



Guida alla gestione

# Amazon Redshift



# Amazon Redshift: Guida alla gestione

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

Che cos'è Amazon Redshift? .....	1
È la prima volta che utilizzi Amazon Redshift? .....	1
Panoramica delle funzionalità di Amazon Redshift Serverless .....	2
Panoramica sui cluster con provisioning di Amazon Redshift .....	5
Gestione dei cluster .....	5
Sicurezza e accesso ai cluster .....	6
Monitoraggio dei cluster .....	8
Database .....	8
Confronto di Amazon Redshift Serverless con un data warehouse con provisioning di Amazon Redshift .....	9
Utilizzo delle interfacce di gestione Amazon Redshift per i cluster predisposti .....	35
Lavorare con AWS gli SDK .....	36
Firma di una richiesta HTTP .....	37
Configurazione della CLI di Amazon Redshift .....	42
Amazon Redshift Serverless .....	44
Cos'è Amazon Redshift Serverless? .....	44
Console Serverless Amazon Redshift .....	45
Considerazioni su quando utilizzare Amazon Redshift Serverless .....	48
Capacità di calcolo per Amazon Redshift Serverless .....	51
Conoscere la capacità di Amazon Redshift Serverless .....	51
Dimensionamento e ottimizzazione basati sull'intelligenza artificiale (anteprima) .....	52
Fatturazione per Amazon Redshift Serverless .....	54
Prezzi .....	54
Fatturazione per la capacità di calcolo .....	54
Fatturazione per l'archiviazione .....	59
Usare la prova gratuita di Amazon Redshift Serverless .....	60
Note di utilizzo nella fatturazione .....	60
Connessione ad Amazon Redshift Serverless .....	62
Connessione ad Amazon Redshift Serverless .....	62
Connessione ad Amazon Redshift Serverless tramite driver JDBC .....	62
Connessione ad Amazon Redshift Serverless con l'API dei dati .....	64
Connessione con SSL ad Amazon Redshift Serverless .....	65
Connessione ad Amazon Redshift Serverless da un endpoint VPC gestito da Amazon Redshift .....	67

Connessione ad Amazon Redshift serverless da un endpoint VPC Redshift di un altro account o un'altra regione .....	68
Configurazione delle impostazioni appropriate per il traffico di rete per Amazon Redshift serverless .....	73
Definizione dei ruoli del database da assegnare agli utenti federati in Amazon Redshift serverless .....	73
Altre risorse .....	73
Definizione dei ruoli del database da assegnare agli utenti federati in Amazon Redshift serverless .....	73
Identity and Access Management in Amazon Redshift Serverless .....	77
Concessione delle autorizzazioni ad Amazon Redshift Serverless .....	77
Nozioni di base sulle credenziali IAM per Amazon Redshift .....	79
Gestione dell'accesso agli oggetti del database Amazon Redshift Serverless con autorizzazioni relative ai ruoli del database .....	80
Migrazione di un cluster con provisioning ad Amazon Redshift Serverless .....	82
Creazione di uno snapshot del cluster con provisioning .....	82
Connessione ad Amazon Redshift serverless usando un driver .....	83
Utilizzo dell'SDK di Amazon Redshift Serverless .....	85
Panoramica dei gruppi di lavoro di Amazon Redshift Serverless .....	86
Panoramica dei gruppi di lavoro di Amazon Redshift Serverless .....	86
Gestione di Amazon Redshift serverless tramite la console .....	88
Configurazione di Amazon Redshift Serverless per la prima volta .....	88
Utilizzo con gruppi di lavoro .....	89
Utilizzo degli spazi dei nomi .....	94
Gestione dei limiti di utilizzo, dei limiti delle query e di altre attività amministrative .....	98
Monitoraggio di query e carichi di lavoro con Amazon Redshift Serverless .....	100
Monitoraggio di query e carichi di lavoro con Amazon Redshift Serverless .....	100
Registrazione di verifiche per Amazon Redshift Serverless .....	104
Esportazione dei log .....	104
Utilizzo di snapshot e punti di ripristino .....	114
Snapshot .....	115
Punti di ripristino .....	118
Pianificazione degli snapshot .....	119
Copia dei backup in un'altra Regione AWS .....	122
Ripristino di una tabella .....	123
Utilizzo della AWS Command Line Interface e dell'API Amazon Redshift serverless .....	124

Condivisione dei dati in Amazon Redshift Serverless .....	127
Condivisione dei dati in Amazon Redshift Serverless .....	127
Panoramica delle risorse di tagging .....	129
Cluster con provisioning di Amazon Redshift .....	131
Panoramica di Amazon Redshift .....	131
Cluster e nodi .....	132
Utilizzo di EC2-VPC durante la creazione del cluster .....	137
EC2-VPC .....	138
Allarme predefinito dello spazio su disco .....	138
Stato del cluster .....	139
Considerazioni sull'utilizzo dei cluster con provisioning di Amazon Redshift .....	142
Considerazioni su regioni e zone di disponibilità .....	142
Manutenzione del cluster .....	142
Gestione dei limiti di utilizzo .....	149
Funzionalità di rete supportate dai nodi RA3 .....	151
Tipi di nodo .....	152
Operazioni del cluster .....	158
Ridimensionamento di cluster .....	158
Sospensione e ripristino dei cluster .....	174
Ridenominazione dei cluster .....	177
Chiusura ed eliminazione di cluster .....	178
Trasferimento del cluster .....	178
Snapshot e backup .....	184
Configurazione dell'implementazione multi-AZ .....	213
Configurazione di un'implementazione multi-AZ .....	213
Gestione di un'implementazione multi-AZ .....	216
Errore dell'implementazione multi-AZ .....	224
Monitoraggio delle query per Multi-AZ .....	226
Gestione dei cluster con la console .....	228
Creazione di un cluster .....	229
Creazione di un cluster di anteprima .....	233
Modifica di un cluster .....	234
Eliminazione di un cluster .....	235
Riavvio di un cluster .....	236
Ridimensionamento di un cluster .....	237
Per aggiornare una versione di rilascio del cluster .....	238

Recupero di informazioni sulla configurazione del cluster .....	238
Visualizzazione di una panoramica dello stato di un cluster .....	239
Acquisizione di uno snapshot di un cluster .....	239
Creazione o modifica dell'allarme dello spazio su disco .....	239
Utilizzo dei dati di prestazioni del cluster .....	240
Gestione dei cluster utilizzando l'API AWS CLI Amazon Redshift .....	240
Gestione dei cluster in un VPC .....	241
Panoramica .....	241
Creazione di un cluster in un VPC .....	244
Gestione dei gruppi di sicurezza VPC per un cluster .....	245
Configurazione delle impostazioni di comunicazione dei gruppi di sicurezza per i cluster Amazon Redshift o per un gruppo di lavoro di Amazon Redshift serverless .....	247
Come funziona Amazon Redshift con la condivisione di risorse tramite VPC AWS .....	250
Gruppi di sottoreti dei cluster .....	252
Cronologia delle versioni del cluster .....	254
Utilizzo delle integrazioni Zero-ETL .....	255
Considerazioni .....	257
Guida introduttiva alle integrazioni Zero-ETL .....	259
Creazione e configurazione di un data warehouse Amazon Redshift di destinazione .....	260
Attivazione della distinzione tra maiuscole e minuscole .....	263
Configurazione dell'autorizzazione in Amazon Redshift .....	265
Passaggi successivi .....	269
Creazione di database di destinazione .....	269
Creazione di un database di destinazione in Amazon Redshift .....	269
Aggiunta dei dati all'origine .....	271
Esecuzione di query e creazione di viste materializzate con i dati replicati .....	271
Esecuzione di query sui dati replicati in Amazon Redshift .....	271
Creazione di viste materializzate con i dati replicati .....	272
Gestione delle integrazioni Zero-ETL .....	274
Condivisione dei dati in Amazon Redshift .....	276
Metriche per le integrazioni Zero-ETL .....	277
Risoluzione dei problemi delle integrazioni Zero-ETL .....	278
Esecuzione di query su un database .....	289
Connessione ad Amazon Redshift .....	290
Esecuzione di query in un database con l'editor di query v2 di Amazon Redshift .....	290
Configurazione del Account AWS .....	292

Utilizzo dell'editor di query v2 .....	299
Interazione con SQL generativo dell'editor di query v2 (anteprima) .....	318
Caricamento dei dati in un database .....	326
Autorizzazione e esecuzione di query .....	336
Autorizzazione ed esecuzione di notebook .....	342
Interrogare il AWS Glue Data Catalog .....	345
Esecuzione di query in un data lake .....	349
Utilizzo dell'unità di condivisione dati .....	351
Pianificazione di una query .....	355
Visualizzazione dei risultati .....	365
Collaborazione e condivisione come team .....	371
Esecuzione di query in un database con l'editor della query .....	373
Considerazioni .....	374
Abilitazione dell'accesso .....	375
Connessione con l'editor di query .....	377
Utilizzo dell'editor della query .....	378
Pianificazione di una query .....	379
Connessione a un data warehouse utilizzando gli strumenti client SQL .....	384
Consigli per la connessione con gli strumenti client .....	385
Configurazione delle connessioni in Amazon Redshift .....	385
Configurazione delle opzioni di sicurezza per le connessioni .....	563
Connessione da codice e strumenti client .....	572
Connessione con SQL Workbench/J .....	622
Connect al tuo data warehouse in modo programmatico .....	622
Connettersi ad Amazon Redshift con un profilo di autenticazione. ....	622
Risoluzione dei problemi di connessione in Amazon Redshift .....	626
Utilizzo dell'API Data .....	634
Utilizzo dell'API dati .....	635
Considerazioni da fare durante la chiamata all'API dati di Amazon Redshift .....	635
Esecuzione di istruzioni SQL con un token di idempotenza .....	641
Autorizzazione di accesso .....	642
Chiamata dell'API dati .....	649
Risoluzione dei problemi correlati alla configurazione dell'API dati .....	674
Pianificazione delle operazioni Data API con Amazon EventBridge .....	675
Monitoraggio dell'API dati .....	679
Gruppi di parametri .....	682

Panoramica .....	682
Informazioni sui gruppi di parametri .....	682
Valori di parametro predefiniti .....	683
Configurazione dei valori dei parametri utilizzando il AWS CLI .....	685
Configurazione della gestione del carico di lavoro .....	686
Proprietà WLM dinamiche e statiche .....	687
Proprietà del parametro <code>wlm_json_configuration</code> .....	687
Configurazione del parametro <code>wlm_json_configuration</code> utilizzando il AWS CLI .....	695
Gestione di gruppi di parametri mediante la console .....	703
Creazione di un gruppo di parametri .....	704
Modifica di un gruppo di parametri .....	704
Creazione o modifica di una regola di monitoraggio di query mediante la console .....	707
Eliminazione di un gruppo di parametri .....	709
Associazione di un gruppo di parametri a un cluster .....	709
Gestione dei gruppi di parametri utilizzando AWS CLI l'API Amazon Redshift .....	709
Integrazione con un partner AWS .....	711
Integrazione con un AWS partner tramite la console Amazon Redshift .....	711
Caricamento dei dati con i partner AWS .....	712
Acquisto di nodi riservati .....	714
Panoramica .....	714
Informazioni sulle offerte di nodi riservati .....	714
Confronto tra i prezzi delle offerte di nodi riservati .....	715
Modalità di funzionamento dei nodi riservati .....	717
Nodi riservati e fatturazione consolidata .....	718
Esempi di nodi riservati .....	718
Acquisto di un'offerta di nodi riservati con la console .....	719
Aggiornamento dei nodi riservati con AWS CLI .....	720
Acquisto di un'offerta di nodi riservati tramite la AWS CLI e l'API Amazon Redshift .....	722
Sicurezza .....	723
Protezione dei dati .....	725
Crittografia dei dati .....	726
Tokenizzazione dei dati .....	744
Riservatezza del traffico Internet .....	745
Gestione dell'identità e degli accessi .....	746
Autenticazione con identità .....	746
Controllo accessi .....	750

Panoramica sulla gestione degli accessi .....	750
Utilizzo di policy basate su identità (policy IAM) .....	757
Native identity provider (IdP) federation for Amazon Redshift (Federazione di provider di identità nativi (IdP) per Amazon Redshift) .....	814
Connessione di Redshift al Centro identità IAM per offrire agli utenti un'esperienza di autenticazione unica .....	818
Uso di ruoli collegati ai servizi .....	837
Utilizzo dell'autenticazione IAM per generare credenziali utente di database .....	843
Autorizzazione di Amazon Redshift ad accedere ai servizi AWS .....	901
Gestione delle password di amministrazione di Amazon Redshift tramite AWS Secrets Manager .....	937
Autorizzazioni necessarie per l'integrazione AWS Secrets Manager .....	937
Rotazione del segreto della password dell'amministratore .....	938
Recupero del nome della risorsa Amazon (ARN) del segreto in Amazon Redshift .....	939
Creazione di un segreto per le credenziali di connessione al database .....	939
Considerazioni sull'utilizzo AWS Secrets Manager con Amazon Redshift .....	943
Registrazione e monitoraggio .....	943
Logging di controllo dei database .....	944
Registrazione con CloudTrail .....	956
Convalida della conformità .....	968
Resilienza .....	969
Sicurezza dell'infrastruttura .....	970
Isolamento di rete .....	745
Gruppi di sicurezza .....	972
Connessione a utilizzando un endpoint VPC di interfaccia .....	972
Analisi della configurazione e delle vulnerabilità .....	978
Attività di rete .....	979
Utilizzo di un nome di dominio personalizzato per le connessioni client .....	979
Sicurezza per un nome di dominio personalizzato .....	980
Configurazione di un nome di dominio personalizzato .....	980
Utilizzo degli endpoint VPC gestiti da RedShift .....	988
Considerazioni .....	989
Gestione degli endpoint tramite la console Redshift .....	990
Gestione tramite AWS CLI .....	992
Gestione tramite le operazioni API Amazon Redshift .....	992
Gestione tramite AWS CloudFormation .....	993

Routing VPC avanzato .....	993
Uso di endpoint VPC .....	995
Routing VPC avanzato .....	996
Redshift Spectrum e il routing VPC avanzato .....	998
Monitoraggio delle prestazioni dei cluster .....	1003
Panoramica .....	1003
Dati di prestazioni .....	1004
Parametri di Amazon Redshift .....	1005
Dimensioni per i parametri di Amazon Redshift .....	1016
Dati di prestazioni di query e caricamento di Amazon Redshift .....	1019
Utilizzo dei dati di prestazioni .....	1020
Visualizzazione di dati di prestazioni dei cluster .....	1021
Visualizzazione dei dati della cronologia delle query .....	1030
Visualizzazione dei dati delle prestazioni dei database .....	1034
Visualizzazione dei dati relativi alla simultaneità del carico di lavoro e al dimensionamento simultaneo .....	1037
Visualizzazione di query e caricamenti .....	1039
Visualizzazione dei parametri del cluster durante le operazioni di caricamento .....	1044
Analisi delle prestazioni del carico di lavoro .....	1045
Gestione degli allarmi .....	1047
Utilizzo delle metriche delle prestazioni nella console CloudWatch .....	1048
Eventi .....	1050
Panoramica degli eventi del cluster .....	1050
Utilizzo di Amazon Simple Notification Service .....	1051
Sottoscrizione alle notifiche degli eventi del cluster di Amazon Redshift .....	1052
Visualizzazione degli eventi del cluster mediante la console .....	1054
Visualizzazione degli eventi del cluster utilizzando AWS CLI l'API Amazon Redshift .....	1054
Gestione delle notifiche degli eventi del cluster .....	1054
Gestione delle notifiche degli eventi del cluster mediante la console Amazon Redshift .....	1055
Gestione delle notifiche degli eventi del cluster utilizzando AWS CLI l'API Amazon Redshift .....	1055
Notifiche di eventi Amazon Redshift .....	1056
Categorie di eventi Amazon Redshift e messaggi di evento .....	1056
Notifiche di eventi Serverless di Amazon Redshift con Amazon EventBridge .....	1078
Notifiche di eventi di integrazione zero-ETL con Amazon EventBridge .....	1085
Quote e limiti .....	1094

Quote per gli oggetti Amazon Redshift .....	1094
Quote per gli oggetti Amazon Redshift Serverless .....	1102
Quote per l'API di dati Amazon Redshift .....	1104
Quote per gli oggetti dell'editor di query v2 .....	1106
Quote e limiti per oggetti Amazon Redshift Spectrum .....	1108
Vincoli per la denominazione .....	1109
Assegnazione di tag .....	1113
Panoramica del tagging .....	1113
Requisiti per il tagging .....	1114
Gestione di tag delle risorse tramite la console .....	1115
Gestione dei tag tramite l'API di Amazon Redshift .....	1115
Versioni dei cluster .....	1117
Patch 181 .....	1117
Nuove funzionalità .....	1118
Patch 180 .....	1119
Nuove funzionalità .....	1120
Patch 179 .....	1121
Nuove funzionalità .....	1122
Patch 178 .....	1123
Nuove funzionalità .....	1124
Patch 177 .....	1126
Nuove funzionalità .....	1127
Patch 176 .....	1128
Nuove funzionalità .....	1129
Patch 175 .....	1130
Nuove funzionalità .....	1131
Patch 174 .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Nuove funzionalità in questa versione .....	1131
Patch 173 .....	1132
Nuove funzionalità in questa versione .....	1132

Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Nuove funzionalità in questa versione .....	1132
Patch 172 .....	1134
Nuove funzionalità .....	1134
Patch 171 .....	1135
Nuove funzionalità .....	1135
Patch 170 .....	1135
Nuove funzionalità .....	1136
Patch 169 .....	1136
Nuove funzionalità .....	1136
Patch 168 .....	1136
Nuove funzionalità .....	1137
Esempi di codice .....	1138
Azioni .....	1141
CreateCluster .....	1142
CreateTable .....	1148
DeleteCluster .....	1151
DescribeClusters .....	1156
DescribeStatement .....	1163
GetStatementResult .....	1165
Insert .....	1168
ModifyCluster .....	1170
Query .....	1174
Scenari .....	1176
Inizia a usare Amazon Redshift .....	1176
Esempi di servizi incrociati .....	1203
Creazione di un'applicazione Web per tracciare i dati Amazon Redshift .....	1203
Cronologia dei documenti .....	1205
.....	mccxxxiv

# Cos'è Amazon Redshift?

Benvenuto nella Guida alla gestione di Amazon Redshift. Amazon Redshift è un servizio di data warehouse nel cloud in scala petabyte interamente gestito. Amazon Redshift serverless consente di accedere e analizzare i dati senza le configurazioni di un data warehouse con provisioning. Viene eseguito automaticamente il provisioning delle risorse e la capacità del data warehouse viene dimensionata in modo intelligente per fornire prestazioni rapide per carichi di lavoro maggiormente impegnativi e imprevedibili. Quando il data warehouse è inattivo non vengono addebitati costi, si paga solo l'utilizzo. Puoi caricare i dati e iniziare subito a eseguire query nell'editor di query Amazon Redshift v2 o nello strumento di business intelligence (BI) preferito. Goditi il miglior rapporto prezzo/prestazioni e le familiari funzionalità SQL in un easy-to-use ambiente senza amministrazione.

Indipendentemente dalle dimensioni del set di dati, Amazon Redshift offre prestazioni di query veloci tramite le stesse applicazioni di business intelligence e gli stessi strumenti basati su SQL utilizzati correntemente.

## È la prima volta che utilizzi Amazon Redshift?

Se Amazon Redshift viene utilizzato per la prima volta, consigliamo di iniziare leggendo le seguenti sezioni:

- [Punti salienti del servizio e prezzi](#): questa pagina di dettaglio del prodotto fornisce la proposta di valore, i punti salienti del servizio e i prezzi di Amazon Redshift.
- [Guida introduttiva ad Amazon Redshift serverless](#): questo argomento illustra il processo di configurazione di un data warehouse serverless, creazione di risorse e query su dati di esempio.
- [Guida per gli sviluppatori di database di Amazon Redshift](#): dedicata agli sviluppatori di database, questa guida spiega come progettare, creare, sottoporre a query e gestire i database che costituiscono il data warehouse.

Se preferisci gestire le risorse Amazon Redshift manualmente, puoi creare cluster con provisioning per le tue esigenze di query sui dati. Per ulteriori informazioni, consultare [Cluster Amazon Redshift](#).

In qualità di sviluppatore di applicazioni, puoi utilizzare l'API Amazon Redshift o le librerie AWS Software Development Kit (SDK) per gestire i cluster a livello di codice. Se utilizzi l'API Amazon Redshift, devi autenticare ogni richiesta HTTP o HTTPS nell'API firmandola. Per ulteriori informazioni sulla firma delle richieste, consultare [Firma di una richiesta HTTP](#).

Per informazioni sulla CLI, sull'API e sugli SDK, consultare le pagine Web seguenti:

- [Documentazione di riferimento delle API di Amazon Redshift serverless](#)
- [Documentazione di riferimento dell'API Amazon Redshift](#)
- [Documentazione di riferimento dell'API dati Amazon Redshift](#)
- [AWS CLI Riferimento ai comandi](#)
- Informazioni di riferimento sugli SDK in [Strumenti per Amazon Web Services](#).

## Panoramica delle funzionalità di Amazon Redshift Serverless

La maggior parte delle funzionalità supportate da un data warehouse con provisioning Amazon Redshift è supportata anche su Amazon Redshift Serverless. Di seguito sono elencate alcune delle sue funzionalità chiave.

