e accedere AWS DMS dal tuo Amazon VPC tramite un endpoint di interfaccia VPC creato da te. Questo endpoint di interfaccia consente di isolare tutte le attività di rete dell'istanza di AWS DMS replica all'interno dell'infrastruttura di rete Amazon. Includendo un riferimento a questo endpoint di interfaccia in tutte le chiamate API all' AWS DMS utilizzo dell'SDK AWS CLI o di un SDK, ti assicuri che tutte le AWS DMS attività rimangano invisibili alla rete Internet pubblica. Per ulteriori informazioni, consulta Sicurezza dell'infrastruttura in AWS Database Migration Service.</p> <div data-bbox="544 1041 1507 1262" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>Questa funzionalità è disponibile utilizzando tutte le versioni AWS DMS del motore supportate.</p> </div>
<p>Partizionamento delle cartelle basato sulla data CDC con Amazon S3 come destinazione</p>	<p>AWS DMS ora supporta il partizionamento delle cartelle basato sulla data durante la replica dei dati utilizzando S3 come destinazione. Per ulteriori informazioni, consulta Utilizzo del partizionamento delle cartelle in base alla data.</p>

I problemi risolti nella versione 3.4.2 includono quanto segue: AWS DMS

- È stata aggiunta un'opzione STATUPDATE per l'esecuzione di una migrazione con Redshift come destinazione.
- Sono state migliorate le attività di convalida introducendo una nuova impostazione. `ValidQueryCdcDelaySecond` ritarda la prima query di convalida sugli endpoint di origine e

di destinazione per contribuire a ridurre il conflitto di risorse quando la latenza di migrazione è elevata.

- È stato risolto un problema che AWS DMS richiedeva molto tempo per avviare le attività di convalida.
- È stato risolto un problema a causa del quale venivano generati record vuoti all'avvio o all'arresto delle attività di replica con S3 come destinazione.
- È stato risolto un problema a causa del quale le attività si bloccavano alla fine di un pieno carico.
- È stato risolto un problema a causa del quale le attività si bloccavano quando una tabella di origine conteneva errori nei dati con S3 come origine.
- È stato risolto un problema a causa del quale le attività si bloccavano all'avvio quando l'account utente dell'endpoint di origine era disabilitato.
- È stato risolto un problema a causa del quale le attività si bloccavano con PostgreSQL come origine con `REPLICA IDENTITY FULL`.
- È stato risolto un problema a causa del quale le attività perdevano le transazioni con PostgreSQL come origine con il plug-in `pglogical`.
- È stato risolto un problema AWS DMS che impediva l'eliminazione dei file sorgente compressi quando si utilizzava Redshift come destinazione.
- È stato risolto un problema a causa del quale le attività di convalida segnalavano falsi negativi con MySQL come origine e destinazione con il tipo di dati `BIGINT UNSIGNED`.
- È stato risolto un problema a causa del quale le attività di convalida segnalavano falsi positivi con SQL Server come origine con una colonna di chiave primaria di tipo `CHAR`.
- È stato risolto un problema AWS DMS che impediva la cancellazione degli oggetti di destinazione quando si utilizzavano `start-replication` per avviare attività di replica utilizzando S3 come destinazione.
- Sono stati risolti diversi problemi relativi alla convalida dei dati con Db2 come origine.
- È stato risolto un problema a causa del quale le attività di convalida si bloccavano con SQL Server come origine con la colonna `VARCHAR` come chiave primaria.
- È stato aggiunto il supporto per il tipo di dati `TIMESTAMP WITH TIMEZONE` con PostgreSQL come origine.

AWS Note sulla versione beta di Database Migration Service 3.4.1

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.4.1 Beta.


Nuova caratteristica o miglioramento	Descrizione
Nuova versione di MongoDB	MongoDB versione 4.0 è ora supportato come origine.
Supporto di TLS 1.2 per SQL Server	AWS DMS ora supporta TLS 1.2 per gli endpoint SQL Server.