Funzionalità	Descrizione
Snapshot	È possibile ripristinare uno snapshot di Amazon Redshift Serverless o di un data warehouse con provisioning su Amazon Redshift Serverless. Per ulteriori informazioni, consulta <a href="#">Utilizzo di snapshot e punti di ripristino</a> .
Punti di ripristino	Amazon Redshift Serverless crea automaticamente un punto di ripristino ogni 30 minuti. Questi punti di ripristino vengono conservati per 24 ore. È possibile utilizzarli per ripristinare dopo scritture o eliminazioni accidentali. Quando si ripristina da un punto di ripristino, tutti i dati nel database di Amazon Redshift Serverless vengono ripristinati a un punto nel tempo precedente. È inoltre possibile creare uno snapshot da un punto di ripristino se è necessario mantenerli o per un periodo più lungo. Per ulteriori informazioni, consulta <a href="#">Utilizzo di snapshot e punti di ripristino</a> .
Capacità RPU di base	Puoi impostare una capacità di base in Redshift Processing Unit (RPU). Una RPU fornisce 16 GB di memoria. Questa impostazione consente di controllare l'equilibrio tra risorse in uso e costi per il carico di lavoro. È possibile aumentare questo valore per aumentare le risorse disponibili e migliorare le prestazioni delle query o ridurre il valore per limitare la spesa. Il valore predefinito è 128 RPU. Per controllare i costi, è inoltre possibile impostare limiti di utilizzo, come le RPU

Funzionalità	Descrizione
	utilizzate al giorno. Per ulteriori informazioni, consulta <a href="#">Fatturazione per Amazon Redshift Serverless</a> .
Limiti di utilizzo della condivisione dei dati	Puoi limitare la quantità di dati trasferiti da una regione producer a una regione consumer usando la console o l'API. Questi costi di trasferimento dei dati sono diversi e vengono misurati in terabyte. Regione AWS Per ulteriori informazioni sulla condivisione dei dati, consulta <a href="#">Nozioni di base sulla condivisione dei dati tramite la console</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Funzioni definite dall'utente (FDU)	Puoi eseguire funzioni definite dall'utente (UDF) su Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Creazione funzioni definite dall'utente</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Stored procedure	Puoi eseguire stored procedure in Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Creazione di procedure archiviate</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Viste materializzate	Puoi creare viste materializzate in Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Creazione di viste materializzate</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Funzioni spaziali	Puoi eseguire funzioni spaziali in Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Query su dati spaziali</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Query federate	Puoi eseguire query per unire i dati con il cluster Aurora DB e i database Amazon RDS da Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Esecuzione di query su dati con query federate</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Query sui data lake	Puoi eseguire query per unire i dati dal tuo data lake Amazon S3 con Amazon Redshift Serverless. Per ulteriori informazioni, consulta <a href="#">Esecuzione di query in un data lake</a> nella Guida alla gestione di Amazon Redshift.

Funzionalità	Descrizione
HyperLogR egistro	Puoi eseguire HyperLogLog funzioni in Amazon Redshift Serverless. Per ulteriori informazioni, consulta <a href="#">HyperLogLogUsing sketches</a> nella Amazon Redshift Database Developer Guide.
Esecuzioni e di query sui dati tra database	Puoi eseguire query sui dati tra database con Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Esecuzione di query sui dati tra database</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Condivisione dei dati	Puoi accedere alle unità di condivisione dati sui data warehouse con provisioning con Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Condivisione dei dati tra cluster</a> nella Guida per gli sviluppatori di database di Amazon Redshift.
Query sui dati semistrutturati	Puoi importare e archiviare dati semistrutturati con il tipo di dati SUPER con Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Importazione ed esecuzione di query su dati semistrutturati</a> nella Guida per sviluppatori di database Amazon Redshift.
Tagging di risorse	Puoi utilizzare l'API Serverless di Amazon Redshift AWS CLI o l'API Amazon Redshift per etichettare le risorse con i metadati relativi alla risorsa. Per ulteriori informazioni, consulta l'articolo relativo all' <a href="#">Assegnazione di tag alle risorse</a> .
Machine learning	Puoi utilizzare le funzionalità di machine learning di Amazon Redshift con Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Utilizzo di machine learning</a> nella Guida per sviluppatori di database Amazon Redshift.
Comandi e funzioni SQL	Con alcune eccezioni (come ad esempio REBOOT_CLUSTER ), puoi utilizzare i comandi e le funzioni SQL di Amazon Redshift con Amazon Redshift Serverless. Per ulteriori informazioni, consultare <a href="#">Referenza SQL</a> nella Guida per gli sviluppatori di database di Amazon Redshift.

Funzionalità	Descrizione
CloudFormation risorse	Utilizzando CloudFormation i modelli, puoi distribuire e aggiornare le risorse Serverless di Amazon Redshift. Questa integrazione ti permette di dedicare meno tempo alla gestione delle risorse e concentrarti sulle tue applicazioni. Per ulteriori informazioni sulle CloudFormation risorse in Amazon Redshift Serverless, consulta il riferimento ai tipi di risorse <a href="#">Amazon Redshift Serverless</a> .
CloudTrail risorse	Amazon Redshift Serverless è integrato con AWS CloudTrail per fornire un registro delle azioni intraprese in Amazon Redshift Serverless. CloudTrail acquisisce tutte le chiamate API per Amazon Redshift Serverless come eventi. Per ulteriori informazioni, consulta <a href="#">CloudTrail Amazon Redshift Serverless</a> .

## Panoramica sui cluster con provisioning di Amazon Redshift

Il servizio Amazon Redshift gestisce tutte le attività di configurazione, esecuzione e dimensionamento di un data warehouse. Queste attività includono il provisioning della capacità, il monitoraggio e il backup del cluster e l'applicazione di patch e aggiornamenti al motore di Amazon Redshift.

Il video seguente mostra come creare un cluster ed eseguire le query sui dati utilizzando l'Editor di query Amazon Redshift v2.

### Gestione dei cluster

Un cluster Amazon Redshift è un set di nodi costituito da un nodo principale e da uno o più nodi di calcolo. Il tipo e il numero di nodi di calcolo necessari dipendono dalle dimensioni dei dati, dal numero di query che saranno eseguite e dalle prestazioni di runtime delle query necessarie.

### Creazione e gestione di cluster

A seconda delle esigenze di data warehousing, puoi iniziare con un piccolo cluster a nodo singolo per poi aumentarne la capacità fino a ottenere un cluster a più nodi più grande in base al mutare dei requisiti. Puoi aggiungere o rimuovere nodi di calcolo nel cluster senza alcuna interruzione del servizio. Per ulteriori informazioni, consultare [Cluster con provisioning di Amazon Redshift](#).

### Prenotazione di nodi di calcolo

Se intendi mantenere il cluster in esecuzione per un anno o più, puoi risparmiare sui costi prenotando nodi di calcolo per un periodo di un anno o di tre anni. La prenotazione di nodi di calcolo assicura

risparmi significativi rispetto alle tariffe orarie dovute per il provisioning di nodi di calcolo on demand. Per ulteriori informazioni, consultare [Acquisto di nodi riservati di Amazon Redshift](#).

## Creazione di snapshot di cluster

Le istantanee sono point-in-time backup di un cluster. Esistono due tipi di snapshot: automatici e manuali. Amazon Redshift archivia questi snapshot internamente in Amazon Simple Storage Service (Amazon S3) utilizzando una connessione Secure Sockets Layer (SSL) crittografata. Se è necessario eseguire un ripristino da uno snapshot, Amazon Redshift crea un nuovo cluster e importa i dati dallo snapshot specificato. Per ulteriori informazioni sugli snapshot, consulta [Snapshot e backup di Amazon Redshift](#).

## Sicurezza e accesso ai cluster

Amazon Redshift offre diverse caratteristiche correlate all'accesso ai cluster e alla sicurezza. Queste caratteristiche ti aiutano a controllare l'accesso ai cluster, definire regole di connettività e crittografare dati e connessioni. Si tratta di caratteristiche aggiuntive rispetto a quelle correlate all'accesso ai database e alla loro sicurezza in Amazon Redshift. Per ulteriori informazioni sulla sicurezza dei database, consultare [Gestione della sicurezza dei database](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## AWS account e credenziali IAM

Per impostazione predefinita, un cluster Amazon Redshift è accessibile solo all' AWS account che lo crea. Il cluster è bloccato in modo che nessun altro possa accedervi. All'interno del tuo AWS account, utilizzi il servizio AWS Identity and Access Management (IAM) per creare account utente e gestire le autorizzazioni di tali account per controllare le operazioni del cluster. Per ulteriori informazioni, consulta [Sicurezza di Amazon Redshift](#). Per ulteriori informazioni sulla gestione delle identità IAM, comprese le linee guida e le best practice per i ruoli IAM, consulta [Identity and Access Management in Amazon Redshift](#).

## Gruppi di sicurezza

Per impostazione predefinita, qualsiasi cluster creato è chiuso a tutti. Le credenziali IAM controllano l'accesso solo alle risorse correlate all'API Amazon Redshift, ovvero la console Amazon Redshift, l'interfaccia a riga di comando (CLI), l'API e l'SDK. Per abilitare l'accesso al cluster da strumenti client SQL tramite JDBC o ODBC, devi usare gruppi di sicurezza:

- Se si utilizza la piattaforma EC2-VPC per il cluster Amazon Redshift, è necessario usare gruppi di sicurezza VPC. È consigliabile lanciare il cluster in una piattaforma EC2-VPC.

Non è possibile spostare un cluster in un VPC dopo che è stato lanciato con EC2-Classic. Tuttavia, è possibile ripristinare uno snapshot EC2-Classic in un cluster EC2-VPC usando la console Amazon Redshift. Per ulteriori informazioni, consultare [Ripristino di un cluster da uno snapshot](#).

- Se si utilizza la piattaforma EC2-Classic per il cluster Amazon Redshift, è necessario usare i gruppi di sicurezza di Amazon Redshift.

In entrambi i casi, è necessario aggiungere regole al gruppo di sicurezza per concedere accesso in ingresso esplicito a un intervallo specifico di indirizzi CIDR/IP o a un gruppo di sicurezza Amazon Elastic Compute Cloud (Amazon EC2) se il client SQL è in esecuzione in un'istanza Amazon EC2. Per ulteriori informazioni, consultare [Gruppi di sicurezza dei cluster Amazon Redshift](#).

Oltre alle regole di accesso in ingresso, devi creare utenti di database per fornire credenziali per l'autenticazione al database all'interno del cluster stesso. Per ulteriori informazioni, consultare [Database](#) in questo argomento.

## Crittografia

Quando effettui il provisioning del cluster, puoi facoltativamente scegliere di crittografarlo per un ulteriore livello di sicurezza. Quando si abilita la crittografia, Amazon Redshift archivia tutti i dati in tabelle create dall'utente usando un formato crittografato. È possibile utilizzare AWS Key Management Service (AWS KMS) per gestire le chiavi di crittografia di Amazon Redshift.

La crittografia è una proprietà immutabile del cluster. L'unico modo di modificare un cluster crittografato in cluster non crittografato consiste nello scaricare i dati e ricaricarli in un nuovo cluster. La crittografia viene applicata al cluster e a tutti i backup. Quando ripristini un cluster da uno snapshot crittografato, viene crittografato anche il nuovo cluster.

Per ulteriori informazioni sulle chiavi di crittografia e sui moduli di sicurezza hardware, consultare [Crittografia dei database di Amazon Redshift](#).

## Connessioni SSL

Puoi usare la crittografia Secure Sockets Layer (SSL) per crittografare la connessione tra il client SQL e il cluster. Per ulteriori informazioni, consultare [Configurazione delle opzioni di sicurezza per le connessioni](#).

## Monitoraggio dei cluster

Amazon Redshift offre diverse caratteristiche correlate al monitoraggio. Puoi utilizzare il logging di controllo dei database per generare log di attività, configurare eventi e sottoscrizioni di notifiche per tenere traccia delle informazioni che più interessano. Utilizza le metriche di Amazon Redshift e CloudWatch Amazon per conoscere lo stato e le prestazioni dei tuoi cluster e database.

### Logging di controllo dei database

Puoi usare la caratteristica di logging di controllo dei database per tenere traccia delle informazioni su tentativi di autenticazione, connessioni, disconnessioni, modifiche apportate alle definizioni degli utenti di database e query eseguite nel database. Queste informazioni sono utili per scopi di sicurezza e risoluzione dei problemi in Amazon Redshift. I log vengono archiviati in bucket Amazon S3. Per ulteriori informazioni, consultare [Logging di controllo dei database](#).

### Eventi e notifiche

Amazon Redshift tiene traccia degli eventi e conserva le informazioni su di essi per un periodo di diverse settimane nel tuo account. AWS Per ogni evento, Amazon Redshift fornisce informazioni come la data in cui si è verificato, una descrizione, l'origine (ad esempio un cluster, un gruppo di parametri o uno snapshot) e l'ID di origine. È possibile creare abbonamenti a notifiche di eventi di Amazon Redshift che specificano un set di filtri di evento. Quando si verifica un evento che corrisponde alle opzioni di filtro, Amazon Redshift utilizza Amazon Simple Notification Service per informare del verificarsi dell'evento. Per ulteriori informazioni su eventi e notifiche, consultare [Eventi di Amazon Redshift](#).

### Prestazioni

Amazon Redshift fornisce parametri e dati di prestazioni in modo che sia possibile monitorare l'integrità e le prestazioni di database e cluster. Amazon Redshift utilizza i CloudWatch parametri di Amazon per monitorare gli aspetti fisici del cluster, come l'utilizzo della CPU, la latenza e il throughput. Amazon Redshift fornisce inoltre dati sulle prestazioni di query e caricamento per monitorare l'attività del database nel cluster. Per ulteriori informazioni sui parametri e sul monitoraggio delle prestazioni, consultare [Monitoraggio delle prestazioni del cluster Amazon Redshift](#).

### Database

Amazon Redshift crea un database quando si effettua il provisioning di un cluster. Questo è il database che verrà utilizzato per caricare dati ed eseguire query sui dati. Puoi creare altri database in base alle esigenze eseguendo un comando SQL. Per ulteriori informazioni sulla creazione di altri

database, consultare [Fase 1: Creazione di un database](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Quando effettui il provisioning di un cluster, devi specificare un utente amministratore che ha accesso a tutti i database creati all'interno del cluster. Questo utente amministratore è un utente con privilegi avanzati, che è l'unico utente che inizialmente può accedere al database, ma può creare altri utenti con privilegi avanzati e utenti. Per ulteriori informazioni, consultare [Utenti con privilegi avanzati](#) e [Utenti](#) nella Guida per sviluppatori di database di Amazon Redshift.

Amazon Redshift usa gruppi di parametri per definire il comportamento di tutti i database in un cluster, ad esempio lo stile di presentazione delle date e la precisione dei valori a virgola mobile. Se non si specifica un gruppo di parametri quando si effettua il provisioning del cluster, Amazon Redshift associa un gruppo di parametri predefinito al cluster. Per ulteriori informazioni, consultare [Gruppi di parametri di Amazon Redshift](#).

Per ulteriori informazioni sui database in Amazon Redshift, consultare la [Guida per gli sviluppatori di database di Amazon Redshift](#).

## Confronto di Amazon Redshift Serverless con un data warehouse con provisioning di Amazon Redshift

Per Amazon Redshift Serverless, alcuni concetti e caratteristiche sono diversi dalle funzionalità corrispondenti relative ai data warehouse con provisioning di Amazon Redshift. Ad esempio, rispetto ad Amazon Redshift, in Amazon Redshift Serverless non è previsto il concetto di cluster o nodo. La tabella seguente descrive le caratteristiche e il comportamento di Amazon Redshift Serverless e ne spiega la differenza rispetto alla funzionalità corrispondente in un data warehouse con provisioning.

Funzionalità	Descrizione	Serverless	Assegnata
Gruppo di lavoro e spazio dei nomi	Per isolare i carichi di lavoro e gestire diverse risorse in Amazon	Uno spazio dei nomi è una raccolta di oggetti di database e utenti.	Un cluster con provisioning è una raccolta di nodi di calcolo e un nodo leader, che vengono gestiti direttamente. Per ulteriori informazioni, consulta <a href="#">Cluster con provisioning di Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
	Redshift Serverless, puoi creare spazi dei nomi e gruppi di lavoro per gestire separatamente le risorse di archiviazione e calcolo.	Un gruppo di lavoro è una raccolta di risorse di calcolo. Per ulteriori informazioni, consulta la pagina <a href="#">Amazon Redshift Serverless</a> per ulteriori informazioni sulla struttura di Amazon Redshift Serverless.	

Funzionalità	Descrizione	Serverless	Assegnata
Tipi di nodo	Quando utilizzi Amazon Redshift Serverless, non devi scegliere i tipi di nodi né specificare il conteggio dei nodi come fai con un cluster Amazon Redshift con provisioning.	Amazon Redshift Serverless effettua automaticamente il provisioning e la gestione della capacità per te. Facoltativamente, è possibile specificare la capacità del data warehouse di base per selezionare il giusto bilanciamento prezzo/prestazioni per i carichi di lavoro. È inoltre possibile specificare il numero massimo	Crea un cluster con i tipi di nodi che soddisfano le tue specifiche di costi e prestazioni. Per ulteriori informazioni, consulta <a href="#">Cluster con provisioning di Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
		di ore RPU per impostare controlli sui costi in modo da garantirne la prevedibilità. Per ulteriori informazioni, consulta <a href="#">Conoscere la capacità di Amazon Redshift Serverless</a> .	

Funzionalità	Descrizione	Serverless	Assegnata
Gestione del carico di lavoro e dimensionamento simultaneo	Amazon Redshift è dimensionabile per periodi di carico elevato. Amazon Redshift Serverless è inoltre dimensionabile per soddisfare periodi di carico elevato non continui.	Amazon Redshift Serverless gestisce automaticamente le risorse in modo efficiente e scalabile, in base ai carichi di lavoro, entro le soglie dei controlli dei costi. Per ulteriori informazioni, consulta <a href="#">Fatturazione per la capacità di calcolo</a> .	Con un data warehouse con provisioning, è possibile abilitare il dimensionamento simultaneo sul cluster per gestire i periodi di carico elevato. Per ulteriori informazioni sul dimensionamento simultaneo, consulta <a href="#">Utilizzo del dimensionamento della simultaneità</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Porta	Il numero di porta utilizzato per la connessione.	Con Amazon Redshift serverless, puoi passare a un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215. Per ulteriori informazioni, consulta <a href="#">Connessione ad Amazon Redshift Serverless</a> .	Con un data warehouse con provisioning, puoi scegliere qualsiasi porta da connettere.

Funzionalità	Descrizione	Serverless	Assegnata
Riridimensionamento	Aggiungi o rimuovi risorse di calcolo per ottimizzare le prestazioni del carico di lavoro.	Il ridimensionamento non è applicabile in Amazon Redshift Serverless. Tuttavia, è possibile modificare la capacità RPU del data warehouse di base, in base ai requisiti di prezzo e prestazioni. Per ulteriori informazioni, consulta <a href="#">Conoscere la capacità di Amazon Redshift Serverless</a> .	Con un cluster con provisioning, esegui un ridimensionamento del cluster per aggiungere o rimuovere nodi. Per ulteriori informazioni, consulta <a href="#">Panoramica della gestione dei cluster in Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Sospensione e ripristino	Puoi sospendere e un cluster con provisioning quando non hai carichi di lavoro da eseguire, per risparmiare sui costi.	Con Amazon Redshift Serverless, paghi solo quando vengono eseguite le query, quindi non è necessario sospendere o ripristinare l'esecuzione. Per ulteriori informazioni, consulta <a href="#">Fatturazione per la capacità di calcolo</a> .	Con un cluster con provisioning, è possibile sospendere e ripristinare un cluster manualmente, in base a una valutazione del carico di lavoro in vari momenti. Per ulteriori informazioni, consulta <a href="#">Panoramica della gestione dei cluster in Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Esecuzione di query su dati esterni mediante query Spectrum	Puoi eseguire query sui dati nei bucket Amazon S3, in una varietà di formati, come JSON.	La fatturazione viene calcolata quando le risorse di calcolo elaborano i carichi di lavoro. La fatturazione viene inoltre calcolata quando vengono eseguite query sui dati esterni di Redshift Spectrum, come qualsiasi altra transazione. Per ulteriori informazioni, consulta <a href="#">Fatturazione per la capacità di calcolo</a> .	Con un data warehouse con provisioning, la capacità di Amazon Redshift Spectrum è disponibile sui vari server sottoposti a query dal cluster Amazon Redshift. Per ulteriori informazioni, consulta <a href="#">Esecuzione di query su dati esterni mediante query Amazon Redshift Spectrum</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Fatturazione delle risorse di calcolo	Calcolato della fatturazione in Amazon Redshift e in Amazon Redshift Serverless.	Con Amazon Redshift Serverless, paghi i carichi di lavoro eseguiti, in ore RPU al secondo, con un costo minimo di 60 secondi. Ciò include le query che accedono ai dati nei formati di file aperti in Amazon S3. Per ulteriori informazioni, consulta <a href="#">Fatturazione per la capacità di calcolo</a> .	Con un cluster con provisioning, la fatturazione viene calcolata al secondo quando il cluster non è in pausa.

Funzionalità	Descrizione	Serverless	Assegnata
Maintenance window (Finestra di manutenzione)	Funzionamento della manutenzione del server.	Non esiste una finestra di manutenzione con Amazon Redshift Serverless. Gli aggiornamenti vengono gestiti in modo ottimale. Per ulteriori informazioni, consulta <a href="#">Cos'è Amazon Redshift Serverless?</a>	Con un cluster con provisioning, è possibile specificare una finestra di manutenzione durante l'applicazione di patch. (In genere, si sceglie un tempo ricorrente quando l'uso è basso.)

Funzionalità	Descrizione	Serverless	Assegnata
Encryption (Crittografia)	È possibile abilitare la crittografia del database.	Amazon Redshift Serverless è sempre crittografato con AWS KMS, con chiavi AWS gestite o gestite dal cliente.	I dati in un data warehouse fornito possono essere crittografati con AWS KMS (con chiavi AWS gestite o gestite dal cliente) o non crittografati. Per informazioni, consulta <a href="#">Crittografia dei database di Amazon Redshift</a> .
Fatturazione dello spazio di archiviazione	Funzionamento della fatturazione dello spazio di archiviazione.	Per Amazon Redshift Serverless. La tariffa viene calcolata in base ai GB al mese. Per informazioni, consulta <a href="#">Fatturazione per la capacità di calcolo</a> .	Lo spazio di archiviazione viene fatturato a parte rispetto alle risorse di calcolo per un cluster con provisioning con nodi RA3.

Funzionalità	Descrizione	Serverless	Assegnata
Gestione degli utenti	Gestione degli utenti.	<p>Per Amazon Redshift Serverless, gli utenti sono utenti IAM o Redshift. Per ulteriori informazioni, consulta <a href="#">Identity and Access Management in Amazon Redshift Serverless</a>.</p> <p>Per ulteriori informazioni sulla gestione delle identità IAM, comprese le best practice per i ruoli IAM, consulta</p>	<p>Per un data warehouse fornito, gli utenti sono utenti IAM o Redshift. Per ulteriori informazioni, consulta <a href="#">Managing database security</a> nella Amazon Redshift Database Developer Guide.</p> <p>Per ulteriori informazioni sulla gestione delle identità IAM, comprese le best practice per i ruoli IAM, consulta <a href="#">Identity and Access Management in Amazon Redshift</a>.</p>

Funzionalità	Descrizione	Serverless	Assegnata
		<a href="#">Identity and Access Management in Amazon Redshift.</a>	

Funzionalità	Descrizione	Serverless	Assegnata
Strumenti e compatibilità JDBC e ODBC	Funzionamento delle connessioni client.	Amazon Redshift Serverless è compatibile con qualsiasi strumento o applicazione client conforme a JDBC o ODBC. Per ulteriori informazioni sui driver, consulta <a href="#">Configurazione delle connessioni</a> nella Guida alla gestione di Amazon Redshift. Per informazioni sulla connessione ai cluster, consulta <a href="#">Connessione a un data warehouse Amazon Redshift utilizzando gli strumenti client SQL</a> .	Amazon Redshift provisioned è compatibile con qualsiasi strumento o applicazione client conforme a JDBC o ODBC. Per ulteriori informazioni sui driver, consulta <a href="#">Configurazione delle connessioni</a> nella Guida alla gestione di Amazon Redshift. Per informazioni sulla connessione ai cluster, consulta <a href="#">Connessione a un data warehouse Amazon Redshift utilizzando gli strumenti client SQL</a> .