I problemi risolti nella versione AWS DMS 3.4.1 Beta includono quanto segue:

- È stato migliorato il supporto TDE per Oracle 19c.
- È stato migliorato il supporto del set di caratteri utf8mb4 e del tipo di dati di identità con Redshift come destinazione.
- È stata migliorata la gestione degli errori delle attività di replica con MySQL come origine senza il log binario.
- È stato migliorato il supporto per la convalida dei dati su vari tipi di dati e set di caratteri.
- È stata migliorata la gestione dei valori nulli con una nuova impostazione degli endpoint `IncludeNullAndEmpty` con Kinesis e Kafka come destinazione.
- È stata migliorata la registrazione e la gestione degli errori con Kafka come destinazione.
- È stata migliorata la compensazione dell'ora legale con SQL Server come origine.
- È stato risolto un problema a causa del quale le attività di replica tentavano di creare tabelle esistenti per Oracle come destinazione.
- È stato risolto un problema a causa del quale le attività di replica si bloccavano dopo l'interruzione della connessione al database con Oracle come origine.
- È stato risolto un problema a causa del quale le attività di replica non riuscivano a rilevare e riconnettersi al nuovo primario con SQL Server come origine con l'impostazione `AlwaysON`.
- È stato risolto un problema a causa del quale le attività di replica non aggiungevano una "0P" per la colonna "D" in determinate condizioni per S3 come destinazione.

AWS Note sulla versione beta di Database Migration Service 3.4.0

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.4.0.

Nuova caratteristica o miglioramento	Descrizione
Nuova versione di MySQL	AWS DMS ora supporta la versione 8.0 di MySQL come sorgente, tranne quando il payload della transazione è compresso.
Supporto di TLS 1.2 per MySQL	AWS DMS ora supporta TLS 1.2 per endpoint MySQL.
Nuova versione di MariaDB	AWS DMS ora supporta MariaDB versione 10.3.13 come sorgente.
Mancato SysAdmin accesso a sorgenti Microsoft SQL Server autogestite	<p>AWS DMS ora supporta l'accesso da parte di non SysAdmin utenti agli endpoint di origine SQL Server locali e ospitati da EC2.</p> <div data-bbox="544 976 1507 1249" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note</p> <p>Questa funzionalità è attualmente in versione beta. Se vuoi provarlo, contatta AWS l'assistenza per ulteriori informazioni.</p> </div>
Attività di CDC e tabelle di origine Oracle create utilizzando CREATE TABLE AS	AWS DMS ora supporta sia le attività a pieno carico che quelle esclusivamente CDC e CDC eseguite su tabelle di sorgenti Oracle create utilizzando l'istruzione. CREATE TABLE AS

I problemi risolti nella versione AWS DMS 3.4.0 includono:

- È stata migliorata la valutazione delle attività preliminari alla migrazione. Per ulteriori informazioni, consulta [Abilitazione e utilizzo delle valutazioni preliminari alla migrazione di un'attività](#).
- È stata migliorata la convalida dei dati per tipi di dati mobili, reali e doppi.
- È stato migliorato Amazon Redshift come destinazione gestendo meglio l'errore: "The specified key does not exist."

- Supporta le impostazioni delle attività di caricamento CDC multithread, tra cui `ParallelApplyThreadsParallelApplyBufferSize`, e, `ParallelApplyQueuesPerThread` per Amazon OpenSearch Service (OpenSearch Service) come destinazione.
- OpenSearch Servizio migliorato come destinazione supportando l'uso di chiavi primarie composite.
- È stato risolto un problema a causa del quale la connessione di prova non riusciva con PostgreSQL come origine e la password contenente caratteri speciali.
- È stato risolto un problema relativo all'utilizzo di SQL Server come origine a causa del quale alcune colonne VARCHAR venivano troncate.
- È stato risolto un problema AWS DMS che impediva la chiusura delle transazioni aperte quando si utilizza Amazon RDS SQL Server come sorgente. Ciò poteva causare la perdita di dati se il parametro dell'intervallo di polling era impostato in modo errato. Per ulteriori informazioni su come impostare un valore di intervallo di polling consigliato, consulta [Utilizzo di un database Microsoft SQL Server come origine per AWS DMS](#).
- È stato risolto un problema relativo a Oracle Standby come origine a causa del quale le attività di CDC si interrompevano inaspettatamente con Binary Reader.
- È stato risolto un problema relativo a IBM DB2 per LUW a causa del quale l'attività non riusciva con il messaggio "The Numeric literal 0 is not valid because its value is out of range."
- È stato risolto un problema relativo alla migrazione da PostgreSQL a PostgreSQL a causa del quale veniva aggiunta una nuova colonna all'origine PostgreSQL e la colonna veniva creata con un tipo di dati diverso dal tipo di dati per cui la colonna era stata inizialmente creata nell'origine.
- È stato risolto un problema relativo all'origine MySQL a causa del quale l'attività di migrazione si interrompeva in modo imprevisto quando non era in grado di recuperare i binlog.
- È stato risolto un problema relativo alla destinazione Oracle quando si utilizza `BatchApply`.
- È stato risolto un problema relativo a MySQL e MariaDB per la migrazione del tipo di dati TIME.
- È stato risolto un problema relativo all'origine IBM DB2 LUW a causa del quale la migrazione delle tabelle con LOB non riusciva quando le tabelle non avevano una chiave primaria o una chiave unica.

AWS Note di rilascio di Database Migration Service 3.3.4

I problemi risolti nella versione AWS DMS 3.3.4 includono quanto segue:

- È stato risolto un problema a causa del quale le transazioni venivano eliminate o duplicate con PostgreSQL come origine.
- È stato migliorato il supporto per l'uso del simbolo del dollaro (\$) nei nomi degli schemi.
- È stato risolto un problema a causa del quale le istanze di replica non chiudevano le transazioni aperte con RDS SQL Server come origine.
- È stato risolto un problema a causa del quale la connessione di prova non riusciva con PostgreSQL come origine e la password contenente caratteri speciali.
- È stato migliorato Amazon Redshift come destinazione gestendo meglio l'errore: "The specified key does not exist."
- È stato migliorato il supporto per la convalida dei dati su vari tipi di dati e set di caratteri.
- È stato risolto un problema a causa del quale le attività di replica tentavano di creare tabelle esistenti per Oracle come destinazione.
- È stato risolto un problema a causa del quale le attività di replica non aggiungevano una "OP" per la colonna "D" in determinate condizioni per Amazon S3 come destinazione.

AWS Note di rilascio di Database Migration Service 3.3.3

La tabella seguente mostra le nuove funzionalità e i miglioramenti introdotti in AWS DMS versione 3.3.3.

Nuova caratteristica o miglioramento	Descrizione
La nuova versione di PostgreSQL	PostgreSQL versione 12 è ora supportato come origine e destinazione.
Supporto per chiave primaria composta con Amazon OpenSearch Service come destinazione	A partire da AWS DMS 3.3.3, l'uso di una chiave primaria composta è supportato dagli obiettivi del OpenSearch servizio.
Supporto per i tipi di dati estesi Oracle	I tipi di dati estesi Oracle sia per l'origine Oracle che per le destinazioni sono ora supportati.

Nuova caratteristica o miglioramento	Descrizione
Aumento del numero di AWS DMS risorse per account	Il limite al numero di AWS DMS risorse che è possibile creare è aumentato. Per ulteriori informazioni, consulta Quote per AWS Database Migration Service .