Funzionalità	Descrizione	Serverless	Assegnata
		s, consulta <a href="#">Connessione a Redshift Serverless</a> .	
Requisiti per le credenziali all'accesso	Gestione delle credenziali.	Per Amazon Redshift Serverless, non è necessario inserire credenziali in ogni istanza. Per ulteriori informazioni, consulta <a href="#">Connessione ad Amazon Redshift Serverless</a> .	L'accesso ad Amazon Redshift richiede le credenziali di accesso di un utente associato a un ruolo IAM. Al ruolo IAM sono collegate autorizzazioni specifiche per un data warehouse allocato. Una volta autenticato, l'utente può connettersi direttamente al database, alla console di Redshift e all'editor di query v2.

Funzionalità	Descrizione	Serverless	Assegnata
Data API (API dati).	È possibile accedere ai dati da servizi Web e da altre applicazioni.	Amazon Redshift Serverless supporta l'API dati di Amazon Redshift. In Amazon Redshift Serverless utilizzi invece il parametro <code>workgroup-name</code> al posto del parametro <code>cluster-identity</code> . Per informazioni sulla chiamata dell'API dati, consultare <a href="#">Uso dell'API dati di Amazon Redshift</a> .	Amazon Redshift provisioned supporta l'API Amazon Redshift Data. Con i cluster Amazon Redshift, utilizzi il <code>cluster-identity</code> parametro anziché il parametro <code>.workgroup-name</code> . Per informazioni sulla chiamata dell'API dati, consultare <a href="#">Uso dell'API dati di Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Snapshot	Fornisce point-in-time il ripristino.	Amazon Redshift Serverless supporta snapshot e punti di ripristino. Per ulteriori informazioni sugli snapshot e i punti di ripristino per uno spazio dei nomi, consulta <a href="#">Utilizzo di snapshot e punti di ripristino</a> .	I cluster con provisioning supportano gli snapshot. Per ulteriori informazioni, consulta <a href="#">Gestione di snapshot tramite la console</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Condivisione dei dati	Consente di condividere dati tra database nello stesso account o in account diversi.	Amazon Redshift serverless supporta tutte le funzionalità di condivisione dei dati supportate dai data warehouse con provisioning. Supporta anche la condivisione dei dati tra Amazon Redshift serverless e un data warehouse con provisioning, uno strumento o un'applicazione client.	I cluster con provisioning supportano la condivisione di dati e AWS Data Exchange database, tra più account, tra diverse regioni. Per ulteriori informazioni, consulta <a href="#">Condivisione di dati tra cluster in Amazon Redshift</a> .

Funzionalità	Descrizione	Serverless	Assegnata
Tracce	Fornisce una pianificazione per gli aggiornamenti software.	Amazon Redshift Serverless non ha il concetto di traccia. Le versioni e gli aggiornamenti sono gestiti dal servizio. Per ulteriori informazioni sulla struttura di Amazon Redshift Serverless, consulta <a href="#">Utilizzo di snapshot e punti di ripristino</a> .	I cluster con provisioning supportano il passaggio tra le tracce correnti e finali.

Funzionalità	Descrizione	Serverless	Assegnata
Tabelle e viste di sistema	Consentono di monitorare le risorse e i metadati di sistema.	Amazon Redshift Serverless supporta nuove tabelle e visualizzazioni di sistema. Per ulteriori informazioni sulle tabelle di sistema, consultare <a href="#">Viste di monitoraggio</a> . Per informazioni su come migrare le query dall'utilizzo delle tabelle e delle viste di sistema con provisioning alle nuove viste,	Un data warehouse con provisioning supporta il set esistente di tabelle e viste di sistema per il monitoraggio del cluster e altre attività che richiedono metadati di sistema.

Funzionalità	Descrizione	Serverless	Assegnata
		consulta <a href="#">Migrazione alle viste di monitoraggio SYS.</a>	
Gruppi di parametri	Gruppo di parametri applicati a tutti i database creati in un cluster. Questi parametri configurano le impostazioni dei database, come timeout di query e stile delle date.	Amazon Redshift Serverless non ha il concetto di gruppo di parametri.	I data warehouse con provisioning supportano i gruppi di parametri. Per ulteriori informazioni sui gruppi di parametri per un cluster con provisioning, consulta <a href="#">Gruppi di parametri di Amazon Redshift.</a>

Funzionalità	Descrizione	Serverless	Assegnata
Monitoraggio delle query	Fornisce una visualizzazione temporale delle query eseguite.	Il monitoraggio delle query in Amazon Redshift Serverless richiede agli utenti di connettersi al database per utilizzare le tabelle di sistema. Pertanto, il monitoraggio delle query e le tabelle di sistema sono sincronizzate. Le query di tabelle di sistema per Amazon Redshift Serverless utilizzano	Il monitoraggio delle query nei cluster con provisioning non mostra tutti i dati nelle tabelle di sistema.

Funzionalità	Descrizione	Serverless	Assegnata
		l'utente del database mappato all'utente IAM per l'utilizzo del monitoraggio delle query. Per ulteriori informazioni sul monitoraggio delle query, consulta <a href="#">Monitoraggio di query e carichi di lavoro con Amazon Redshift Serverless</a> .	

Funzionalità	Descrizione	Serverless	Assegnata
Registrazione di controllo	Fornisce informazioni su connessioni e attività degli utenti nel database.	<p>Con Amazon Redshift Serverless, CloudWatch è una destinazione per i log di controllo. La consegna del registro di controllo basata su Amazon S3 non è supportata per Amazon Redshift Serverless. Per ulteriori informazioni consulta <a href="#">Registrazione di verifiche per Amazon Redshift Serverless</a>.</p>	Per un cluster con provisioning, la distribuzione dei registri di controllo basata su Amazon S3 è una prassi standard. Ora, la consegna dei log di controllo a CloudWatch è estesa ai data warehouse predisposti.

Funzionalità	Descrizione	Serverless	Assegnata
Notifiche eventi	Amazon EventBridge è un servizio di bus eventi senza server che puoi utilizzare e per connettere le tue applicazioni con dati sugli eventi provenienti da una varietà di fonti.	Amazon Redshift Serverless utilizza Amazon EventBridge per gestire le notifiche degli eventi per tenerti aggiornato o up-to-date sulle modifiche nel tuo data warehouse. Per ulteriori informazioni, consulta <a href="#">Notifiche di eventi Serverless di Amazon Redshift con Amazon EventBridge</a> .	Per un cluster con provisioning, puoi gestire le notifiche di eventi mediante la console Amazon Redshift in modo da creare sottoscrizioni alle notifiche. Per ulteriori informazioni, consulta <a href="#">Gestione delle notifiche degli eventi del cluster</a> .

# Utilizzo delle interfacce di gestione Amazon Redshift per i cluster predisposti

## Note

Questo argomento si concentra sulle interfacce di gestione di Amazon Redshift per i cluster predisposti. Esistono interfacce di gestione simili per Amazon Redshift Serverless e Amazon Redshift Data API.

Amazon Redshift supporta diverse interfacce di gestione che puoi utilizzare per creare, gestire ed eliminare i cluster Amazon Redshift: gli AWS SDK, la ()AWS CLI e l'API di gestione Amazon Redshift. AWS Command Line Interface

API Amazon Redshift: è possibile chiamare questa API di gestione Amazon Redshift inviando una richiesta. Sono richieste HTTP o HTTPS che utilizzano i verbi HTTP GET o POST con un parametro denominato `Action`. La chiamata dell'API Amazon Redshift è il modo più diretto di accedere al servizio Amazon Redshift. Richiede tuttavia che la propria applicazione gestisca dettagli di basso livello, come il controllo degli errori e la generazione di un hash per la firma della richiesta.

- Per informazioni sulla creazione e la firma di una richiesta API di Amazon Redshift, consultare [Firma di una richiesta HTTP](#).
- Per informazioni sulle operazioni API di Amazon Redshift e sui tipi di dati per Amazon Redshift, consultare [Documentazione di riferimento dell'API Amazon Redshift](#).

AWS SDK: puoi utilizzare gli AWS SDK per eseguire operazioni relative ai cluster Amazon Redshift. Molte delle librerie SDK eseguono il wrap dell'API Amazon Redshift sottostante. Queste integrano la funzionalità API nel linguaggio di programmazione specifico e gestiscono molti dettagli di basso livello, come il calcolo delle firme, la gestione dei tentativi di richiesta e la gestione degli errori. La chiamata delle funzioni wrapper nelle librerie SDK può semplificare notevolmente il processo di scrittura di un'applicazione per la gestione di un cluster Amazon Redshift.

- Amazon Redshift è supportato dagli AWS SDK per Java, .NET, PHP, Python, Ruby e Node.js. Le funzioni wrapper per Amazon Redshift sono documentate nel manuale di riferimento per ogni SDK. Per un elenco degli AWS SDK e i collegamenti alla relativa documentazione, consulta [Tools for Amazon Web Services](#).

- Questa guida fornisce esempi di utilizzo di Amazon Redshift mediante l'SDK Java. Per esempi di codice AWS SDK più generali, consulta [Esempi di codice per Amazon Redshift con SDK AWS](#)

AWS CLI— La CLI fornisce un set di strumenti da riga di comando che è possibile utilizzare per gestire AWS i servizi da computer Windows, Mac e Linux. La AWS CLI include comandi basati sulle operazioni API Amazon Redshift.

- Per informazioni sull'installazione e la configurazione della CLI di Amazon Redshift, consultare [Configurazione della CLI di Amazon Redshift](#).
- Per il materiale di riferimento sui comandi della CLI di Amazon Redshift, consultare [Amazon Redshift](#) in Riferimenti di AWS CLI

## Utilizzo di questo servizio con un SDK AWS

AWS I kit di sviluppo software (SDK) sono disponibili per molti linguaggi di programmazione più diffusi. Ogni SDK fornisce un'API, esempi di codice, e documentazione che facilitano agli sviluppatori la creazione di applicazioni nel loro linguaggio preferito.

Documentazione sugli SDK	Esempi di codice
<a href="#">AWS SDK for C++</a>	<a href="#">AWS SDK for C++ esempi di codice</a>
<a href="#">AWS CLI</a>	<a href="#">AWS CLI esempi di codice</a>
<a href="#">AWS SDK for Go</a>	<a href="#">AWS SDK for Go esempi di codice</a>
<a href="#">AWS SDK for Java</a>	<a href="#">AWS SDK for Java esempi di codice</a>
<a href="#">AWS SDK for JavaScript</a>	<a href="#">AWS SDK for JavaScript esempi di codice</a>
<a href="#">SDK AWS for Kotlin</a>	<a href="#">SDK AWS for Kotlin esempi di codice</a>
<a href="#">AWS SDK for .NET</a>	<a href="#">AWS SDK for .NET esempi di codice</a>
<a href="#">AWS SDK for PHP</a>	<a href="#">AWS SDK for PHP esempi di codice</a>
<a href="#">AWS Tools for PowerShell</a>	<a href="#">Strumenti per esempi di PowerShell codice</a>
<a href="#">AWS SDK for Python (Boto3)</a>	<a href="#">AWS SDK for Python (Boto3) esempi di codice</a>

Documentazione sugli SDK	Esempi di codice
<a href="#">AWS SDK for Ruby</a>	<a href="#">AWS SDK for Ruby esempi di codice</a>
<a href="#">AWS SDK for Rust</a>	<a href="#">AWS SDK for Rust esempi di codice</a>
<a href="#">SDK AWS per SAP ABAP</a>	<a href="#">SDK AWS per SAP ABAP esempi di codice</a>
<a href="#">SDK AWS per Swift</a>	<a href="#">SDK AWS per Swift esempi di codice</a>

### Esempio di disponibilità

Non riesci a trovare quello che ti serve? Richiedi un esempio di codice utilizzando il link [Provide feedback \(Fornisci un feedback\)](#) nella parte inferiore di questa pagina.

## Firma di una richiesta HTTP

Amazon Redshift richiede che ogni richiesta inviata all'API di gestione venga autenticata con una firma. In questo argomento viene illustrato come firmare le richieste.

Se utilizzi uno dei AWS Software Development Kit (SDK) o il AWS Command Line Interface, la firma delle richieste viene gestita automaticamente e puoi saltare questa sezione. Per ulteriori informazioni sull'utilizzo AWS degli SDK, consulta [Utilizzo delle interfacce di gestione Amazon Redshift per i cluster predisposti](#). Per ulteriori informazioni sull'uso dell'interfaccia a riga di comando di Amazon Redshift, consultare [Guida di riferimento alla riga di comando di Amazon Redshift](#).

Per firmare una richiesta, è necessario calcolare una firma digitale usando una funzione hash crittografica. Una funzione hash crittografica è una funzione che restituisce un valore hash univoco basato sull'input. L'input alla funzione hash include il testo della richiesta e la chiave di accesso segreta che puoi ottenere dalle credenziali temporanee. La funzione hash restituisce un valore hash che includi nella richiesta come firma. La firma è parte dell'intestazione Authorization della richiesta.

## Note

Gli utenti necessitano dell'accesso programmatico se desiderano interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface</a></li> <li>• Per AWS SDK, strumenti e AWS API, consulta <a href="#">l'autenticazione IAM Identity Center</a> nella Guida di riferimento agli AWS SDK e agli strumenti.</li> </ul>
IAM	Utilizza credenziali temporanee per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in <a href="#">Uso delle credenziali temporanee e con AWS risorse</a> nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Autenticazione tramite credenziali utente IAM nella Guida per l'utente</a>.AWS Command Line Interface</li> <li>• Per gli AWS SDK e gli strumenti, consulta <a href="#">Autenticazione tramite credenziali a lungo termine</a> nella Guida di riferimento agli SDK e agli AWS strumenti.</li> <li>• Per le AWS API, consulta <a href="#">Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM</a>.</li> </ul>

Dopo aver ricevuto la richiesta, Amazon Redshift ricalcola la firma usando la stessa funzione hash e lo stesso input che hai usato per firmare la richiesta. Se la firma risultante corrisponde a quella nella richiesta, Amazon Redshift elabora la richiesta. In caso contrario, la richiesta viene rifiutata.

Amazon Redshift supporta l'autenticazione con [AWS Signature Version 4](#). La procedura per il calcolo di una firma è composta da tre attività. Queste attività sono illustrate nell'esempio seguente.

- [Fase 1: creazione di una richiesta canonica](#)

Riorganizza la richiesta HTTP in un formato canonico. L'uso di un formato canonico è necessario perché Amazon Redshift utilizza lo stesso formato canonico per calcolare la firma da confrontare con quella che inviata.

- [Fase 2: creazione di una stringa di firma](#)

Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata stringa di firma, è una concatenazione del nome dell'algoritmo hash, della data della richiesta, di una stringa di ambito credenziali e della richiesta in formato canonico creata nella fase precedente. La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

- [Attività 3: calcolo di una firma](#)

Calcola una firma per la richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input, ovvero la stringa di firma e una chiave derivata. La chiave derivata viene calcolata a partire dalla chiave di accesso segreta e usando la stringa di ambito delle credenziali per creare una serie di codici di autenticazione dei messaggi basati su hash (HMAC-SHA256).

## Esempio di calcolo di firma

L'esempio seguente illustra i dettagli della creazione di una firma per la richiesta. [CreateCluster](#) Puoi usare questo esempio come riferimento per verificare il metodo di calcolo della firma usato. Altri calcoli di riferimento sono inclusi nella sezione [Richiesta di esempi di firma](#) della Guida per l'utente IAM.

Per inviare richieste ad Amazon Redshift è possibile utilizzare una richiesta GET o POST. La differenza tra le due opzioni è legata al fatto che per la richiesta GET i parametri vengono inviati come parametri della stringa di query. Per la richiesta POST sono invece inclusi nel corpo della richiesta. L'esempio seguente mostra una richiesta POST.

L'esempio presuppone quanto segue:

- Il time stamp della richiesta è `Fri, 07 Dec 2012 00:00:00 GMT`.
- L'endpoint è la regione Stati Uniti orientali (Virginia settentrionale), `us-east-1`.

La sintassi generale della richiesta è la seguente:

```
https://redshift.us-east-1.amazonaws.com/
```

```
?Action=CreateCluster
&ClusterIdentifier=examplecluster
&MasterUsername=masteruser
&MasterUserPassword=12345678Aa
&NumberOfNode=2
&NodeType=dc2.large
&Version=2012-12-01
&x-amz-algorithm=AWS4-HMAC-SHA256
&x-amz-credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request
&x-amz-date=20121207T000000Z
&x-amz-signedheaders=content-type;host;x-amz-date
```

Il formato canonico della richiesta calcolata per [Fase 1: creazione di una richiesta canonica](#) è:

```
POST
/

content-type:application/x-www-form-urlencoded; charset=utf-8
host:redshift.us-east-1.amazonaws.com
x-amz-date:20121207T000000Z

content-type;host;x-amz-date
55141b5d2aff6042ccd9d2af808fdf95ac78255e25b823d2dbd720226de1625d
```

L'ultima riga della richiesta canonica è l'hash del corpo della richiesta. La terza riga nella richiesta canonica è vuota perché non ci sono parametri di query per l'API.

La stringa di firma per [Fase 2: creazione di una stringa di firma](#) è:

```
AWS4-HMAC-SHA256
20121207T000000Z
20121207/us-east-1/redshift/aws4_request
06b6bef4f4f060a5558b60c627cc6c5b5b5a959b9902b5ac2187be80cbac0714
```

La prima riga della stringa di firma è l'algoritmo, la seconda è il timestamp, la terza è l'ambito credenziali e l'ultima è un hash del formato della richiesta canonica in [Fase 1: creazione di una richiesta canonica](#). Il nome del servizio da utilizzare nell'ambito credenziali è `redshift`.

In [Attività 3: calcolo di una firma](#), la chiave derivata può essere rappresentata come segue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey, "20121207"), "us-east-1"), "redshift"), "aws4_request")
```

La chiave derivata viene calcolata come una serie di funzioni hash. A partire dall'istruzione HMAC interna nella formula precedente, la frase **AWS4** viene concatenata con la chiave di accesso segreta e il risultato viene usato come chiave per l'hash dei dati "us-east-1". Il risultato dell'hash diventa la chiave per la funzione hash successiva.

Dopo aver calcolato la chiave derivata, puoi usarla in una funzione hash che accetta due stringhe di input, ovvero la stringa di firma e la chiave derivata. Ad esempio, se usi la chiave di accesso segreta `wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY` e la stringa di firma indicata in precedenza, la firma calcolata è analoga a quanto segue:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

La fase finale consiste nel creare l'intestazione `Authorization`. Per la chiave di accesso `AKIAIOSFODNN7EXAMPLE`, l'intestazione (con interruzioni di riga aggiunte per facilitare la lettura) è:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20121207/us-east-1/redshift/aws4_request,
SignedHeaders=content-type;host;x-amz-date,
Signature=9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

## Configurazione della CLI di Amazon Redshift

Questa sezione spiega come configurare ed eseguire gli strumenti da riga di AWS CLI comando da utilizzare nella gestione di Amazon Redshift. [Gli strumenti a riga di comando di Amazon Redshift vengono eseguiti su AWS Command Line Interface \(AWS CLI\), che a sua volta utilizza Python \(<https://www.python.org/>\)](#). AWS CLI Può essere eseguito su qualsiasi sistema operativo che supporti Python.

### Istruzioni di installazione

Per iniziare a utilizzare gli strumenti da riga di comando di Amazon Redshift, devi prima configurare e poi aggiungere i file di configurazione che definiscono le opzioni della CLI di Amazon Redshift. AWS CLI

Se lo hai già installato e configurato AWS CLI per un altro AWS servizio, puoi saltare questa procedura.

## Per installare AWS Command Line Interface

1. Vai a [Installa o aggiorna alla versione più recente di AWS CLI](#), quindi segui le istruzioni per l'installazione di AWS CLI.

Per l'accesso alla CLI, sono necessari un ID chiave di accesso e una chiave di accesso segreta. Utilizza credenziali temporanee al posto delle chiavi di accesso a lungo termine quando possibile. Le credenziali temporanee includono un ID della chiave di accesso, una chiave di accesso segreta e un token di sicurezza che ne indica la scadenza. Per ulteriori informazioni, consulta [Using temporary credentials with AWS resources](#) nella IAM User Guide.

2. Creare un file contenente informazioni di configurazione come le chiavi di accesso, la regione predefinita e il formato di output dei comandi. Impostare quindi la variabile di ambiente `AWS_CONFIG_FILE` per fare riferimento a quel file. Per istruzioni dettagliate, vai alla [sezione Configurazione dell'interfaccia a riga di AWS comando nella Guida](#) per l' AWS Command Line Interface utente.
3. Esegui un comando di test per confermare che l' AWS CLI interfaccia funziona. Ad esempio, il comando seguente deve visualizzare informazioni della Guida relative all' AWS CLI:

```
aws help
```

Il comando seguente deve visualizzare informazioni della Guida relative ad Amazon Redshift:

```
aws redshift help
```

[Per materiale di riferimento sui comandi CLI di Amazon Redshift, consulta Amazon Redshift nella pagina di riferimento.](#) AWS CLI

# Amazon Redshift Serverless

Amazon Redshift Serverless semplifica l'esecuzione e la scalabilità delle analisi senza dover eseguire il provisioning e la gestione dei data warehouse. Con Amazon Redshift Serverless, analisti di dati, sviluppatori e data scientist possono ora utilizzare Amazon Redshift per ottenere informazioni dettagliate dai dati in pochi secondi semplicemente caricando dati ed eseguendo query sui record nel data warehouse. Amazon Redshift esegue automaticamente il provisioning e la scalabilità della capacità del data warehouse per fornire prestazioni rapide per carichi di lavoro impegnativi e imprevedibili. Verrà effettuato l'addebito solo per la capacità utilizzata. È possibile trarre vantaggio da questa semplicità senza apportare modifiche alle applicazioni di analisi e business intelligence esistenti.

## Cos'è Amazon Redshift Serverless?

Amazon Redshift Serverless effettua automaticamente il provisioning della capacità del data warehouse e ridimensiona in modo intelligente le risorse sottostanti. Amazon Redshift Serverless regola la capacità in pochi secondi per offrire prestazioni costantemente elevate e operazioni semplificate anche per i carichi di lavoro più impegnativi e volatili.

Con Amazon Redshift Serverless, puoi beneficiare delle seguenti funzionalità:

- Accedi e analizza i dati senza la necessità di configurare, regolare e gestire i cluster con provisioning di Amazon Redshift.
- Utilizza le superiori funzionalità SQL di Amazon Redshift, le prestazioni leader del settore e l'integrazione data-lake per eseguire query senza problemi su un data warehouse, un data lake e origini dati operative.
- Offrire prestazioni costantemente elevate e operazioni semplificate anche per i carichi di lavoro più impegnativi e volatili con scalabilità intelligente e automatica.
- Utilizza gruppi di lavoro e spazi dei nomi per organizzare le risorse di calcolo e i dati con controlli granulari dei costi.
- Paga solo quando il data warehouse è in uso.

Con Amazon Redshift Serverless, utilizzi un'interfaccia di console per raggiungere un data warehouse serverless o API per creare applicazioni. Attraverso il data warehouse, puoi accedere allo storage gestito Amazon Redshift e al data lake Amazon S3.

Questo video mostra come Amazon Redshift Serverless semplifica l'esecuzione e la scalabilità delle analisi senza dover gestire l'infrastruttura del data warehouse.

## Console Serverless Amazon Redshift

Per informazioni su come iniziare a utilizzare la console Amazon Redshift serverless, guarda il video [Getting Started with Amazon Redshift serverless](#) (Nozioni di base su Amazon Redshift serverless).

### Pannello di controllo serverless

Sulla pagina Pannello di controllo Serverless, è possibile visualizzare un riepilogo delle risorse e dei grafici del tuo utilizzo.

- Namespace overview (Panoramica dello spazio dei nomi): questa sezione mostra la quantità di snapshot e unità di condivisione dati all'interno dello spazio dei nomi.
- Workgroups (Gruppi di lavoro): questa sezione mostra tutti i gruppi di lavoro di Amazon Redshift Serverless.
- metriche delle query: questa sezione mostra l'attività di query per l'ultima ora.
- Capacità RPU utilizzata – Questa sezione mostra la capacità utilizzata per l'ultima ora.
- Free trial (Prova gratuita): questa sezione mostra i crediti di prova gratuiti che rimangono nel tuo account AWS . Ciò copre tutto l'utilizzo delle risorse e delle operazioni di Amazon Redshift Serverless, inclusi snapshot, archiviazione, gruppo di lavoro e così via, con lo stesso account.
- Alarms (Allarmi): questa sezione mostra gli allarmi configurati in Amazon Redshift Serverless.

### Backup dei dati

Sulla scheda Backup dei dati puoi lavorare con quanto segue:

- Snapshot: è possibile creare, eliminare e gestire snapshot dei dati Amazon Redshift Serverless. Il periodo di conservazione predefinito è *indefinitely*, ma è possibile configurare il periodo di conservazione in modo che sia qualsiasi valore compreso tra 1 e 3653 giorni. È possibile Account AWS autorizzare il ripristino dei namespace da un'istantanea.
- Punti di ripristino – Visualizza i punti di ripristino creati automaticamente in modo da poter eseguire il ripristino da una scrittura o eliminazione accidentale nelle ultime 24 ore. Per recuperare i dati, è possibile ripristinare un punto di ripristino in qualsiasi spazio dei nomi disponibile. È possibile creare uno snapshot da un punto di ripristino se si desidera mantenere un punto di ripristino per

un periodo di tempo più lungo. Il periodo di conservazione predefinito è *indefinitely*, ma è possibile configurarlo in modo che sia qualsiasi valore compreso tra 1 e 3653 giorni.

## Accesso ai dati

Sulla scheda Accesso ai dati puoi lavorare con quanto segue:

- Impostazioni rete e sicurezza – È possibile visualizzare i valori relativi al VPC, i valori di crittografia AWS KMS e i valori di registrazione del controllo. È possibile aggiornare solo la registrazione di controllo. Per ulteriori informazioni sulle impostazioni di rete e di sicurezza sulla console, consulta [Gestione dei limiti di utilizzo, dei limiti delle query e di altre attività amministrative](#).
- AWS KMS key— AWS KMS key Utilizzato per crittografare le risorse in Amazon Redshift Serverless.
- Autorizzazioni – Puoi gestire i ruoli IAM che Amazon Redshift Serverless può assumere per utilizzare le risorse per tuo conto. Per ulteriori informazioni, consulta [Identity and Access Management in Amazon Redshift Serverless](#).
- Endpoint VPC gestiti da Redshift: è possibile accedere all'istanza Amazon Redshift Serverless da un altro VPC o sottorete. Per ulteriori informazioni, consulta [Connessione ad Amazon Redshift Serverless da altri endpoint VPC](#).

## Limiti

Sulla scheda Limiti puoi lavorare con quanto segue:

- Impostazioni Capacità di base nelle unità di elaborazione Redshift (RPU) – È possibile impostare la capacità di base utilizzata per elaborare il carico di lavoro. Per migliorare le prestazioni delle query, aumenta il valore RPU.
- Limiti di utilizzo: le risorse di calcolo massime che l'istanza Amazon Redshift Serverless può utilizzare in un periodo di tempo prima dell'avvio di un'azione. Limiti la quantità di risorse utilizzate da Amazon Redshift Serverless per eseguire il carico di lavoro. L'utilizzo viene misurato in ore Redshift Processing Units (RPU). Un'ora RPU è il numero di RPU utilizzati in un'ora. Puoi determinare l'azione da eseguire quando raggiungi il limite impostato, come segue:
  - Invia un avviso.
  - Registra una voce a una tabella di sistema.
  - Disattiva le query utente.

Puoi impostare fino a quattro limiti.

- Query limits (Limiti delle query): è possibile aggiungere un limite per monitorare prestazioni e limiti. Per ulteriori informazioni sui limiti di monitoraggio delle query, consulta [Regole di monitoraggio delle query WLM](#).

Per ulteriori informazioni, consulta [Conoscere la capacità di Amazon Redshift Serverless](#).

## Unità di condivisione dati

Sulla scheda Unità di condivisione dati puoi lavorare con quanto segue:

- Impostazioni Unità di condivisione dati creati nel mio spazio dei nomi – È possibile creare una unità di condivisione di dati e condividerla con altri spazi dei nomi e Account AWS.
- Datashare da altri namespace e Account AWS: puoi creare un database da un datashare da un altro namespace e Account AWS

Per ulteriori informazioni sulla condivisione dei dati, consultare [Condivisione dei dati in Amazon Redshift Serverless](#).

## Monitoraggio di query e database

Su Monitoraggio di query e database, è possibile visualizzare grafici di Cronologia query e Prestazioni del database.

Sulla scheda Cronologia query vedi i seguenti grafici (puoi scegliere tra Elenco di query e Parametri delle risorse):

- Tempo di esecuzione query – Questo grafico mostra quali query sono in esecuzione nello stesso intervallo di tempo. Scegliere una barra nel grafico per visualizzare ulteriori dettagli di esecuzione delle query.
- Query e caricamenti – Questa sezione elenca le query e i caricamenti per ID query.
- Capacità RPU utilizzata: questo grafico mostra la capacità complessiva in Redshift Processing Unit (RPU).
- Connessioni al database: – Questo grafico mostra il numero di connessioni database attive.

## Prestazioni del database

Sulla scheda Prestazioni database, vedi i seguenti grafici:

- Query completate al secondo – Questo grafico mostra il numero medio di query completate al secondo.
- Durata della query: – Questo grafico mostra il tempo medio per il completamento di una query.
- Connessioni al database: – mostra il numero di connessioni database attive.
- Esecuzione di query – Questo grafico mostra il numero totale di query in esecuzione in un determinato momento.
- Query in coda – Questo grafico mostra il numero totale di query in coda in un determinato momento.
- Suddivisione del tempo di esecuzione delle query— Questo grafico mostra il tempo totale impiegato dalle query in esecuzione per tipo di query.

## Monitoraggio delle risorse

Sulla pagina Monitoraggio delle risorse, è possibile visualizzare grafici delle risorse consumate. È possibile filtrare i dati in base a diversi aspetti.

- Metric filter (Filtro di parametri): è possibile utilizzare i filtri delle metriche per selezionare i filtri per un gruppo di lavoro specifico, nonché scegliere l'intervallo di tempo.
- Capacità RPU utilizzata – Questo grafico mostra la capacità complessiva delle unità di elaborazione Redshift (RPU).
- Utilizzo del calcolo: questo grafico mostra l'utilizzo delle ore RPU in base al periodo per l'intervallo di tempo selezionato. Per intervalli di tempo inferiori a 6 ore, le ore RPU vengono visualizzate in termini di ora esatta. Per intervalli di tempo pari o superiori a 6 ore, le ore RPU vengono visualizzate come media.

Sulla pagina Unità di condivisione dati, è possibile gestire unità di condivisione dati Nel mio account e Da altri account. Per ulteriori informazioni sulla condivisione dei dati, consultare [Condivisione dei dati in Amazon Redshift Serverless](#).

## Considerazioni su quando utilizzare Amazon Redshift Serverless

Per un elenco delle aree Regioni AWS in cui è disponibile Amazon Redshift Serverless, consulta gli endpoint elencati per l'API [Redshift](#) Serverless nel. Riferimenti generali di Amazon Web Services

Alcune risorse utilizzate da Amazon Redshift Serverless sono soggette a quote. Per ulteriori informazioni, consulta [Quote per gli oggetti Amazon Redshift Serverless](#).

Quando si dichiara un cursore, le specifiche delle dimensioni del set di risultati per Amazon Redshift Serverless vengono immesse nel comando [DECLARE](#).

Finestra di manutenzione: non è presente una finestra di manutenzione in Amazon Redshift serverless. Gli aggiornamenti delle versioni software vengono applicati automaticamente. Non si verificano interruzioni per la connessione o l'esecuzione delle query esistenti quando Amazon Redshift cambia le versioni. Le nuove connessioni si conetteranno e funzioneranno sempre con Amazon Redshift Serverless all'istante.

ID delle zone di disponibilità: quando configuri l'istanza Amazon Redshift serverless, apri Additional considerations (Ulteriori considerazioni) e accertati che gli ID di sottorete forniti in Subnet (Sottorete) contengano almeno uno degli ID delle tre zone di disponibilità supportate. Per visualizzare la sottorete alla mappatura dell'ID zona di disponibilità, accedere alla console VPC e scegliere Sottoreti per visualizzare l'elenco degli ID sottorete con i relativi ID zona di disponibilità. Verificare che la sottorete sia mappata a un ID zona di disponibilità supportato. Per creare una sottorete, consultare [Creazione di una sottorete nel VPC](#) nella Guida per l'utente di Amazon VPC.

Tre sottoreti: è necessario disporre di almeno tre sottoreti in tre zone di disponibilità. Ad esempio, è possibile utilizzare tre sottoreti mappate alle zone di disponibilità us-east-1a, us-east-1b e us-east-1c. Un'eccezione è la regione Stati Uniti occidentali (California settentrionale). Richiede tre sottoreti, allo stesso modo delle altre regioni, ma queste devono estendersi solo su due zone di disponibilità. Una condizione è che una delle zone di disponibilità estese debba contenere due delle sottoreti.

Requisiti di indirizzi IP gratuiti: devi avere indirizzi IP gratuiti disponibili quando crei un gruppo di lavoro Amazon Redshift Serverless. Il numero minimo di indirizzi IP aumenta all'aumentare del numero di Redshift Processing Unit (RPU) per il gruppo di lavoro. In particolare, ogni sottorete del VPC del gruppo di lavoro richiede un numero minimo di indirizzi IP. Per ulteriori informazioni sull'allocazione di indirizzi IP, consulta [Indirizzamento IP](#) nella Guida per l'utente di Amazon VPC.

Il numero minimo di indirizzi IP gratuiti richiesti per la creazione di un gruppo di lavoro è il seguente:

Numero di indirizzi IP gratuiti richiesti per ogni sottorete

Redshift Processing Unit (RPU)	Indirizzi IP disponibili richiesti	Dimensione minima CIDR
8	9	/27

Redshift Processing Unit (RPU)	Indirizzi IP disponibili richiesti	Dimensione minima CIDR
16	15	/27
32	13	/27
64	21	/27
128	37	/26
256	69	/25
512	133	/24

Sono necessari indirizzi IP disponibili anche quando si aggiorna il gruppo di lavoro per utilizzare più RPU. Il numero di indirizzi IP gratuiti richiesti per l'aggiornamento delle sottoreti per un gruppo di lavoro è il seguente:

Numero di indirizzi IP disponibili richiesti per l'aggiornamento di una sottorete

Redshift Processing Unit (RPU)	Redshift Processing Unit (RPU) aggiornate	Indirizzi IP disponibili richiesti
8	16	10
16	32	13
32	64	16
64	128	28
128	256	52
256	512	100

Spazio di archiviazione dopo la migrazione: quando si esegue la migrazione di cluster Amazon Redshift con provisioning di piccole dimensioni ad Amazon Redshift serverless, è possibile che si verifichi un aumento dell'allocazione dello spazio di archiviazione dopo la migrazione. Ciò è il risultato

dell'allocazione ottimizzata dello spazio di archiviazione, con conseguente spazio di archiviazione preallocato. Questo spazio viene utilizzato per un periodo di tempo man mano che i dati crescono in Amazon Redshift Serverless.

Unità di condivisione dati tra cluster con provisioning di Amazon Redshift serverless e Amazon Redshift: in presenza di unità di condivisione dati, dove Amazon Redshift serverless è il producer e un cluster con provisioning è il consumer, la versione del cluster con provisioning deve essere successiva alla 1.0.38214. Se si utilizza una versione di cluster precedente a questa, si verifica un errore durante l'esecuzione di una query. È possibile visualizzare la versione del cluster nella console di Amazon Redshift sulla scheda Maintenance (Manutenzione). Puoi anche eseguire `SELECT version();`.

Tempo massimo di esecuzione della query: il tempo di esecuzione trascorso per una query in secondi. Il tempo di esecuzione non include il tempo trascorso in attesa in una coda. Se una query supera il tempo di esecuzione impostato, Amazon Redshift Serverless la arresta. I valori validi sono compresi nell'intervallo 0-86.399.

Migrazione di tabelle con chiavi di ordinamento interlacciate: durante la migrazione dei cluster di cui Amazon Redshift ha effettuato il provisioning ad Amazon Redshift Serverless, Redshift converte le tabelle con chiavi di ordinamento interlacciate e `DISTSTYLE KEY` in chiavi di ordinamento composte. `DISTSTYLE` non cambia. Per ulteriori informazioni sugli stili di distribuzione, consulta [Utilizzo degli stili di distribuzione dati](#) nella guida per sviluppatori di Amazon Redshift. Per ulteriori informazioni sulle chiavi di ordinamento, consulta [Utilizzo delle chiavi di ordinamento](#).

Condivisione del VPC: puoi creare gruppi di lavoro Amazon Redshift serverless in un VPC condiviso. In tal caso, ti consigliamo di non eliminare la condivisione delle risorse in quanto il gruppo di lavoro potrebbe non essere più disponibile.

## Capacità di calcolo per Amazon Redshift Serverless

### Conoscere la capacità di Amazon Redshift Serverless

#### RPU

Amazon Redshift Serverless misura la capacità del data warehouse in Redshift Processing Units (RPU). Le RPU sono risorse utilizzate per gestire i carichi di lavoro.

#### Capacità base

Rappresenta la capacità di base del data warehouse utilizzata da Amazon Redshift per elaborare le query. La capacità di base è specificata in RPU. Puoi impostare una capacità di base in Redshift Processing Unit (RPU). Una RPU fornisce 16 GB di memoria. L'impostazione di una capacità di base superiore migliora le prestazioni delle query, in particolare per i processi di elaborazione dati che consumano molte risorse. La capacità di base predefinita per Amazon Redshift Serverless è 128 RPU. È possibile regolare l'impostazione della capacità di base da 8 RPU a 512 RPU in unità da 8 (8,16,24... 512), utilizzando la AWS console, l'operazione `UpdateWorkgroup` API o `update-workgroup` l'operazione in AWS CLI

Con una capacità minima di 8 RPU, ora si ha maggiore flessibilità per eseguire carichi di lavoro sia semplici che complessi in base ai requisiti di prestazioni. Le capacità RPU di base da 8, 16 e 24 RPU sono destinate a carichi di lavoro che richiedono meno di 128 TB di dati. Se i requisiti di dati sono superiori a 128 TB, è necessario utilizzare un minimo di 32 RPU. Per i carichi di lavoro con tabelle con un elevato numero di colonne numeriche e maggiore simultaneità, si consiglia di utilizzare 32 o più RPU.

## Considerazioni e limitazioni per la capacità di Amazon Redshift serverless

Di seguito sono riportate le considerazioni e limitazioni per la capacità di Amazon Redshift serverless.

- Le configurazioni da 8 o 16 RPU supportano una capacità di archiviazione gestita da Redshift fino a 128 TB. Se utilizzi più di 128 TB di archiviazione gestita, non è possibile effettuare il downgrade a meno di 32 RPU.
- La modifica della capacità di base del gruppo di lavoro potrebbe annullare alcune delle query in esecuzione sul gruppo di lavoro.

## Dimensionamento e ottimizzazione basati sull'intelligenza artificiale (anteprima)

Questa è di una documentazione di pre-rilascio per il dimensionamento e l'ottimizzazione basati sull'intelligenza artificiale in Amazon Redshift serverless, che è nella versione di anteprima. La documentazione e la funzionalità sono soggette a modifiche. Consigliamo di utilizzare questa caratteristica solo in ambienti di test e non in ambienti di produzione. Per i termini e condizioni dell'anteprima, consulta la sezione su beta e anteprime nei [AWS termini del servizio](#).

Questa anteprima è disponibile nei seguenti formati: Regioni AWS

- Stati Uniti orientali (Ohio) (us-east-2)
- Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Stati Uniti occidentali (Oregon) (us-west-2)
- Asia Pacifico (Tokyo) (ap-northeast-1)
- Europa (Irlanda) (eu-west-1)
- Europa (Stoccolma) (eu-north-1)

È possibile creare un gruppo di lavoro di anteprima per testare le nuove funzionalità di Amazon Redshift serverless. Non è possibile utilizzare queste funzionalità in produzione o spostare il gruppo di lavoro di anteprima in un gruppo di lavoro di produzione. Per i termini e le condizioni dell'anteprima, consulta Beta and Previews in [AWS Service Terms](#). Per istruzioni su come creare un gruppo di lavoro di anteprima, consulta [Creazione di un gruppo di lavoro di anteprima](#).

Puoi anche impostare un obiettivo di rapporto prezzo/prestazioni per il gruppo di lavoro, in modo che Redshift possa apportare automaticamente alle tue risorse le ottimizzazioni basate sull'intelligenza artificiale. Puoi così raggiungere i tuoi obiettivi di rapporto prezzo/prestazioni ottimizzando al contempo i costi. Questa ottimizzazione automatica del rapporto prezzo/prestazioni è particolarmente utile se non sai quale capacità di base impostare per i carichi di lavoro o se alcune parti del carico di lavoro potrebbero essere più efficienti con un numero maggiore di risorse allocate.

Ad esempio, se l'organizzazione esegue in genere carichi di lavoro che richiedono solo 32 RPU ma improvvisamente introduce una query più complessa, è possibile che non si conosca la quantità appropriata della capacità di base. L'impostazione di una capacità di base più elevata comporta un miglior rapporto prezzo/prestazioni, ma anche costi più elevati che potrebbero non corrispondere alle aspettative. Utilizzando il dimensionamento e l'ottimizzazione delle risorse basati sull'intelligenza artificiale, Amazon Redshift serverless adatta automaticamente le RPU per soddisfare gli obiettivi di rapporto prezzo/prestazioni, mantenendo al contempo i costi ottimizzati per l'organizzazione. Questa ottimizzazione automatica è utile indipendentemente dalla dimensione del carico di lavoro. L'ottimizzazione automatica consente di raggiungere gli obiettivi di rapporto prezzo/prestazioni dell'organizzazione in presenza di un numero illimitato di query complesse.

Gli obiettivi di rapporto prezzo/prestazioni sono un'impostazione specifica del gruppo di lavoro. Gruppi di lavoro diversi possono avere obiettivi di rapporto prezzo/prestazioni diversi.

Per mantenere i costi prevedibili, imposta il limite di capacità massima che Amazon Redshift serverless può allocare ai carichi di lavoro.

Per configurare gli obiettivi di rapporto prezzo/prestazioni, utilizza la AWS console. Per impostazione predefinita, l'obiettivo del rapporto prezzo/prestazioni è abilitato quando si crea un nuovo gruppo di lavoro ed è impostato su Bilanciato. Per impostare un diverso obiettivo di rapporto prezzo/prestazioni o specificare una capacità di base per il gruppo di lavoro, utilizza le impostazioni personalizzate durante la creazione del gruppo di lavoro. Per ulteriori informazioni sulla creazione di un gruppo di lavoro, consulta [Creazione di un gruppo di lavoro con uno spazio dei nomi](#).

Per modificare l'obiettivo di rapporto prezzo/prestazioni per il gruppo di lavoro:

1. Nella console Amazon Redshift serverless scegli Configurazione del gruppo di lavoro.
2. Scegli il gruppo di lavoro per cui desideri modificare l'obiettivo di rapporto prezzo/prestazioni. Seleziona la scheda Prestazioni e scegli Modifica.
3. Scegli Obiettivo di rapporto prezzo/prestazioni e regola il cursore in base all'obiettivo che desideri impostare per il gruppo di lavoro.
4. Seleziona Salvataggio delle modifiche.

Per aggiornare la quantità massima di RPU che Amazon Redshift serverless può allocare al carico di lavoro, passa alla scheda Limiti della configurazione del gruppo di lavoro.

Per informazioni sull'ottimizzazione e sul dimensionamento delle risorse basati sull'intelligenza artificiale, guarda il video seguente.

## Fatturazione per Amazon Redshift Serverless

### Prezzi

Per ulteriori informazioni sui prezzi, consultare [Prezzi di Amazon Redshift](#).

### Fatturazione per la capacità di calcolo

La capacità di base e il suo impatto sulla fatturazione

Quando vengono eseguite query, la fatturazione si basa sulla capacità utilizzata in una determinata durata, in ore RPU su base al secondo. Quando non vengono eseguite query, non viene fatturata alcuna capacità di calcolo. Inoltre, viene addebitato il costo di Redshift Managed Storage (RMS) in base alla quantità di dati archiviati.

Quando crei il tuo gruppo di lavoro, hai la possibilità di impostare Capacità base e il computing. È possibile regolare la capacità di base superiore o inferiore per un gruppo di lavoro esistente per

soddisfare i requisiti prezzo/prestazioni del carico di lavoro a livello di gruppo di lavoro. Seleziona il gruppo di lavoro da Configurazione del gruppo di lavoro e scegli la scheda Limiti per modificare la capacità di base utilizzando la console.

Con l'aumentare del numero di query, Amazon Redshift Serverless viene dimensionato automaticamente per fornire prestazioni uniformi.

### Limite massimo di utilizzo in ore RPU

Per mantenere i costi prevedibili per Amazon Redshift Serverless, puoi impostare il valore Maximum RPU hours (Numero massimo di ore RPU) utilizzato al giorno, a settimana o al mese. Puoi impostare questo valore con la console o l'API. Quando viene raggiunto un limite, è possibile specificare di scrivere una voce di log in una tabella di sistema, di ricevere un avviso o di disattivare le query utente. L'impostazione delle ore RPU massime aiuta a mantenere sotto controllo i costi. Le impostazioni per il massimo delle ore RPU si applicano al gruppo di lavoro sia per le query che accedono ai dati nel data warehouse sia per le query che accedono a dati esterni, ad esempio in una tabella esterna in Amazon S3.

Di seguito è riportato un esempio:

Supponi di impostare il limite di 100 ore per settimana. Per eseguire questa operazione sulla console, procedi come segue:

1. Scegli il gruppo di lavoro, quindi seleziona Gestisci i limiti di utilizzo nella scheda Limiti.
2. Aggiungi un limite di utilizzo, scegliendo la frequenza Settimanale, la durata di 100 ore e impostando l'azione su Disattiva query degli utenti.

Con questo esempio, se si raggiunge il limite di 100 ore RPU in una settimana, le query vengono disattivate.

L'impostazione del numero massimo di ore RPU per il gruppo di lavoro non limita le prestazioni o le risorse di calcolo del gruppo di lavoro. Puoi regolare le impostazioni in qualsiasi momento senza interessare l'elaborazione delle query. L'obiettivo dell'impostazione del numero massimo di ore RPU è quello di aiutarti a soddisfare i requisiti di prezzo e prestazioni. Per ulteriori informazioni sulla fatturazione serverless, consulta [Prezzi di Amazon Redshift](#).

Un altro modo per mantenere prevedibile il costo di Amazon Redshift serverless è quello di utilizzare [Rilevamento di anomalie dei costi](#) di AWS per ridurre le sorprese nella fatturazione e fornire un maggiore controllo.

 Note

Il [calcolatore dei prezzi di Amazon Redshift](#) è utile per stimare i prezzi. Inserisci le risorse di calcolo necessarie e ti verrà fornita un'anteprima del costo.

## Impostazione della capacità massima per controllare i costi delle risorse di calcolo

L'impostazione della capacità massima funge da limite di RPU fino al quale Amazon Redshift serverless può aumentare. Ti aiuta a controllare il costo delle risorse di calcolo. Analogamente a come la capacità di base stabilisce una quantità minima di risorse di calcolo disponibili, la capacità massima stabilisce un limite all'utilizzo di RPU. In questo modo, le spese rispetteranno i tuoi piani. La capacità massima si applica specificamente a ciascun gruppo di lavoro e limita l'utilizzo delle risorse di calcolo in qualsiasi momento.

In che modo la capacità massima differisce dal limite di utilizzo in ore RPU

Lo scopo del limite massimo in ore RPU e dell'impostazione della capacità massima è per entrambi controllare i costi, ma con mezzi diversi. I seguenti punti spiegano le differenze:

- **Capacità massima:** questa impostazione stabilisce il numero massimo di RPU utilizzate da Amazon Redshift serverless per scopi di dimensionamento. Quando è richiesto il dimensionamento automatico delle risorse di calcolo, un valore elevato per la capacità massima può migliorare la velocità di trasmissione effettiva delle query. Quando viene raggiunto il limite massimo di capacità, il gruppo di lavoro non aumenta ulteriormente le risorse.
- **Limite massimo di utilizzo in ore RPU:** a differenza della capacità massima, questa impostazione non stabilisce un limite alla capacità. Tuttavia esegue altre azioni per aiutarti a limitare i costi. tra cui l'aggiunta di una voce a un log, l'invio di una notifica o l'interruzione dell'esecuzione delle query, se lo desideri.

È possibile utilizzare esclusivamente la capacità massima oppure integrarla con azioni relative ai limiti massimi di utilizzo in ore RPU.

### Caso d'uso relativo alla capacità massima

Ogni gruppo di lavoro può avere un'impostazione di capacità massima diversa. Questo approccio ti aiuta a rispettare i requisiti di budget. Per illustrare come funziona, supponi quanto segue:

- Disponi di un gruppo di lavoro con la capacità di base impostata su 256 RPU. Disponi di carichi di lavoro costanti a poco più di 256 RPU per la maggior parte del mese.
- La capacità massima è impostata su 512 RPU.

Supponi di avere un utilizzo inatteso ed elevato in un periodo di tre giorni per generare report statistici ad hoc. In questo caso, la capacità massima impostata evita costi di elaborazione superiori a quelli per 512 RPU. In questo modo, puoi essere certo che la capacità di calcolo non superi mai questo limite massimo.

### Note di utilizzo per la capacità massima

Le seguenti note possono aiutarti a impostare la capacità massima in modo appropriato:

- Ogni gruppo di lavoro Amazon Redshift serverless può avere un'impostazione di capacità massima diversa.
- Se in un periodo hai un utilizzo delle risorse molto elevato e la capacità massima è impostata su un livello di RPU basso, l'elaborazione del carico di lavoro può ritardare e comportare un'esperienza non ottimale per l'utente.
- La configurazione dell'impostazione della capacità massima non interferisce con l'esecuzione delle query, anche durante i periodi di utilizzo elevato di RPU. Non funziona come il limite di utilizzo, che può impedire l'esecuzione delle query. Limita solo le risorse di calcolo disponibili per il gruppo di lavoro. È possibile visualizzare la capacità utilizzata in un periodo di tempo sul pannello di controllo Amazon Redshift serverless. Per ulteriori informazioni sulla visualizzazione dei dati di riepilogo, consulta [Controllo dei dati di riepilogo di Amazon Redshift serverless utilizzando il pannello di controllo](#).
- L'impostazione della capacità massima è 5632 RPU.

### In che modo impostare la capacità massima

È possibile impostare la capacità massima nella console. Per un gruppo di lavoro esistente, puoi modificare l'impostazione in Configurazione del gruppo di lavoro. È anche possibile utilizzare la CLI per impostarla utilizzando un comando come il seguente:

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity 512
```