I problemi risolti nella versione AWS DMS 3.3.3 includono quanto segue:

- È stato risolto un problema a causa del quale si verificava l'arresto anomalo di un'attività utilizzando una specifica istruzione di aggiornamento con Parallel Apply in Amazon Kinesis.
- È stato risolto un problema a causa del quale si verificava l'arresto anomalo sull'istruzione ALTER TABLE con Amazon S3 come destinazione.
- Risolto un problema per cui i valori delle colonne poligonali vengono troncati quando si utilizza Microsoft SQL Server come origine.
- Risolto un problema relativo al convertitore Unicode di JA16SJITILDE e JA16EUCTILDE quando si utilizzava Oracle come origine.
- Risolto un problema per cui le colonne MEDIUMTEXT e LONGTEXT non riuscivano a migrare dal formato MySQL al formato S3 con valori separati da virgole (CSV).
- Risolto un problema per cui le colonne booleane venivano trasformate in tipi non corretti con l'output di Apache Parquet.
- Risolto un problema relativo alle colonne varchar estese in Oracle.
- Risolto un problema per il quale le attività di convalida dei dati non erano riuscite a causa di determinate combinazioni di timestamp.
- Risolto un problema con la replica DDL (Data Definition Language) di Sybase.
- Risolto un problema che riguardava un arresto anomalo di origine Oracle Real Application Clusters (RAC) con Oracle Binary Reader.
- Risolto un problema di convalida per le destinazioni Oracle con il caso dei nomi dello schema.
- Risolto un problema con la convalida delle versioni 9.7 e 10 di IBM Db2.
- Risolto un problema per un'attività che non si fermava due volte con `StopTaskCachedChangesApplied` e `StopTaskCachedChangesNotApplied` abilitata.

Cronologia dei documenti

Nella seguente tabella vengono descritte le modifiche importanti per la documentazione della guida per l'utente di AWS Database Migration Service dopo gennaio 2018.

Puoi abbonarti a un feed RSS per ricevere le notifiche sugli aggiornamenti di questa documentazione. Per ulteriori dettagli sulle versioni di AWS DMS, consulta [AWS Note di rilascio DMS](#).

Modifica	Descrizione	Data
AWS DMS ha aggiunto il supporto per RDS IBM DB2 come destinazione	AWS DMS ora supporta l'utilizzo di Amazon RDS IBM DB2 come destinazione.	4 dicembre 2023
AWS DMS ha aggiunto il supporto per Timestream come destinazione	AWS DMS ora supporta Timestream come destinazione.	17 novembre 2023
AWS DMS ha aggiunto il supporto per la convalida dei dati delle destinazioni Redshift	AWS DMS ora supporta la convalida dei dati nelle destinazioni Redshift.	14 novembre 2023
AWS DMS ha aggiunto il supporto per quattro nuovi tipi di endpoint	AWS DMS ora supporta l'utilizzo di Microsoft Azure Database per PostgreSQL, Microsoft Azure Database per MySQL, OCI MySQL Heatwave e Google Cloud per PostgreSQL come origine.	26 ottobre 2023
AWS DMS ha aggiunto il supporto per il nuovo ruolo collegato ai servizi AWS	AWS DMS ora supporta il ruolo collegato ai servizi AWS <code>AWSServiceRoleForDMS</code> <code>Serverless</code> che consente di creare e gestire risorse AWS DMS per tuo conto, ad esempio la pubblicazione di punti dati	22 maggio 2023