In tal modo configuri l'impostazione della capacità massima per il gruppo di lavoro con il nome specificato. Dopo averla configurata, puoi controllare il valore sulla console per verificarlo. È anche possibile controllare il valore utilizzando la CLI eseguendo il comando `get-workgroup`.

È possibile disattivare l'impostazione della capacità massima configurandola su `-1`, come segue:

```
aws redshift-serverless update-workgroup --workgroup-name myworkgroup --max-capacity -1
```

## Monitoraggio dell'utilizzo e dei costi di Amazon Redshift serverless

Sono disponibili diversi modi per stimare l'utilizzo e la fatturazione per Amazon Redshift Serverless. Le visualizzazioni di sistema possono essere utili perché i metadati di sistema, inclusi i dati di interrogazione e utilizzo, sono tempestivi e non è necessario eseguire alcuna configurazione per interrogarli. CloudWatch può anche essere utile per monitorare l'utilizzo di un'istanza Serverless di Amazon Redshift e dispone di funzionalità aggiuntive per fornire approfondimenti e impostare azioni.

Visualizzazione dell'utilizzo mediante query su una vista di sistema

Esegui query sulla tabella di sistema `SYS_SERVERLESS_USAGE` per monitorare l'utilizzo e ottenere i costi delle query:

```
select trunc(start_time) "Day",
(sum(charged_seconds)/3600::double
precision) * <Price for 1 RPU> as cost_incurred
from sys_serverless_usage
group by 1
order by 1
```

Questa query indica il costo giornaliero sostenuto per Amazon Redshift serverless in base all'utilizzo.

Note sull'utilizzo per stabilire uso e costi

- Pagi i carichi di lavoro eseguiti, in ore RPU su base al secondo, con un costo minimo di 60 secondi.
- I record della tabella di sistema `sys_serverless_usage` mostrano i costi sostenuti in intervalli di tempo di 1 minuto. È importante comprendere il contenuto delle seguenti colonne:

La colonna `charged_seconds`:

- Fornisce i secondi di RPU addebitati durante l'intervallo di tempo. I risultati includono gli eventuali addebiti minimi di Amazon Redshift serverless.

- Include informazioni sull'utilizzo delle risorse di calcolo dopo il completamento delle transazioni. Pertanto, il valore di questa colonna può essere 0 se le transazioni non sono terminate.

La colonna `compute_seconds`:

- Fornisce informazioni in tempo reale sull'utilizzo del calcolo. Non sono inclusi gli addebiti minimi di Amazon Redshift serverless. Pertanto può differire in una certa misura dai secondi addebitati e fatturati durante l'intervallo.
- Mostra le informazioni sull'utilizzo durante ogni transazione (anche se una transazione non è terminata), per cui i dati forniti sono in tempo reale.
- Esistono situazioni in cui `compute_seconds` è 0 ma `charged_seconds` è maggiore di 0 o viceversa. Si tratta di un comportamento normale dovuto al modo in cui i dati vengono registrati nella vista di sistema. Per una rappresentazione più accurata dei dettagli sull'utilizzo serverless, consigliamo di aggregare i dati in `SYS_SERVERLESS_USAGE`.

Per ulteriori informazioni sul monitoraggio delle tabelle e delle viste, consulta [Monitoraggio di query e carichi di lavoro con Amazon Redshift serverless](#).

### Visualizzazione dell'utilizzo con CloudWatch

Puoi utilizzare le metriche disponibili in CloudWatch per monitorare l'utilizzo. Le metriche generate per `CloudWatch ComputeSeconds` i secondi RPU totali utilizzati nel minuto corrente e `ComputeCapacity` indicano la capacità di elaborazione totale per quel minuto. I parametri di utilizzo sono disponibili anche sulla console Redshift sul Pannello di controllo serverless di Redshift. Per ulteriori informazioni su CloudWatch, consulta [What is Amazon CloudWatch?](#)

## Fatturazione per l'archiviazione

La capacità di archiviazione principale viene fatturata come Redshift Managed Storage (RMS). L'archiviazione è fatturata per GB/mese. La fatturazione dell'archiviazione è separata dalla fatturazione per le risorse di elaborazione. Lo storage utilizzato per gli snapshot degli utenti viene fatturato alla tariffa di fatturazione di backup standard.

I costi di trasferimento dati e di machine learning si applicano separatamente, così come quelli dei cluster sottoposti a provisioning. Replica di snapshot e unità di condivisione dei dati tra le regioni AWS vengono fatturate alle tariffe di trasferimento indicate nella pagina dei prezzi. Per ulteriori informazioni sui prezzi, consultare [Prezzi di Amazon Redshift](#).

## Visualizzazione dell'utilizzo della fatturazione con CloudWatch

La metrica `SnapshotStorage`, che tiene traccia dell'utilizzo dello storage delle istantanee, viene generata e inviata a CloudWatch. Per ulteriori informazioni su CloudWatch, consulta [What is Amazon CloudWatch?](#)

## Usare la prova gratuita di Amazon Redshift Serverless

Amazon Redshift Serverless offre una versione di prova gratuita. Se partecipi alla prova gratuita, puoi visualizzare il saldo del credito di prova gratuito nella console di Redshift e controllare l'utilizzo della prova gratuita nella visualizzazione di sistema `SYS_SERVERLESS_USAGE`. Tieni presente che i dettagli di fatturazione per l'utilizzo di prova gratuito non vengono visualizzati nella console di fatturazione. Puoi visualizzare l'utilizzo nella console di fatturazione solo dopo la fine della prova gratuita. Per ulteriori informazioni sulla prova gratuita di Amazon Redshift Serverless, consulta [Prova gratuita di Amazon Redshift Serverless](#).

## Note di utilizzo nella fatturazione

- **Utilizzo della registrazione** - Una query o una transazione viene misurata e registrata solo dopo il completamento, il rollback o l'arresto della transazione. Ad esempio, se una transazione viene eseguita per due giorni, l'utilizzo della RPU viene registrato dopo il completamento. È possibile monitorare l'uso continuo in tempo reale eseguendo query `sys_serverless_usage`. La registrazione delle transazioni può riflettere la variazione di utilizzo della RPU e influire sui costi per orari specifici e per l'uso quotidiano.
- **Scrittura di transazioni esplicite** - È importante come best practice per porre fine alle transazioni. Se non interrompi o esegui il rollback di una transazione aperta, Amazon Redshift Serverless continua a utilizzare le RPU. Ad esempio, se scrivi un esplicito `BEGIN TRAN`, è importante avere il corrispondente `COMMIT` e le istruzioni `ROLLBACK`.
- **Query annullate** - Se si esegue una query e la si annulla prima che finisca, ti verrà fatturato il tempo di esecuzione della query.
- **Dimensionamento**: l'istanza Amazon Redshift Serverless può avviare la scalabilità per la gestione di periodi di carico più elevato, al fine di mantenere prestazioni costanti. La fatturazione Amazon Redshift Serverless include sia la capacità di calcolo di base che la capacità scalata alla stessa tariffa RPU.
- **Ridimensionamento verso il basso**: Amazon Redshift Serverless aumenta la scalabilità rispetto alla sua capacità RPU di base per gestire periodi di carico più elevato. In alcuni casi, la capacità RPU può rimanere a un'impostazione più elevata per un periodo dopo il calo del caricamento della

query. Si consiglia di impostare il valore massimo delle ore RPU nella console per evitare costi imprevisti.

- Tabelle di sistema - Quando si esegue una query su una tabella di sistema, viene fatturato il tempo della query.
- Redshift Spectrum: quando disponi di Amazon Redshift Serverless ed esegui query, non è previsto un costo separato per le query di data-lake. Per le query sui dati archiviati in Amazon S3, l'addebito è lo stesso, in base al tempo della transazione, delle query sui dati locali.
- Query federate - Le query federate vengono addebitate in termini di RPU, utilizzate in un intervallo di tempo specifico, nello stesso modo delle query sul data warehouse o sul data lake.
- Storage - Lo storage viene fatturato separatamente, in GB/mese.
- Costo minimo: il costo minimo è di 60 secondi per l'utilizzo delle risorse di calcolo, misurato su base al secondo.
- Fatturazione snapshot - La fatturazione snapshot non cambia. Viene addebitata in base allo spazio di archiviazione, fatturata a una tariffa di GB/mese. È possibile ripristinare il data warehouse in punti specifici nelle ultime 24 ore con una granularità di 30 minuti, gratuitamente. Per ulteriori informazioni sui prezzi, consultare [Prezzi di Amazon Redshift](#).

## Best practice di Amazon Redshift Serverless per mantenere la fatturazione prevedibile

Esistono alcune best practice da seguire e impostazioni integrate che aiutano a mantenere la fatturazione coerente.

- Assicurati di terminare ogni transazione. Quando si utilizza BEGIN per iniziare una transazione, è importante anche END.
- Usa la gestione degli errori con le best practice per rispondere con grazia agli errori e terminare ogni transazione. La riduzione al minimo delle transazioni aperte aiuta a evitare l'uso inutile della RPU.
- Usa SESSION TIMEOUT per terminare le transazioni aperte e le sessioni inattive. Fa scadere qualsiasi sessione inattiva per più di 3600 secondi (1 ora). Fa scadere qualsiasi transazione mantenuta aperta e inattiva per più di 21600 secondi (6 ore). Questa impostazione di timeout può essere modificata esplicitamente per un utente specifico, ad esempio quando si desidera mantenere aperta una sessione per una query di lunga durata. L'argomento [CREA UTENTE](#) mostra come regolare SESSION TIMEOUT per un utente.
  - Nella maggior parte dei casi, si consiglia di non estendere il valore SESSION TIMEOUT, a meno che non si disponga di un caso d'uso che lo richiede specificamente. Se la sessione rimane

inattiva, con una transazione aperta, può risultare in un caso in cui le RPU vengono utilizzate fino alla chiusura della sessione. Ciò comporterà costi inutili.

- Il tempo massimo per una query in esecuzione in Amazon Redshift serverless è di 86.399 secondi (24 ore). Il periodo massimo di inattività per una transazione aperta prima che Amazon Redshift serverless termini la sessione associata alla transazione è sei ore. Per ulteriori informazioni, consulta [Quote per gli oggetti Amazon Redshift Serverless](#).

## Connessione ad Amazon Redshift Serverless

Dopo aver configurato la tua istanza Amazon Redshift Serverless, puoi connetterti con una varietà di metodi, descritti di seguito. Se hai più team o progetti e desideri gestire i costi separatamente, puoi utilizzare separatamente Account AWS.

Per un elenco delle aree Regioni AWS in cui è disponibile Amazon Redshift Serverless, consulta gli endpoint elencati per l'API [Redshift](#) Serverless nel. Riferimenti generali di Amazon Web Services

Amazon Redshift Serverless si connette all'ambiente serverless del tuo Account AWS sistema attuale. Regione AWS Amazon Redshift serverless viene eseguito in un VPC all'interno degli intervalli di porte 5431-5455 e 8191-8215. Il valore predefinito è 5439. Attualmente, puoi modificare le porte solo con il funzionamento UpdateWorkgroup e l'operazione dell'API. AWS CLI update-workgroup

## Connessione ad Amazon Redshift Serverless

Puoi connetterti a un database (denominato dev) in Amazon Redshift serverless con la seguente sintassi.

```
workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:port/dev
```

Ad esempio, la seguente stringa di connessione specifica la regione us-east-1.

```
default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev
```

## Connessione ad Amazon Redshift Serverless tramite driver JDBC

È possibile utilizzare uno dei seguenti metodi per connettersi all'endpoint Amazon Redshift Serverless con il client SQL preferito utilizzando il driver JDBC versione 2 fornito da Amazon Redshift.

Per eseguire la connessione con le credenziali di accesso per l'autenticazione del database utilizzando il driver JDBC versione 2.1.x o successiva, utilizza la seguente sintassi. Il numero di porta è facoltativo; se non incluso, Amazon Redshift Serverless imposta il numero di porta 5439. È possibile passare a un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215. Per modificare la porta predefinita per un endpoint serverless, utilizza la AWS CLI e l'API Amazon Redshift.

```
jdbc:redshift://workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:5439/dev
```

Ad esempio, la seguente stringa di connessione specifica il gruppo di lavoro predefinito, l'ID account 123456789012 e la regione us-east-2.

```
jdbc:redshift://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/dev
```

Per connettersi a IAM utilizzando il driver JDBC versione 2.1.x o successiva, utilizzare la seguente sintassi. Il numero di porta è facoltativo; se non incluso, Amazon Redshift Serverless imposta il numero di porta 5439. È possibile passare a un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215. Per modificare la porta predefinita per un endpoint serverless, usa l'API AWS CLI e Amazon Redshift.

```
jdbc:redshift:iam://workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com:5439/dev
```

Ad esempio, la seguente stringa di connessione specifica il gruppo di lavoro predefinito, l'ID account 123456789012 e la regione us-east-2.

```
jdbc:redshift:iam://default.123456789012.us-east-2.redshift-serverless.amazonaws.com:5439/dev
```

Utilizza la seguente sintassi per ODBC.

```
Driver={Amazon Redshift (x64)}; Server=workgroup-name.account-number.aws-region.redshift-serverless.amazonaws.com; Database=dev
```

Se si utilizza una versione del driver JDBC precedente alla 2.1.0.9 e si connette a IAM, è necessario utilizzare la seguente sintassi.

```
jdbc:redshift:iam://redshift-serverless-<name>:aws-region/database-name
```

Ad esempio, la seguente stringa di connessione specifica l'impostazione predefinita del gruppo di lavoro e Regione AWS us-east-1.

```
jdbc:redshift:iam://redshift-serverless-default:us-east-1/dev
```

Per ulteriori informazioni sui driver, consulta [Configurazione delle connessioni in Amazon Redshift](#).

## Individuazione della stringa di connessione JDBC e ODBC

Per connettersi al gruppo di lavoro con il proprio strumento client SQL è richiesta la stringa di connessione JDBC o ODBC. Tale stringa di connessione è presente nella console di Amazon Redshift serverless, nella pagina dei dettagli del gruppo di lavoro.

Per trovare la stringa di connessione di un gruppo di lavoro

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Redshift Serverless.
3. Dal menu di navigazione scegli Configurazione del gruppo di lavoro, quindi scegli dall'elenco il nome del gruppo di lavoro per visualizzarne i dettagli.
4. Sono disponibili le stringhe di connessione URL JDBC e URL ODBC, insieme a dettagli aggiuntivi, nella sezione Informazioni generali. Ogni stringa si basa sulla AWS regione in cui viene eseguito il gruppo di lavoro. Scegli l'icona accanto alla stringa di connessione corretta per copiare la stringa di connessione.

## Connessione ad Amazon Redshift Serverless con l'API dei dati

Puoi anche utilizzare l'Amazon Redshift Data API per connetterti ad Amazon Redshift Serverless. Utilizzate il `workgroup-name` parametro al posto del `cluster-identifier` parametro nelle AWS CLI chiamate.

Consulta [Uso dell'API dati di Amazon Redshift](#) per ulteriori informazioni sull'API dati. Ad esempio, che chiama l'API Data in Python e altri esempi, consulta [Getting Started with Redshift Data API](#) e cerca nelle cartelle `and in quick-start use-cases` GitHub

# Connessione con SSL ad Amazon Redshift Serverless

## Configurazione di una connessione sicura ad Amazon Redshift Serverless

Per supportare le connessioni SSL, Redshift Serverless crea e installa [AWS Certificate Manager un certificato SSL emesso da \(ACM\)](#) per ogni gruppo di lavoro. I certificati ACM sono attendibili pubblicamente dalla maggior parte dei sistemi operativi, dei browser Web e dei client. Potrebbe essere necessario scaricare un pacchetto di certificati se i client o le applicazioni SQL si connettono a Redshift Serverless tramite SSL con `sslmode` l'opzione di connessione impostata `require`, oppure `verify-ca` `verify-full`. Se il tuo cliente necessita di un certificato, Redshift Serverless fornisce un pacchetto di certificati come segue:

- [Scaricate il pacchetto da `https://s3.amazonaws.com/redshift-downloads/.cert.amazon-trust-ca-bundle`](https://s3.amazonaws.com/redshift-downloads/.cert.amazon-trust-ca-bundle)

- Il numero di checksum MD5 previsto è `418dea9b6d5d5de7a8f1ac42e164cdf`.
- Il numero di checksum sha256 è `36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550`.

Non utilizzare certificato di bundle precedente che si trovava in `https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt`.

- [In Cina Regione AWS, scaricate il pacchetto da `https://s3.cn-north-1.amazonaws.com.cn/.cert.redshift-downloads-cn.amazon-trust-ca-bundle`](https://s3.cn-north-1.amazonaws.com.cn/.cert.redshift-downloads-cn.amazon-trust-ca-bundle)

- Il numero di checksum MD5 previsto è `418dea9b6d5d5de7a8f1ac42e164cdf`.
- Il numero di checksum sha256 è `36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550`.

Non utilizzare i certificati di bundle precedenti che si trovavano in `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt` e `https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem`

### Important

Redshift Serverless ha cambiato il modo in cui vengono gestiti i certificati SSL. Potrebbe essere necessario aggiornare i certificati Trust Root CA correnti per continuare a connetterti

ai tuoi gruppi di lavoro tramite SSL. Per ulteriori informazioni sui certificati ACM per le connessioni SSL, consulta. [Passaggio ai certificati ACM per connessioni SSL](#)

Per impostazione predefinita, i database dei gruppi di lavoro accettano una connessione indipendentemente dal fatto che utilizzi SSL o meno.

Per creare un nuovo gruppo di lavoro che accetti solo connessioni SSL, usa il `create-workgroup` comando e imposta il parametro su `require_ssl true` Per utilizzare l'esempio seguente, sostituiscilo *yourNamespaceName* con il nome del tuo namespace e sostituiscilo *yourWorkgroupName* con il nome del tuo gruppo di lavoro.

```
aws redshift-serverless create-workgroup \  
--namespace-name yourNamespaceName \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Per aggiornare un gruppo di lavoro esistente in modo che accetti solo connessioni SSL, utilizzate il `update-workgroup` comando e impostate il parametro su `require_ssl true` Tieni presente che Redshift Serverless riavvierà il gruppo di lavoro quando aggiorni il parametro `require_ssl` Per utilizzare l'esempio seguente, sostituiscilo *yourWorkgroupName* con il nome del tuo gruppo di lavoro.

```
aws redshift-serverless update-workgroup \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=require_ssl,parameterValue=true
```

Amazon Redshift supporta il protocollo di accordo chiave Elliptic Curve DiffieHellman Ephemeral (ECDHE). Con il protocollo ECDHE, il client e il server hanno ciascuno una coppia di chiavi pubblica-privata a curva ellittica utilizzata per stabilire un segreto condiviso su un canale insicuro. Per abilitare ECDHE non è necessario eseguire alcuna configurazione in Amazon Redshift. Se ci si connette da uno strumento client SQL che utilizza ECDHE per crittografare la comunicazione tra il client e il server, Amazon Redshift utilizza l'elenco di crittografie fornito per stabilire la connessione appropriata. Per ulteriori informazioni, consultare [Elliptic curve diffie-hellman](#) su Wikipedia e [Ciphers](#) sul sito Web di OpenSSL.

## Configurazione di una connessione SSL conforme a FIPS ad Amazon Redshift Serverless

Per creare un nuovo gruppo di lavoro che utilizza una connessione SSL conforme a FIPS, usa il comando e imposta il parametro su. `create-workgroup use_fips_ssl true` Per utilizzare l'esempio seguente, sostituiscilo con il nome del tuo namespace e sostituiscilo *yourNamespaceName* con il nome del tuo gruppo di lavoro. *yourWorkgroupName*

```
aws redshift-serverless create-workgroup \  
--namespace-name yourNamespaceName \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=use_fips_ssl,parameterValue=true
```

Per aggiornare un gruppo di lavoro esistente per utilizzare una connessione SSL conforme a FIPS, utilizzate il comando e impostate il parametro su. `update-workgroup use_fips_ssl true` Tieni presente che Redshift Serverless riavvierà il gruppo di lavoro quando aggiorni il parametro. `use_fips_ssl` Per utilizzare l'esempio seguente, sostituiscilo *yourWorkgroupName* con il nome del tuo gruppo di lavoro.

```
aws redshift-serverless update-workgroup \  
--workgroup-name yourWorkgroupName \  
--config-parameters parameterKey=use_fips_ssl,parameterValue=true
```

[Per ulteriori informazioni sulla configurazione di Redshift Serverless per l'utilizzo di connessioni conformi a FIPS, consulta `use\_fips\_ssl` nella Amazon Redshift Database Developer Guide.](#)

## Connessione ad Amazon Redshift Serverless da un endpoint VPC gestito da Amazon Redshift

### Connessione ad Amazon Redshift Serverless da altri endpoint VPC

[Per informazioni sulla configurazione o sulla configurazione di un endpoint VPC gestito per un gruppo di lavoro Serverless Amazon Redshift, consulta Lavorare con endpoint VPC gestiti da Redshift.](#)

## Connessione ad Amazon Redshift serverless da un endpoint VPC Redshift di un altro account o un'altra regione

### Connessione ad Amazon Redshift serverless dagli endpoint VPC

Amazon Redshift Serverless Puoi fornire l'accesso al VPC di un altro account per accedere ad Amazon Redshift serverless nel tuo account. Il concetto è simile alla connessione da un endpoint VPC gestito, ma in questo caso la connessione proviene, ad esempio, da un client di database di un altro account. Sono disponibili alcune operazioni che puoi eseguire:

- Il proprietario di un database può fornire l'accesso a un VPC contenente Amazon Redshift serverless a un altro account della stessa regione.
- Il proprietario di un database può revocare l'accesso ad Amazon Redshift serverless.

Il vantaggio principale dell'accesso multi-account è consentire una collaborazione più semplice tra i database. Non è necessario che gli utenti abbiano accesso all'account che contiene il database per accedervi, pertanto si riducono i passaggi di configurazione e si risparmia tempo.

### Autorizzazioni necessarie per fornire l'accesso a un VPC di un altro account

Per fornire l'accesso o modificare l'accesso consentito, il concedente deve avere una policy di autorizzazioni assegnata con le seguenti autorizzazioni:

- redshift-serverless: PutResourcePolicy
- redshift-senza server: GetResourcePolicy
- redshift-senza server: DeleteResourcePolicy
- ec2: CreateVpcEndpoint
- ec2: ModifyVpcEndpoint

Potrebbero essere necessarie altre autorizzazioni specificate nella politica AWS gestita.

AmazonRedshiftFullAccess Per ulteriori informazioni, consulta [Concessione delle autorizzazioni ad Amazon Redshift Serverless](#).

L'assegnatario deve avere una policy di autorizzazioni assegnata con le seguenti autorizzazioni:

- redshift-serverless: ListWorkgroups
- redshift-senza server: CreateEndpointAccess

- redshift-senza server: UpdateEndpointAccess
- redshift-senza server: GetEndpointAccess
- redshift-senza server: ListEndpointAccess
- redshift-senza server: DeleteEndpointAccess

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

Di seguito è riportata una policy di risorse di esempio utilizzata per configurare l'accesso tra VPC:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CrossAccountCrossVPCAccess",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "123456789012",
          "234567890123"
        ]
      },
      "Action": [
        "redshift-serverless:CreateEndpointAccess",
        "redshift-serverless:UpdateEndpointAccess",
        "redshift-serverless>DeleteEndpointAccess",
        "redshift-serverless:GetEndpointAccess"
      ],
      "Condition": {
        "ArnLike": {
          "redshift-serverless:AuthorizedVpc": [
            "arn:aws:ec2:us-east-1:123456789012:vpc/*",
            "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-456",
            "arn:aws:ec2:us-east-1:234567890123:vpc/vpc-987"
          ]
        }
      }
    }
  ]
}
```

}

Nelle procedure che seguono in questa sezione si presuppone che l'utente che le esegue disponga delle autorizzazioni assegnate appropriate, ad esempio un ruolo IAM assegnato con le autorizzazioni elencate. Inoltre si presuppone che al gruppo di lavoro sia associato un ruolo IAM con le autorizzazioni appropriate per le risorse.

### Autorizzazione dell'accesso VPC ad altri account mediante la console

Questa procedura mostra i passaggi per configurare l'accesso al database quando sei il proprietario e desideri concedere l'accesso.

### Autorizzazione dell'accesso dall'account proprietario

1. Nella scheda Accesso ai dati delle proprietà del gruppo di lavoro Amazon Redshift serverless è presente un elenco denominato Account autorizzati. Mostra gli account e i VPC che dispongono dell'accesso autorizzato al gruppo di lavoro. Trova l'elenco e scegli Concedi l'accesso per aggiungere un account all'elenco.
2. Viene visualizzata una finestra in cui è possibile aggiungere le informazioni sull'assegnatario. Inserisci l'ID dell'account AWS , ossia l'ID composto da 12 cifre dell'account a cui desideri autorizzare l'accesso.
3. Autorizza l'accesso a tutti i VPC per l'assegnatario oppure a VPC specifici. Se autorizzi l'accesso solo a VPC specifici, aggiungi ciascun ID corrispondente e scegli Aggiungi VPC.
4. Al termine, seleziona Salva le modifiche.

Quando salvi le modifiche, l'account viene visualizzato nell'elenco Account autorizzati. La voce mostra l'ID dell'account e l'elenco dei VPC a cui è stato autorizzato l'accesso.

Il proprietario del database può anche revocare l'accesso a un account. Il proprietario può revocare l'accesso in qualsiasi momento.

### Revoca dell'accesso a un account

1. Puoi iniziare dall'elenco degli account autorizzati. Per prima cosa, seleziona uno o più account.
2. Scegli Revoca accesso.

Una volta autorizzato l'accesso, l'amministratore del database dell'assegnatario può controllare la console per determinare se dispone dell'accesso.

## Utilizzo della console per verificare l'autorizzazione per accedere a un altro account

1. Nella scheda Accesso ai dati delle proprietà del gruppo di lavoro Amazon Redshift serverless è presente un elenco denominato Account autorizzati. Mostra gli account a cui è possibile accedere dal gruppo di lavoro. L'assegnatario non può utilizzare l'URL dell'endpoint del gruppo di lavoro per accedere direttamente al gruppo di lavoro. Per accedere al gruppo di lavoro, in qualità di assegnatario, vai alla sezione Endpoint e scegli Crea un endpoint.
2. Quindi, in qualità di assegnatario, fornisci un nome di endpoint e un VPC per accedere al gruppo di lavoro.
3. Una volta creato correttamente, l'endpoint viene visualizzato nella sezione Endpoint con il relativo URL. Puoi utilizzare questo URL dell'endpoint per accedere al gruppo di lavoro.

## Autorizzazione dell'accesso ad altri account mediante i comandi CLI

L'account che autorizza l'accesso deve prima autorizzare l'accesso a un altro account da connettere utilizzando `put-resource-policy`. Il proprietario del database può chiamare `put-resource-policy` per autorizzare un altro account a creare le connessioni al gruppo di lavoro. L'account dell'assegnatario può quindi utilizzare `create-endpoint-authorization` per creare le connessioni al gruppo di lavoro tramite i VPC consentiti.

Di seguito vengono illustrate le proprietà per `put-resource-policy` che puoi chiamare per consentire l'accesso a un account e a un VPC specifici.

```
aws redshift-serverless put-resource-policy
--resource-arn <value>
--policy <value>
```

Dopo aver eseguito il comando, puoi chiamare `get-resource-policy`, specificando `resource-arn` per vedere quali account e VPC sono autorizzati ad accedere alla risorsa.

La seguente chiamata può essere effettuata dall'assegnatario. Mostra informazioni sull'accesso autorizzato. In particolare, restituisce un elenco contenente i VPC a cui è stato autorizzato l'accesso.

```
aws redshift-serverless list-workgroups
--owner-account <value>
```

Lo scopo è che l'assegnatario ottenga informazioni dall'account che fornisce l'autorizzazione sulle autorizzazioni degli endpoint. L'elemento `owner-account` rappresenta l'account di condivisione.

Quando lo esegui, restituisce per ogni gruppo di lavoro `CrossAccountVpcs`, che è un elenco di VPC consentiti. Per riferimento, di seguito sono riportate tutte le proprietà disponibili per un gruppo di lavoro:

```
Output: workgroup (Object)
workgroupId String,
workgroupArn String,
workgroupName String,
status: String,
namespaceName: String,
baseCapacity: Integer, (Not-applicable)
enhancedVpcRouting: Boolean,
configParameters: List,
securityGroupIds: List,
subnetIds: List,
endpoint: String,
publiclyAccessible: Boolean,
creationDate: Timestamp,
port: Integer,
CrossAccountVpcs: List
```

### Note

Ricordiamo che il [trasferimento del cluster non è un prerequisito per la](#) configurazione di funzionalità di rete aggiuntive di Redshift. Inoltre, non è necessario attivarlo per abilitare le seguenti funzionalità:

- Connessione da un VPC multiaccount o interregionale a Redshift: puoi connetterti da un cloud privato AWS virtuale (VPC) a un altro che contiene un database Redshift, come descritto in questa sezione.
- Configurazione di un nome di dominio personalizzato: puoi creare un nome di dominio personalizzato, denominato anche URL personalizzato, per il cluster Amazon Redshift o il gruppo di lavoro Amazon Redshift serverless, per rendere il nome dell'endpoint più semplice e facile da ricordare. Per ulteriori informazioni, consulta [Utilizzo di un nome di dominio personalizzato per le connessioni client](#).

## Configurazione delle impostazioni appropriate per il traffico di rete per Amazon Redshift serverless

### Connessione a un'istanza Amazon Redshift Serverless accessibile al pubblico

Le istruzioni per impostare le impostazioni del traffico di rete sono disponibili in [Accessibilità pubblica con configurazione predefinita o personalizzata dei gruppi di sicurezza](#). Ciò include un caso d'uso in cui il cluster è accessibile pubblicamente.

### Connessione a un'istanza Amazon Redshift serverless non accessibile al pubblico

Le istruzioni per impostare le impostazioni del traffico di rete sono disponibili in [Accessibilità privata con configurazione predefinita o personalizzata del gruppo di sicurezza](#). Ciò include un caso d'uso in cui il cluster non è disponibile su Internet.

## Definizione dei ruoli del database da assegnare agli utenti federati in Amazon Redshift serverless

Puoi definire ruoli nell'organizzazione che determinano quali ruoli del database concedere in Amazon Redshift serverless. Per ulteriori informazioni, consulta [Definizione dei ruoli del database da assegnare agli utenti federati in Amazon Redshift serverless](#).

## Altre risorse

Per ulteriori informazioni sulle connessioni sicure ad Amazon Redshift serverless, tra cui la concessione di autorizzazioni, l'autorizzazione all'accesso a servizi aggiuntivi e la creazione di ruoli IAM, consulta [Identity and Access Management in Amazon Redshift Serverless](#).

## Definizione dei ruoli del database da assegnare agli utenti federati in Amazon Redshift serverless

Quando si fa parte di un'organizzazione, si dispone una raccolta di ruoli associati. Ad esempio, disponi di ruoli per la tua funzione lavorativa, come programmatore e manager. I ruoli determinano a quali applicazioni e dati hai accesso. La maggior parte delle organizzazioni utilizza un provider di identità, come Microsoft Active Directory, per assegnare ruoli a utenti e gruppi. L'uso dei ruoli per controllare l'accesso alle risorse è aumentato, perché le organizzazioni non devono gestire i singoli utenti.

Recentemente, il controllo degli accessi basato su ruoli è stato introdotto in Amazon Redshift serverless. Utilizzando i ruoli del database, puoi proteggere l'accesso a dati e oggetti, come ad esempio, schemi o tabelle. Oppure puoi utilizzare i ruoli per definire una serie di autorizzazioni elevate, ad esempio per un monitoraggio del sistema o un amministratore di database. Tuttavia, dopo aver concesso le autorizzazioni per le risorse ai ruoli del database, c'è una fase aggiuntiva, che consiste nel connettere i ruoli di un utente dall'organizzazione ai ruoli del database. Puoi assegnare a ciascun utente i ruoli del database al momento dell'accesso iniziale eseguendo istruzioni SQL, ma è molto impegnativo. Un modo più semplice è definire i ruoli del database da concedere e passarli ad Amazon Redshift serverless. Questa operazione ha il vantaggio di semplificare il processo di accesso iniziale.

Puoi passare ruoli ad Amazon Redshift serverless utilizzando `GetCredentials`. Quando un utente accede per la prima volta a un database Amazon Redshift serverless, viene creato un utente del database associato e mappato ai ruoli del database corrispondenti. Questo argomento descrive in dettaglio il meccanismo per passare i ruoli ad Amazon Redshift serverless.

Il passaggio dei ruoli del database ha un paio di casi d'uso principali:

- Quando un utente accede tramite un provider di identità di terze parti, in genere con la federazione configurata, e passa i ruoli tramite un tag di sessione.
- Quando un utente accede tramite le credenziali di accesso IAM e i suoi ruoli vengono passati tramite una chiave e un valore di tag.

Per ulteriori informazioni sul controllo degli accessi basato sui ruoli, consulta [Controllo accessi basato sui ruoli \(RBAC\)](#).

## Configurazione dei ruoli del database

Prima di poter passare i ruoli ad Amazon Redshift serverless, è necessario configurare i ruoli del database e concedere loro le autorizzazioni appropriate sulle risorse del database. Ad esempio, in uno scenario semplice, puoi creare un ruolo del database denominato vendite e concedergli l'accesso per eseguire query sulle tabelle con i dati di vendita. Per ulteriori informazioni su come creare ruoli del database e concedere autorizzazioni, consulta [CREATE ROLE](#) e [GRANT](#).

## Casi d'uso per definire i ruoli del database da concedere agli utenti federati

Queste sezioni descrivono un paio di casi d'uso in cui il passaggio dei ruoli del database ad Amazon Redshift serverless può semplificare l'accesso alle risorse del database.

## Accesso tramite un provider di identità

Il primo caso d'uso presuppone che l'organizzazione disponga di identità utente in un servizio Identity and Access Management. Questo servizio può essere basato sul cloud, ad esempio JumpCloud Okta, o locale, come Microsoft Active Directory. L'obiettivo è mappare automaticamente i ruoli di un utente dal provider di identità ai ruoli del database quando, ad esempio, accede a un client l'editor di query V2 o con un client JDBC. Per configurare questo controllo, è necessario completare un paio di attività di configurazione. Questi sono i seguenti:

1. Configurazione dell'integrazione federata con il gestore dell'identità digitale utilizzando una relazione di trust. È un prerequisito. Quando si configura questa impostazione, il provider di identità è responsabile dell'autenticazione dell'utente tramite un'asserzione SAML e della fornitura delle credenziali di accesso. Per ulteriori informazioni, consulta [Integrazione di fornitori di soluzioni SAML di terze parti](#) con AWS. Per ulteriori informazioni, consulta [Federate access to Amazon Redshift query editor V2 with Active Directory Federation Services \(AD FS\)](#) (Accesso federato all'editor di query Amazon Redshift v2 con Active Directory Federation Services (ADFS) o [Federate single sign-on access to Amazon Redshift query editor v2 with Okta](#) (Accesso federato SSO all'editor di query Amazon Redshift v2 con Okta).
2. L'utente deve disporre delle seguenti autorizzazioni delle policy:
  - `GetCredentials`: fornisce le credenziali per l'autorizzazione temporanea all'accesso ad Amazon Redshift serverless.
  - `sts:AssumeRoleWithSAML`— Fornisce un meccanismo per collegare un archivio o una directory di identità aziendali all'accesso basato sui ruoli. AWS
  - `sts:TagSession`: autorizzazione all'operazione della sessione di tag, sul principale del provider di identità.

In questo caso, `AssumeRoleWithSAML` restituisce un set di credenziali di sicurezza per utenti che sono stati autenticati tramite una risposta di autenticazione SAML. Questa operazione fornisce un meccanismo per collegare un archivio di identità o una directory all'accesso basato sui ruoli senza AWS credenziali specifiche dell'utente. Per gli utenti autorizzati per `AssumeRoleWithSAML`, il provider di identità è responsabile della gestione dell'asserzione SAML utilizzata per trasmettere le informazioni sul ruolo.

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

3. Il tag `RedshiftDbRoles` viene configurato con i valori dei ruoli separati da due punti, nel formato `role1:role2`. Ad esempio, `manager:engineer`. Questi possono essere recuperati da un'implementazione di tag di sessione configurata nel provider di identità. La richiesta di autenticazione SAML passa i ruoli a livello di programmazione. Per ulteriori informazioni sul passaggio dei tag di sessione, consulta [Passare i tag di sessione in AWS STS](#).

Nel caso in cui si passi un nome di ruolo che non esiste nel database, questo viene ignorato.

In questo caso d'uso, quando un utente accede utilizzando un'identità federata, i suoi ruoli vengono passati nella richiesta di autorizzazione tramite la chiave e il valore del tag di sessione. Successivamente, dopo l'autorizzazione, `GetCredentials` passa i ruoli al database. Dopo una connessione riuscita, i ruoli del database vengono mappati e l'utente può eseguire attività di database corrispondenti al proprio ruolo. La parte essenziale dell'operazione è che al tag di sessione `RedshiftDbRoles` vengano assegnati i ruoli nella richiesta di autorizzazione iniziale. Per ulteriori informazioni sul passaggio dei tag di sessione, consulta [Passare i tag di sessione utilizzando SAML](#).  
`AssumeRoleWith`

#### Accesso tramite credenziali IAM

Nel secondo caso d'uso, i ruoli possono essere passati per un utente e quest'ultimo può accedere a un'applicazione client del database tramite le credenziali IAM.

1. In questo caso, all'utente che accede devono essere assegnate le autorizzazioni delle policy per le seguenti operazioni:
  - `tag:GetResources`: restituisce le risorse contrassegnate associate ai tag specificati.
  - `tag:GetTagKeys`: restituisce le chiavi dei tag attualmente in uso.

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

2. È inoltre necessario concedere le autorizzazioni per accedere al servizio di database, come Amazon Redshift serverless.
3. In questo caso d'uso, configura i valori dei tag per i tuoi ruoli in AWS Identity and Access Management. Puoi scegliere di modificare i tag e creare una chiave di tag chiamata `RedshiftDbRoles` con una stringa di valori del tag di accompagnamento che contiene i ruoli. Ad esempio, `manager:engineer`.

Quando un utente effettua l'accesso, il suo ruolo viene aggiunto alla richiesta di autorizzazione e passato al database. È mappato a un ruolo del database esistente.

## Risorse aggiuntive

Come indicato nei casi d'uso, è possibile configurare la relazione di trust tra il proprio IdP e AWS. Per ulteriori informazioni, consulta [Configurazione del provider di identità SAML 2.0 con una relazione di attendibilità e aggiungendo attestazioni](#).

## Identity and Access Management in Amazon Redshift Serverless

L'accesso ad Amazon Redshift richiede credenziali che AWS possono essere utilizzate per autenticare le tue richieste. Tali credenziali devono disporre delle autorizzazioni per accedere a AWS risorse, come Amazon Redshift Serverless.