	delle metriche su Amazon CloudWatch.	
<u>AWS DMS ha aggiunto il supporto per una nuova policy gestita da AWS</u>	AWS DMS ora supporta la policy gestita da AWS che consente la pubblicazione di log di replica serverless su File di log CloudWatch.	22 maggio 2023
<u>AWS DMS ha aggiunto il supporto per una nuova policy gestita da AWS</u>	AWS DMS ora supporta la policy gestita da AWS che consente di pubblicare i punti dati delle metriche in Amazon CloudWatch. Inoltre, AWS DMS ha iniziato a monitorar e le modifiche per le policy gestite da AWS.	6 marzo 2023
<u>Supporto per gli endpoint VPC di origine e di destinazione</u>	AWS DMS supporta ora gli endpoint cloud privato virtuale (VPC) come origini e destinazioni. AWS DMS ora può connettersi a qualsiasi servizio AWS con endpoint VPC quando nel VPC AWS DMS sono definite esplicitamente le route ai servizi.	30 giugno 2022
<u>Supporto per la replica di lettura SQL Server come origine</u>	AWS DMS ora supporta la replica di lettura SQL Server come origine. Utilizzando AWS DMS, ora è possibile eseguire migrazioni in tempo reale dalla replica di lettura SQL Server verso qualsiasi destinazione AWS DMS supportata.	30 giugno 2022

[Supporto per i database IBM Db2 z/OS come origine per solo pieno carico](#)

AWS DMS ora supporta i database IBM Db2 z/OS come origine. Utilizzando AWS DMS, ora è possibile eseguire migrazioni in tempo reale dai mainframe Db2 verso qualsiasi destinazione AWS DMS supportata.

30 giugno 2022

[Supporto per gli eventi EventBridge DMS](#)

AWS DMS supporta la gestione delle sottoscrizioni agli eventi utilizzando EventBridge per gli eventi DMS.

30 giugno 2022

[Supporto per Babelfish come destinazione](#)

AWS DMS ora supporta Babelfish come destinazione. Utilizzando AWS DMS ora puoi migrare i dati in tempo reale da qualsiasi origine AWS DMS supportata a Babelfish, con tempi di inattività minimi.

30 giugno 2022

[Supporto per Aurora serverless v2 come destinazione](#)

AWS DMS ora supporta Aurora serverless v2 come destinazione. Con AWS DMS ora puoi eseguire migrazioni in tempo reale ad Aurora serverless v2.

30 giugno 2022

[Tutorial sulle nozioni di base](#)

Un aggiornamento per il tutorial sulle nozioni di base di AWS DMS. Il tutorial utilizza un database MySQL come origine e un database PostgreSQL come destinazione.

20 maggio 2021

Supporto per Amazon Neptune come destinazione	Aggiunto il supporto per Amazon Neptune come destinazione per la migrazione dei dati.	1 giugno 2020
Supporto per Apache Kafka come destinazione	Aggiunto il supporto per Apache Kafka come destinazione per la migrazione dei dati.	20 marzo 2020
Contenuti di sicurezza aggiornati	Contenuti di sicurezza aggiornati e standardizzati in risposta alle richieste dei clienti.	20 dicembre 2019
Migrazione con AWS Snowball Edge	Aggiunto il supporto per l'utilizzo di AWS Snowball Edge per la migrazione di database di grandi dimensioni.	24 gennaio 2019
Supporto per Amazon DocumentDB (compatibile con MongoDB) come destinazione	Aggiunto il supporto per Amazon DocumentDB (compatibile con MongoDB) come destinazione per la migrazione dei dati.	9 gennaio 2019
Supporto per servizio OpenSearch di Amazon e flusso di dati Amazon Kinesis come destinazioni	Aggiunto il supporto per il servizio OpenSearch e il flusso di dati Amazon Kinesis come destinazioni per la migrazione dei dati.	15 novembre 2018
Supporto di avvio nativo CDC	Aggiunto il supporto per i punti di avvio nativo quando si utilizza la funzionalità CDC (Change Data Capture).	28 giugno 2018

[Supporto di Db2 LUW](#)

Aggiunto il supporto per IBM Db2 LUW come origine per la migrazione dei dati.

26 Aprile 2018

[Supporto di SQL Server come destinazione](#)

Aggiunto il supporto per Amazon RDS per Microsoft SQL Server come origine.

6 febbraio 2018

Glossario AWS

Per la terminologia AWS più recente, consultare il [glossario AWS](#) nella documentazione di riferimento per Glossario AWS.

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.