Le seguenti sezioni forniscono dettagli su come utilizzare AWS Identity and Access Management (IAM) e Amazon Redshift per proteggere le risorse controllando chi può accedervi. Per ulteriori informazioni, consulta [Identity and Access Management in Amazon Redshift](#).

## Concessione delle autorizzazioni ad Amazon Redshift Serverless

Per accedere ad altri AWS servizi, Amazon Redshift Serverless richiede autorizzazioni.

### Autorizzazione di Amazon Redshift Serverless ad accedere ad altri servizi AWS per te

Alcune funzionalità di Amazon Redshift richiedono che Amazon Redshift acceda ad AWS altri servizi per tuo conto. Affinché la tua istanza Amazon Redshift Serverless agisca per te, fornisci le credenziali di sicurezza. Il metodo preferito per fornire le credenziali di sicurezza consiste nello specificare un ruolo AWS Identity and Access Management (IAM). Puoi anche creare un ruolo IAM tramite la console Amazon Redshift e impostarlo come predefinito. Per ulteriori informazioni, consulta [Creazione di un ruolo IAM come predefinito per Amazon Redshift](#).

Per accedere ad altri AWS servizi, crea un ruolo IAM con le autorizzazioni appropriate. Devi anche associare il ruolo ad Amazon Redshift Serverless. Inoltre, specificare l'Amazon Resource Name (ARN) del ruolo quando esegui il comando Amazon Redshift oppure specificare la parola chiave `default`.

Quando modifichi la relazione di trust per il ruolo IAM in <https://console.aws.amazon.com/iam/>, assicurati che contenga `redshift-serverless.amazonaws.com` e `redshift.amazonaws.com`

come nomi di servizio principali. Per informazioni su come gestire i ruoli IAM per accedere ad altri AWS servizi per tuo conto, consulta [Autorizzazione di Amazon Redshift ad accedere ad AWS altri servizi per tuo conto](#).

## Creazione di un ruolo IAM come predefinito per Amazon Redshift

Quando crei ruoli IAM tramite la console Amazon Redshift, Amazon Redshift crea programmaticamente i ruoli nel tuo Account AWS Amazon Redshift inoltre allega automaticamente le policy AWS gestite esistenti. Questo approccio significa che puoi rimanere all'interno della console Amazon Redshift senza dover passare alla console IAM per la creazione di ruoli.

Il ruolo IAM creato tramite la console per il cluster ha la policy `AmazonRedshiftAllCommandsFullAccess` gestita allegata automaticamente. Questo ruolo IAM consente ad Amazon Redshift di copiare, scaricare, interrogare e analizzare i dati alla ricerca di AWS risorse nel tuo account IAM. I comandi correlati includono COPY, UNLOAD, CREATE EXTERNAL FUNCTION, CREATE EXTERNAL TABLE, CREATE EXTERNAL SCHEMA, CREATE MODEL e CREATE LIBRARY. Per ulteriori informazioni su come creare un ruolo IAM come predefinito per Amazon Redshift, consultare [Creazione di un ruolo IAM come predefinito per Amazon Redshift](#).

Per iniziare a creare un ruolo IAM come predefinito per Amazon Redshift, apri AWS Management Console, scegli la console Amazon Redshift, quindi scegli Redshift Serverless nel menu. Dalla dashboard Serverless puoi creare un nuovo gruppo di lavoro. I passaggi di creazione ti guidano nella selezione di un ruolo IAM o nella configurazione di un nuovo ruolo IAM.

Se disponi di un gruppo di lavoro Amazon Redshift Serverless esistente e desideri configurare i ruoli IAM per esso, apri il AWS Management Console. Scegli la console Amazon Redshift, quindi scegli Redshift Serverless. Sulla console Amazon Redshift Serverless, scegli la configurazione Namespace per un gruppo di lavoro esistente. In Sicurezza e crittografia, puoi modificare le autorizzazioni.

## Assegnazione di ruoli IAM a uno spazio dei nomi

Ogni ruolo IAM è un'AWS identità con politiche di autorizzazione che determinano le azioni in cui ciascun ruolo può eseguire. AWS Il ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Inoltre, ogni spazio dei nomi è una raccolta di oggetti come tabelle e schemi e utenti. Quando usi Amazon Redshift Serverless, puoi associare più ruoli IAM al tuo spazio dei nomi. In questo modo è più facile strutturare le autorizzazioni in modo appropriato per una raccolta di oggetti di database, in modo che i ruoli possano eseguire azioni sia su dati interni che esterni. Ad esempio, puoi eseguire un comando COPY in un database Amazon Redshift per recuperare i dati da Amazon S3 e popolare una tabella Redshift.

È possibile associare più ruoli a uno spazio dei nomi utilizzando la console, come descritto in precedenza in questa sezione. Inoltre puoi utilizzare l'interfaccia a riga di comando (CLI) `create-namespace` o l'API `CreateNamespace`. Con il comando API o CLI, è possibile assegnare ruoli IAM allo spazio dei nomi popolando `IAMRoles` con uno o più ruoli. In particolare, aggiungi ARN per ruoli specifici alla raccolta.

### Gestione dei ruoli IAM associati allo spazio dei nomi

Su AWS Management Console puoi gestire le politiche di autorizzazione per i ruoli in AWS Identity and Access Management. È possibile gestire ruoli IAM per lo spazio dei nomi, utilizzando le impostazioni disponibili sotto Configurazione dello spazio dei nomi. Per ulteriori informazioni sugli spazi dei nomi e sul loro utilizzo in Amazon Redshift Serverless, consulta [Panoramica dei gruppi di lavoro di Amazon Redshift Serverless](#).

## Nozioni di base sulle credenziali IAM per Amazon Redshift

Quando accedi alla console Amazon Redshift per la prima volta e provi Amazon Redshift Serverless, ti consigliamo di accedere come utente con un ruolo IAM collegato alle policy richieste. Quando si inizia a creare un'istanza Amazon Redshift Serverless, Amazon Redshift registra il nome del ruolo IAM utilizzato al momento dell'accesso. Puoi utilizzare le stesse credenziali per accedere alla console Amazon Redshift e alla console Amazon Redshift Serverless.

Durante la creazione dell'istanza di Amazon Redshift Serverless, è possibile creare un database. Utilizzare l'editor di query v2 per connettersi al database con l'opzione credenziali temporanee.

Per aggiungere un nuovo nome utente e password amministratore che persistono per il database, scegliere Personalizzazione delle credenziali utente amministratore e inserire un nuovo nome utente amministratore e password utente amministratore.

Per iniziare a utilizzare Amazon Redshift Serverless e creare per la prima volta un gruppo di lavoro e uno spazio dei nomi nella console, utilizza un ruolo IAM con una policy di autorizzazioni collegata. Assicurati che il ruolo disponga dell'autorizzazione di amministratore `arn:aws:iam::aws:policy/AdministratorAccess` o dell'autorizzazione completa di Amazon Redshift `arn:aws:iam::aws:policy/AmazonRedshiftFullAccess` collegata alla policy IAM.

Gli scenari seguenti illustrano come le credenziali IAM vengono utilizzate da Amazon Redshift Serverless quando si inizia a utilizzare la console di Amazon Redshift Serverless:

- Se si sceglie Usa impostazioni predefinite – Amazon Redshift Serverless traduce la tua attuale identità IAM in un utente con privilegi avanzati del database. È possibile utilizzare la stessa identità

IAM con la console di Amazon Redshift Serverless per eseguire azioni di utente con privilegi avanzati nel database in Amazon Redshift Serverless.

- Se si sceglie Personalizzazione delle impostazioni senza specificare Nome utente amministratore e password di Amazon Redshift Serverless le credenziali IAM correnti vengono utilizzate come credenziali utente amministratore predefinite.
- Se si sceglie Personalizzazione delle impostazioni e si specifica Nome utente amministratore e password di Amazon Redshift Serverless – Amazon Redshift Serverless traduce la tua attuale identità IAM in un utente con privilegi avanzati del database. Amazon Redshift Serverless crea anche un'altra coppia di nome utente e password di accesso a lungo termine anche come utente con privilegi avanzati. È possibile utilizzare l'identità IAM corrente o la coppia di nome utente e password creata per accedere al database come utente con privilegi avanzati.

## Gestione dell'accesso agli oggetti del database Amazon Redshift Serverless con autorizzazioni relative ai ruoli del database

Questa procedura mostra come concedere l'autorizzazione per interrogare una tabella tramite un [Ruolo del database Amazon Redshift](#). Il ruolo viene assegnato tramite un tag associato a un utente in IAM e passato ad Amazon Redshift al momento dell'accesso. È una spiegazione con l'esempio dei concetti in [Definizione dei ruoli del database da concedere agli utenti federati in Amazon Redshift Serverless](#). Il vantaggio di completare questi passaggi è che è possibile associare un utente a un ruolo del database ed evitare di impostarne le autorizzazioni per ogni oggetto del database. Semplifica la gestione della capacità dell'utente di interrogare, modificare o aggiungere dati alle tabelle e di eseguire altre azioni.

La procedura presuppone che tu abbia già configurato un database Amazon Redshift Serverless e che tu abbia la possibilità di concedere autorizzazioni nel database. Presuppone inoltre che tu disponga delle autorizzazioni per creare un utente IAM nella AWS console, per creare un ruolo IAM e per assegnare le autorizzazioni relative alle policy.

1. Per creare un utente IAM utilizzando la console IAM Successivamente, ti conatterai al database con questo utente.
2. Crea un ruolo del database Redshift, utilizzando l'editor di query v2 o un altro client SQL. Per ulteriori informazioni sulla creazione di ruoli del database, consulta [CREATE ROLE](#).

```
CREATE ROLE urban_planning;
```

Interroga la visualizzazione del sistema [SVV\\_ROLES](#) per verificare che il ruolo sia stato creato. Restituisce anche i ruoli di sistema.

```
SELECT * from SVV_ROLES;
```

3. Concedi al ruolo del database che hai creato l'autorizzazione per la selezione da una tabella. L'utente IAM che hai creato alla fine accederà e selezionerà i record dalla tabella tramite il ruolo del database. Il nome del ruolo e il nome della tabella nell'esempio di codice seguente sono esempi. Qui, viene concessa l'autorizzazione per la selezione da una tabella denominata `cities`.

```
GRANT SELECT on TABLE cities to ROLE urban_planning;
```

4. Usa la AWS Identity and Access Management console per creare un ruolo IAM. Questo ruolo concede il permesso di utilizzare l'editor di query v2. Crea un nuovo ruolo IAM e, per il tipo di entità affidabile, scegli AWS account. Quindi scegli Questo account. Assegna al ruolo le seguenti autorizzazioni di policy:
  - AmazonRedshiftReadOnlyAccess
  - tag:GetResources
  - tag:GetTagKeys
  - Tutte le azioni per `sqlworkbench`, include `sqlworkbench:ListDatabases` e `sqlworkbench:UpdateConnection`.
5. Nella console IAM, aggiungi un tag con Chiave `RedshiftDbRoles` all'utente IAM che hai creato in precedenza. Il valore del tag deve corrispondere al ruolo del database creato nel primo passaggio. È `urban_planning` nell'esempio.

Dopo aver completato questi passaggi, assegna il ruolo IAM all'utente che hai creato nella console IAM. Quando l'utente accede al database con l'editor di query v2, il nome del ruolo del database nel tag viene passato ad Amazon Redshift e associato a lui. Pertanto, possono interrogare le tabelle appropriate tramite il ruolo del database. Per illustrare, l'utente in questo esempio può interrogare la tabella `cities` attraverso il ruolo del database `urban_planning`.

# Migrazione di un cluster con provisioning ad Amazon Redshift Serverless

Per eseguire la migrazione da un cluster con provisioning ad Amazon Redshift Serverless, completa la seguente procedura.

## Creazione di uno snapshot del cluster con provisioning

Per trasferire i dati dal cluster con provisioning ad Amazon Redshift Serverless, crea uno snapshot del cluster, quindi ripristina lo snapshot in Amazon Redshift Serverless. Amazon Redshift converte automaticamente le chiavi interlacciate in chiavi composte quando si ripristina uno snapshot di cluster con provisioning in uno spazio dei nomi serverless.

### Note

Prima di migrare i dati verso un gruppo di lavoro serverless, assicurati che le esigenze del cluster sottoposto a provisioning siano compatibili con la quantità di RPU scelta in Amazon Redshift Serverless.

## Creazione di uno snapshot del cluster con provisioning

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Clusters (Cluster), Snapshots (Snapshot), quindi scegli Create snapshot (Crea snapshot).
3. Inserisci le proprietà della definizione dello snapshot, quindi scegli Create snapshot (Crea snapshot). La disponibilità dello snapshot potrebbe richiedere del tempo.

Per ripristinare uno snapshot cluster con provisioning in uno spazio dei nomi serverless:

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Avvia la console del cluster con provisioning Amazon Redshift e passa alla pagina Clusters (Cluster), Snapshots (Snapshot).
3. Scegliere uno snapshot da utilizzare.

4. Scegli Ripristina da snapshot (Restore snapshot), Restore to serverless namespace (Ripristina su spazio dei nomi serverless).
5. Scegli uno spazio dei nomi in cui ripristinare lo snapshot.
6. Conferma di voler eseguire il ripristino dallo snapshot. Questa azione sostituisce tutti i database dell'endpoint serverless con i dati del cluster sottoposto a provisioning. Scegli Restore (Ripristina).

Per ulteriori informazioni sugli snapshot del cluster con provisioning, consulta [Snapshot di Amazon Redshift](#).

## Connessione ad Amazon Redshift serverless usando un driver

Per connetterti all'endpoint Amazon Redshift Serverless con il client SQL preferito, puoi utilizzare il driver JDBC versione 2 fornito da Amazon Redshift. Consigliamo di connetterti utilizzando il driver JDBC versione 2.1.x o successiva. Il numero di porta è facoltativo. Se non lo includi, Amazon Redshift Serverless utilizzerà il numero di porta 5439. È possibile passare a un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215. Per modificare la porta predefinita per un endpoint serverless, utilizza la AWS CLI e l'API Amazon Redshift.

Per trovare l'endpoint esatto da utilizzare per il driver JDBC, ODBC o Python, consulta Configurazione del gruppo di lavoro in Amazon Redshift serverless. Puoi anche utilizzare l'operazione API Serverless di Amazon Redshift GetWorkgroup o l'AWS CLI operazione `get-workgroups` per restituire informazioni sul tuo gruppo di lavoro e quindi connetterti.

## Connessione tramite autenticazione basata su password

Per connetterti tramite l'autenticazione basata su password, utilizza la sintassi seguente.

```
jdbc:redshift://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439/?username=enter a username&password=enter a password
```

Per connettersi tramite il driver Python di Amazon Redshift, utilizzare la sintassi seguente.

```
import redshift_connector
with redshift_connector.connect(
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com',
```

```
database='<database-name>',
user='enter a user',
password='enter a password'
# port value of 5439 is specified by default
) as conn:
    pass
```

## Connessione tramite IAM

Se preferisci accedere con IAM, usa il seguente endpoint del driver. Questo endpoint del driver ti consente di connetterti a un database specifico e utilizza l'operazione API [GetCredentials](#) di Amazon Redshift Serverless.

```
jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com:5439/<database-name>
```

Questo endpoint del driver non supporta la personalizzazione di `dbUser`, `dbGroup` e `auto-create`. Per impostazione predefinita, il driver crea automaticamente gli utenti del database all'accesso e li assegna ai gruppi in base ai gruppi definiti in IAM. Nota: i nomi dei gruppi che specifichi in IAM devono contenere solo lettere minuscole, numeri, carattere di sottolineatura (`_`), segno più (`+`), punto (`.`), chiocciola (`@`) o trattino (`-`). In caso contrario, il driver potrebbe non connettersi a `dbGroup`.

Assicurati che la tua AWS identità disponga della politica IAM corretta per l'azione.

RedshiftServerlessGetCredentials Di seguito è riportato un esempio di policy IAM che concede le autorizzazioni corrette a un' AWS identità per connettersi ad Amazon Redshift Serverless. Per ulteriori informazioni sulle autorizzazioni IAM, consulta [Aggiunta delle autorizzazioni per le identità IAM](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": "*"
    }
  ]
}
```

## Connessione tramite IAM con dbUser e dbGroups

Se desideri utilizzare opzioni di connessione dbUser e dbGroups personalizzate, utilizza il seguente endpoint del driver. Analogamente all'altro endpoint del driver di Amazon Redshift Serverless, questa sintassi crea automaticamente gli utenti del database al momento dell'accesso. Questo endpoint del driver utilizza l'operazione API [GetCredentials](#) di Amazon Redshift serverless. dbUser deve iniziare con una lettera, deve contenere un massimo di 128 caratteri, tra cui caratteri alfanumerici, carattere di sottolineatura (\_), segno più (+), punto (.), chiocciola (@) o trattino (-). dbGroups deve contenere solo lettere minuscole, carattere di sottolineatura (\_), segno più (+), punto (.), chiocciola (@) o trattino (-).

```
jdbc:redshift:iam://redshift-serverless-<workgroup-name>:<aws-region>/<database-name>
```

Per connettersi tramite il driver Python di Amazon Redshift, utilizzare la sintassi seguente.

```
import redshift_connector
with redshift_connector.connect(
    iam=True,
    host='<workgroup-name>.<account-number>.<aws-region>.redshift-
serverless.amazonaws.com',
    database='<database-name>',
    db_user='enter a user',
    password='enter a password',
    db_groups='<db-groups>'
    # port value of 5439 is specified by default
) as conn:
    pass
```

## Connessione tramite ODBC

Per connetterti tramite ODBC, utilizza la sintassi seguente.

```
Driver={Amazon Redshift (x64)}; Server=<workgroup-name>.<account-number>.<aws-
region>.redshift-serverless.amazonaws.com; Database=dev
```

## Utilizzo dell'SDK di Amazon Redshift Serverless

Se l'utente ha scritto script di gestione utilizzando l'SDK di Amazon Redshift, è necessario utilizzare il nuovo SDK per gestire l'istanza e le risorse di Amazon Redshift serverless. Per ulteriori informazioni

sulle operazioni API disponibili, consulta [Documentazione di riferimento delle API di Amazon Redshift Serverless](#).

## Panoramica dei gruppi di lavoro di Amazon Redshift Serverless

Per isolare i carichi di lavoro e gestire diverse risorse in Amazon Redshift Serverless, puoi creare namespace e gruppi di lavoro e gestire separatamente le risorse di storage e calcolo.

### Panoramica dei gruppi di lavoro di Amazon Redshift Serverless

Lo spazio dei nomi è una raccolta di oggetti di database e utenti. Lo spazio dei nomi relativo allo storage raggruppa schemi, tabelle, utenti o chiavi per la crittografia dei dati. AWS Key Management Service Le proprietà di archiviazione includono il nome e la password del database dell'utente amministratore, le autorizzazioni, la crittografia e la sicurezza. Altre risorse raggruppate in namespace includono datashares, punti di ripristino e limiti di utilizzo. Puoi configurare queste proprietà di storage utilizzando la console Amazon Redshift Serverless o le AWS Command Line Interface API Amazon Redshift Serverless per la risorsa specifica.

Workgroup è una raccolta di risorse di calcolo. I gruppi di lavoro correlati al computer insieme elaborano risorse come RPU, gruppi di subnet VPC e gruppi di sicurezza. Le proprietà per il gruppo di lavoro includono le impostazioni di rete e di sicurezza. Altre risorse raggruppate in gruppi di lavoro includono limiti di accesso e utilizzo. Puoi configurare queste proprietà di calcolo utilizzando la console Amazon Redshift Serverless o AWS Command Line Interface le API Amazon Redshift Serverless.

È possibile creare uno o più spazi dei nomi e gruppi di lavoro. A ogni spazio dei nomi può essere associato un solo gruppo di lavoro. Al contrario, ogni gruppo di lavoro può essere associato a un solo spazio dei nomi.

### Inizia a usare Amazon Redshift Serverless con la console.

La configurazione di Amazon Redshift Serverless comporta la procedura di configurazione. Quando segui i passaggi per configurare Amazon Redshift Serverless, crei uno spazio dei nomi e un gruppo di lavoro e li associi tra loro. Per iniziare a impostare la configurazione di Amazon Redshift Serverless utilizzando la console Amazon Redshift Serverless, puoi scegliere Nozioni di base su Amazon Redshift Serverless per configurare Amazon Redshift Serverless e iniziare a interagire con esso. È possibile scegliere un ambiente con impostazioni predefinite, che rende più rapida la configurazione o configurare esplicitamente le impostazioni in base ai requisiti dell'organizzazione. Durante questo processo, si specificano le impostazioni per il gruppo di lavoro e lo spazio dei nomi.

Dopo aver configurato l'ambiente, [Proprietà del gruppo di lavoro](#) e [Proprietà degli spazi dei nomi](#) aiutano a familiarizzare con le impostazioni.

## Gestione di gruppi di lavoro e namespace utilizzando l'API Serverless di Amazon AWS Command Line Interface Redshift

Oltre a utilizzare la AWS console, puoi anche utilizzare l' AWS CLI API Serverless di Amazon Redshift per interagire con gruppi di lavoro e namespace. La tabella seguente elenca le operazioni API e della CLI che è possibile usare per gestire snapshot e punti di ripristino.

Operazione API	Comando CLI	Descrizione
<a href="#">CreateNamespace</a>	create-namespace	Crea uno spazio dei nomi. Per impostazione predefinita, Amazon Redshift Serverless crea namespace con una AWS Key Management Service chiave predefinita, ma puoi specificare un'altra chiave per crittografare i dati. Puoi anche creare uno spazio dei nomi ripristinando uno snapshot. Per ulteriori informazioni, consulta <a href="#">Utilizzo di snapshot e punti di ripristino</a> .
<a href="#">UpdateNamespace</a>	update-namespace	Aggiorna uno spazio dei nomi.
<a href="#">GetNamespace</a>	get-namespace	Recupera le informazioni su uno spazio dei nomi.
<a href="#">ListNamepaces</a>	list-namespaces	Recupera le informazioni su un elenco di spazi dei nomi.
<a href="#">DeleteNamespace</a>	delete-namespace	Elimina uno spazio dei nomi.
<a href="#">CreateWorkgroup</a>	create-workgroup	Crea un gruppo di lavoro. Quando crei un gruppo di

Operazione API	Comando CLI	Descrizione
		lavoro, assicurati di avere uno spazio dei nomi da associare al gruppo di lavoro. Quando crei il gruppo di lavoro, puoi specificare le risorse di calcolo come sottoreti, gruppi di sicurezza e RPU.
<a href="#">UpdateWorkgroup</a>	update-workgroup	Aggiorna un gruppo di lavoro.
<a href="#">GetWorkgroup</a>	get-workgroup	Recupera le informazioni su un gruppo di lavoro.
<a href="#">ListWorkgroups</a>	list-workgroups	Recupera le informazioni su un elenco di gruppi di lavoro.
<a href="#">DeleteWorkgroup</a>	delete-workgroup	Elimina un gruppo di lavoro.

## Gestione di Amazon Redshift serverless tramite la console

Per creare, modificare ed eliminare un data warehouse Amazon Redshift serverless, utilizza l'opzione serverless dashboard (Pannello di controllo serverless) sulla console Amazon Redshift. L'accesso a singole impostazioni della console dipende dal ruolo IAM e dalle autorizzazioni di cui si dispone.

Per ulteriori informazioni su come configurare Amazon Redshift serverless, consulta [Configurazione di Amazon Redshift serverless per la prima volta](#). Per informazioni sulla creazione e configurazione di gruppi di lavoro, consulta [Utilizzo con gruppi di lavoro](#). Per informazioni sulla configurazione degli spazi dei nomi, consulta [Utilizzo degli spazi dei nomi](#).

## Configurazione di Amazon Redshift Serverless per la prima volta

La prima volta che selezioni l'opzione serverless dashboard (Pannello di controllo serverless) devi seguire la procedura per configurare Amazon Redshift serverless. In Get started with the serverless experience (Inizia a usare l'esperienza serverless) puoi creare un data warehouse Amazon Redshift serverless utilizzando un set di dati di esempio. Amazon Redshift serverless carica automaticamente il set di dati di esempio durante il processo di creazione. È possibile eseguire una query sui dati

subito dopo la creazione del data warehouse. [Per ulteriori informazioni su come configurare Amazon Redshift Serverless per la prima volta, consulta Redshift Serverless.](#)

## Utilizzo con gruppi di lavoro

Per isolare i carichi di lavoro e gestire risorse in Amazon Redshift serverless, puoi creare gruppi di lavoro e spazi dei nomi. I gruppi di lavoro correlati al calcolo insieme elaborano risorse come RPU e gruppi di sottoreti VPC. Se non hai creato un gruppo di lavoro o uno spazio dei nomi e cerchi istruzioni su come iniziare a usare Amazon Redshift serverless, consulta [Configurazione di Amazon Redshift serverless per la prima volta.](#)

### Creazione di un gruppo di lavoro con uno spazio dei nomi

Questa procedura presuppone che sia stata completata la configurazione iniziale di Amazon Redshift serverless. Se non hai creato un gruppo di lavoro o uno spazio dei nomi e cerchi istruzioni su come iniziare a usare Amazon Redshift serverless, consulta [Configurazione di Amazon Redshift serverless per la prima volta.](#)

Attieniti alla seguente procedura per creare un gruppo di lavoro:

1. Scegli serverless dashboard (Pannello di controllo serverless). Seleziona Create workgroup (Crea gruppo di lavoro).
2. Inserisci il nome del gruppo di lavoro.
3. Scegliere una Virtual private cloud (VPC) per Amazon Redshift Serverless. Questo assegna il gruppo di lavoro a una rete virtuale specifica nel tuo ambiente. AWS Per ulteriori informazioni sui VPC, consulta [Panoramica di VPC e sottoreti.](#)
4. Scegli uno o più Gruppi di sicurezza VPC. Per ulteriori informazioni consultare [Controllo del traffico verso le risorse tramite gruppi di sicurezza.](#)
5. In Sottorete, specificare una o più sottoreti da associare al database. Queste sottoreti sono contenute nel VPC scelto in precedenza e devono trovarsi in tre zone di disponibilità distinte. Per ulteriori informazioni, consulta [Considerazioni su quando utilizzare Amazon Redshift Serverless.](#)
6. Seleziona la capacità RPU di base che soddisfa le tue esigenze

### Scelta di uno spazio dei nomi

1. Scegliere Crea un nuovo spazio dei nomi e immettere il nome dello spazio dei nomi, oppure Aggiunta di uno spazio dei nomi esistente e selezionare lo spazio dei nomi dall'elenco a discesa.

2. Per Nome e password del database, specificare il nome del primo database. È inoltre possibile specificare un amministratore diverso dall'amministratore predefinito della console, modificando le Credenziali utente amministratore.
3. Per Autorizzazioni, scegliere Associa il ruolo IAM per associare ruoli IAM specifici allo spazio dei nomi e al gruppo di lavoro. Per ulteriori informazioni sull'associazione dei ruoli IAM ad Amazon Redshift, consultare [Identity and Access Management in Amazon Redshift](#).
4. È possibile personalizzare le impostazioni di crittografia creando una nuova chiave o scegliendo una chiave diversa da quella predefinita. Per Registro di controllo, scegli i log da esportare. Ogni tipo di registro specifica metadati diversi. Scegliere Continua per rivedere le scelte effettuate.

Verificare le selezioni dei gruppi di lavoro

1. Verificare le impostazioni in Rivedi e crea. Mostra le impostazioni scelte nei passaggi precedenti.
2. Selezionare Salva.

Dopo aver creato il gruppo di lavoro, viene aggiunto all'elenco Gruppi di lavoro.

## Creazione di un gruppo di lavoro di anteprima

Per testare le nuove funzionalità di Amazon Redshift serverless., crea un gruppo di lavoro Amazon Redshift serverless in Anteprima. Non è possibile utilizzare queste funzionalità in produzione o trasferire il gruppo di lavoro di anteprima in un gruppo di lavoro di produzione. Per i termini e le condizioni dell'anteprima, consulta la sezione relativa a beta e anteprime nei [termini del servizio AWS](#).

Le seguenti funzionalità non sono attualmente disponibili nei gruppi di lavoro di anteprima:

- [Utilizzo delle integrazioni Zero-ETL](#)

Come creare un gruppo di lavoro di anteprima

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel menu di navigazione, scegli Pannello di controllo serverless e seleziona Configurazione del gruppo di lavoro. Regione AWS Sono elencati i gruppi di lavoro per il tuo account nell'account corrente. Nelle colonne dell'elenco viene mostrato un sottoinsieme delle proprietà di ciascun gruppo di lavoro.

3. Un banner nella pagina Configurazione del gruppo di lavoro presenta i gruppi di lavoro di anteprima. Scegli il pulsante **Create preview workgroup** (Crea gruppo di lavoro di anteprima) per aprire la pagina di creazione del gruppo di lavoro.
4. Inserisci le proprietà del gruppo di lavoro. Consigliamo di assegnare al gruppo di lavoro un nome che indichi che si tratta di un'anteprima. Scegli le opzioni per il gruppo di lavoro, incluse quelle contrassegnate come -anteprima, per le funzionalità che desideri testare. Inserisci le opzioni per il gruppo di lavoro e lo spazio dei nomi all'interno delle varie pagine. Per informazioni generali sulla creazione di gruppi di lavoro, consulta [the section called “Creazione di un gruppo di lavoro con uno spazio dei nomi”](#).
5. Scegli **Crea** per creare un gruppo di lavoro di anteprima.
6. Quando il gruppo di lavoro di anteprima è disponibile, utilizza il client SQL per caricare dati ed eseguire query su di essi.

Per informazioni sull'anteprima nei cluster con provisioning, consulta [Creazione di un cluster di anteprima](#).

## Visualizzazione delle proprietà per un gruppo di lavoro

In Amazon Redshift Serverless, un gruppo di lavoro è una raccolta di risorse disponibili per l'uso. Quando scegli Amazon Redshift Serverless, nella AWS console puoi scegliere la configurazione del gruppo di lavoro dal menu di navigazione per visualizzare un elenco. Puoi utilizzare la casella Cerca per trovare gruppi di lavoro che soddisfano i criteri di ricerca. Ogni voce del gruppo di lavoro ha alcune proprietà visualizzate:

- Gruppo di lavoro: il nome del gruppo di lavoro. È possibile selezionarlo per visualizzare e modificare le proprietà del gruppo di lavoro.
- Stato: mostra se il gruppo di lavoro è disponibile.
- Spazio dei nomi: lo spazio dei nomi associato al gruppo di lavoro. Ogni gruppo di lavoro è associato a uno spazio dei nomi.
- Data di creazione: la data di creazione del gruppo di lavoro.
- Tag: tag associati al gruppo di lavoro.

## Proprietà del gruppo di lavoro

È possibile elencare i gruppi di lavoro scegliendo Configurazione del gruppo di lavoro nel menu a sinistra. Quindi puoi scegliere un gruppo di lavoro dall'elenco. Diversi pannelli mostrano le proprietà

per il gruppo di lavoro. È anche possibile eseguire operazioni. La sezione Informazioni generali mostra quanto segue:

- Gruppo di lavoro: il nome del gruppo di lavoro.
- Spazio dei nomi: lo spazio dei nomi associato al gruppo di lavoro. Puoi sceglierlo per visualizzarne le proprietà. Un gruppo di lavoro è associato a un singolo spazio dei nomi.
- Data di creazione: quando è stato creato il gruppo di lavoro.
- Stato: indica se le risorse del gruppo di lavoro sono disponibili. Se è disponibile, puoi connetterti con un client all'istanza di Amazon Redshift Serverless, per eseguire query sui dati o creare risorse di database oppure connetterti con l'editor di query v2.
- Endpoint: l'URL.
- URL JDBC: l'URL per stabilire le connessioni client JDBC. È possibile utilizzare questo URL per connettersi a un driver JDBC per Amazon Redshift. Per ulteriori informazioni consulta [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).
- URL ODBC: l'URL per stabilire le connessioni client ODBC. Contiene proprietà, come il database e l'ID utente, e i relativi valori.
- Versione del gruppo di lavoro e della patch: Amazon Redshift serverless rilascia regolarmente nuove versioni e patch. Puoi utilizzare i numeri di versione del gruppo di lavoro e della patch per tenere traccia degli aggiornamenti software per il gruppo di lavoro Amazon Redshift serverless. Per ulteriori informazioni sulle modifiche e le funzionalità di patch specifiche, consulta [Versioni dei cluster per Amazon Redshift](#).

La scheda Accesso ai dati contiene diversi pannelli:

- Rete e sicurezza: è possibile visualizzare le proprietà di rete, come ad esempio l'identificatore Cloud privato virtuale (VPC), l'elenco Gruppo di sicurezza VPC, il Routing VPC avanzato e l'impostazione Accessibile pubblicamente. Se scegli Modifica, è possibile modificare tali impostazioni. Inoltre, è possibile selezionare Attiva il routing VPC avanzato, che instrada il traffico di rete tra il database serverless e i repository di dati tramite un VPC, per una maggiore privacy e sicurezza. È possibile anche selezionare Attiva Pubblico Accessibile, che rende il database accessibile pubblicamente dall'esterno del VPC, consentendo la connessione di istanze e dispositivi.
- Endpoint VPC gestiti da Redshift: è possibile creare endpoint VPC gestiti per accedere ad Amazon Redshift Serverless da un altro VPC.

La scheda Limiti dispone di impostazioni per il controllo della capacità e dei limiti di utilizzo per Amazon Redshift Serverless. Contiene i seguenti pannelli:

- Capacità di base nelle unità di elaborazione Redshift (RPU): è possibile impostare la capacità di base delle risorse di calcolo utilizzate per elaborare il carico di lavoro. Per ulteriori informazioni, consulta [Conoscere la capacità di Amazon Redshift Serverless](#).
- Limiti di utilizzo: puoi impostare fino a quattro limiti per il numero massimo di risorse di calcolo che l'istanza Amazon Redshift Serverless può utilizzare in un periodo di tempo e selezionare le azioni che Amazon Redshift serverless esegue al raggiungimento dei limiti. Ad esempio, puoi impostare il gruppo di lavoro in modo che abbia due limiti, uno di 500 ore RPU e uno di 900 ore RPU. Puoi fare in modo che Amazon Redshift serverless invii un avviso quando raggiunge il primo limite di 500 ore RPU e disattivi le query degli utenti quando raggiunge il secondo limite di 900 ore. Questi limiti consentono di controllare i costi rendendoli più prevedibili.
- Limiti delle query: è possibile impostare limiti alle query, come l'impostazione di timeout. Questi limiti consentono di ottimizzare costi e prestazioni.

In Schede è presente il pannello Tag che mostra tutti i tag che hai creato per il gruppo di lavoro. Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta [Panoramica delle risorse di tagging](#).

## Eliminare un gruppo di lavoro

Puoi eliminare un gruppo di lavoro usando la console. Prima di eseguire questa operazione, assicurati di avere backup dei dati e delle snapshot in atto. Le risorse eliminate come parte del gruppo di lavoro in molti casi non possono essere recuperate.

Completa questa procedura:

1. Scegliere Amazon Redshift Serverless, quindi Configurazione del gruppo di lavoro e scegliere Eliminazione dell'istanza Amazon Redshift Serverless.
2. Si aprirà una finestra di dialogo. Quando si sceglie di eliminare il gruppo di lavoro, vengono rimossi tutti i limiti di utilizzo, tutti gli endpoint VPC vengono rimossi e l'accesso agli endpoint VPC viene rimosso.

Digita Elimina e seleziona Elimina per confermare.

Dopo aver completato i passaggi, lo stato del gruppo di lavoro è Eliminazione in corso e il banner indica che è in corso l'eliminazione del gruppo di lavoro. Mentre il processo di eliminazione è in corso, alcune funzionalità nel Dashboard serverless sono disabilitate. Tuttavia, è possibile configurare i cluster con provisioning sul Pannello di controllo dei cluster con provisioning.

Dopo aver eliminato il gruppo di lavoro, non viene visualizzato con lo spazio dei nomi. Puoi scegliere Crea un gruppo di lavoro per crearne uno nuovo.

È possibile eliminare un gruppo di lavoro esistente e associare un nuovo gruppo di lavoro a una configurazione diversa allo stesso spazio dei nomi. Quando si crea il nuovo gruppo di lavoro, scegliere la capacità di base che funziona con le dimensioni dei dati associati allo spazio dei nomi.

È possibile associare un gruppo di lavoro a uno spazio dei nomi creato con una chiave gestita dal cliente (CMK). [Per ulteriori informazioni in merito AWS KMS, consulta i concetti.AWS KMS](#)

## Utilizzo degli spazi dei nomi

In Amazon Redshift Serverless, uno spazio dei nomi definisce un container logico per gli oggetti del database. Può contenere tabelle, gruppi di lavoro e altre risorse di database. Se non hai creato un gruppo di lavoro o uno spazio dei nomi e cerchi istruzioni su come iniziare a usare Amazon Redshift serverless, consulta [Configurazione di Amazon Redshift serverless per la prima volta](#).

### Ricerca di uno spazio dei nomi

Dal menu Amazon Redshift, puoi scegliere dall'elenco Spazi dei nomi per visualizzare o modificare le proprietà di uno spazio dei nomi. Le informazioni sulla console includono il nome dello spazio dei nomi, il nome dell'amministratore e altre proprietà.

Le impostazioni e le proprietà di uno spazio dei nomi sono disponibili in diverse schede. Questi sono i seguenti:

- Gruppo di lavoro: mostra i gruppi di lavoro associati allo spazio dei nomi.
- Backup di dati è possibile configurare e creare snapshot e configurare i punti di ripristino.
- Sicurezza e crittografia: è possibile gestire le autorizzazioni dei ruoli IAM e visualizzare o modificare le impostazioni di sicurezza e crittografia. Questi includono lo stato della chiave di crittografia e le impostazioni di registrazione di controllo.
- condivisione di dati: visualizza le unità di trasmissione dati.

## Proprietà degli spazi dei nomi

In Amazon Redshift Serverless, uno spazio dei nomi definisce un container per gli oggetti del database. È possibile scegliere Configurazione dello spazio dei nomi dall'elenco di navigazione, scegliere uno spazio dei nomi dall'elenco e modificarne le impostazioni.

Le informazioni generali su uno spazio dei nomi includono quanto segue:

- Spazio dei nomi: il nome.
- ID spazio dei nomi: l'identificatore univoco.
- ARN: un identificatore univoco utilizzato per specificare la risorsa trasversale. AWS Contiene proprietà come la regione e il servizio.
- Stato: lo stato, come Disponibilità.
- Data di creazione): la data di creazione dello spazio dei nomi.
- Archiviazione utilizzata: lo spazio di archiviazione utilizzato dallo spazio dei nomi e da tutti i suoi oggetti.
- Nome utente amministratore: l'account amministratore. Questo è in genere l'account utilizzato per creare lo spazio dei nomi.
- Nome del database: il nome del database contenuto nello spazio dei nomi.
- Numero totale di tabelle: il numero di tabelle in tutti gli schemi.

Le impostazioni e le proprietà aggiuntive per lo spazio dei nomi sono disponibili in diverse schede. Questi sono i seguenti:

- Gruppo di lavoro: mostra il gruppo di lavoro associato allo spazio dei nomi.
- Backup di dati: in questo pannello è possibile configurare e creare istantanee e configurare i punti di ripristino.
- Sicurezza e crittografia: è possibile gestire le autorizzazioni dei ruoli IAM e visualizzare o modificare le impostazioni di sicurezza e crittografia. Questi includono lo stato della chiave di crittografia e l'impostazione per attivare la registrazione di controllo. Per ulteriori informazioni sulla registrazione di audit per Amazon Redshift Serverless, consulta [Registrazione di verifiche per Amazon Redshift Serverless](#).
- condivisione di dati: visualizza le unità di trasmissione dati. Con la condivisione dei dati, è possibile fornire accesso ai dati senza la necessità di copiarli o spostarli. Per ulteriori informazioni sulla condivisione dei dati, consulta [Condivisione dei dati in Amazon Redshift Serverless](#).

## Modifica di sicurezza e crittografia

Amazon Redshift serverless è protetto mediante crittografia KMS. Puoi aggiornare le impostazioni di crittografia tramite la console:

1. Scegli Namespace configuration (Configurazione dello spazio dei nomi) dal menu principale della console, seleziona lo spazio dei nomi da modificare e scegli Edit (Modifica) nella scheda Security and encryption (Sicurezza e crittografia). Viene visualizzata una finestra di dialogo.
2. È possibile selezionare Personalizza le impostazioni di crittografia e quindi Scegli una chiave gestita AWS dal cliente per modificare la chiave utilizzata per crittografare le risorse.
3. Per Registro di controllo, scegli i log da esportare. Ogni tipo di registro specifica metadati diversi.
4. Per completare l'aggiornamento della configurazione, scegli Salva le modifiche.

## Modifica della AWS KMS chiave per un namespace

In Amazon Redshift la crittografia protegge i dati a riposo. Amazon Redshift Serverless utilizza automaticamente la crittografia a AWS KMS chiave per crittografare sia le risorse che le istantanee di Amazon Redshift Serverless. Come best practice, la maggior parte delle organizzazioni esamina il tipo di dati archiviati e dispone di un piano per ruotare le chiavi di crittografia secondo una pianificazione. La frequenza delle chiavi rotanti può variare a seconda delle policy di sicurezza dei dati. Amazon Redshift Serverless supporta la modifica della AWS KMS chiave per il namespace in modo da poter rispettare le politiche di sicurezza della tua organizzazione.

Quando si modifica la AWS KMS chiave, i dati rimangono invariati.

### Cambiare una AWS KMS chiave utilizzando la console

In Amazon Redshift la crittografia protegge i dati a riposo. Amazon Redshift Serverless utilizza automaticamente la crittografia a AWS KMS chiave per crittografare sia Amazon Redshift Serverless che le istantanee. Come best practice, la maggior parte delle organizzazioni esamina il tipo di dati archiviati e dispone di un piano per ruotare le chiavi di crittografia secondo una pianificazione. La frequenza delle chiavi rotanti può variare a seconda delle policy di sicurezza dei dati. Amazon Redshift Serverless supporta la modifica della AWS KMS chiave per il namespace in modo da poter rispettare le politiche di sicurezza della tua organizzazione.

Quando si modifica la AWS KMS chiave, i dati rimangono invariati.

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Nel menu di navigazione, scegliere Namespace configurations (Configurazioni spazio dei nomi). Selezionare lo spazio dei nomi dall'elenco.
3. Dalla scheda Sicurezza e crittografia, scegliere Modifica.
4. Scegliere Personalizza impostazioni di crittografia e quindi scegliere una chiave per lo spazio dei nomi. Facoltativamente, puoi creare una nuova chiave.

## Modifica delle chiavi di AWS KMS crittografia utilizzando AWS CLI

Si usa `update-namespace` per cambiare la AWS KMS chiave per il namespace. Di seguito è mostrata la sintassi del comando:

```
aws redshift-serverless update-namespace
--namespace-name
[--kms-key-id <id-of-kms-key>]
// other parameters omitted here
```

È necessario creare uno spazio dei nomi o il comando CLI genera un errore.

Il tempo necessario per cambiare la chiave dipende dalla quantità di dati in Amazon Redshift Serverless. In genere, questo richiede quindici minuti per 8 TB di dati memorizzati.

### Limitazioni

Non è possibile passare da una chiave KMS gestita dal cliente a una chiave AWS KMS. In questo caso, è necessario creare un nuovo spazio dei nomi.

Non è possibile eseguire altre azioni durante la modifica della chiave.

## Eliminazione di uno spazio dei nomi

Se si desidera eliminare uno spazio dei nomi con un gruppo di lavoro associato, è necessario prima eliminare il gruppo di lavoro.

Sulla console di Amazon Redshift Serverless, completare questa procedura:

1. Scegliere Configurazione dello spazio dei nomi dal menu a sinistra e quindi scegli lo spazio dei nomi da eliminare dall'elenco.
2. Scegli Operazioni, quindi Elimina spazio dei nomi.
3. Si aprirà una finestra di dialogo. È possibile conservare i dati creando uno snapshot manuale prima di completare l'operazione di eliminazione.

Digita Elimina e seleziona Elimina per confermare.

## Gestione dei limiti di utilizzo, dei limiti delle query e di altre attività amministrative

È possibile configurare nella console impostazioni per controllare l'utilizzo e limitare i costi.

### Gestione dei limiti di utilizzo, inclusa l'impostazione dei limiti di RPU

Nella scheda Limiti per un gruppo di lavoro, è possibile aggiungere uno o più limiti di utilizzo per controllare le RPU massime utilizzate in un determinato periodo di tempo o per impostare un limite di utilizzo per la condivisione dei dati.

1. Scegliere Gestione dei limiti di utilizzo. La sezione dei limiti viene visualizzata nella parte inferiore del pannello Calcola utilizzo per periodo.
2. Imposta un limite di utilizzo, in numero di ore RPU.
3. Innanzitutto scegli una Frequenza che può essere Giornaliero, Settimanale oppure Mensile. Imposta il periodo di tempo per il limite di utilizzo. Scegliere Giornaliero in questo caso ti dà un controllo più dettagliato.
4. Imposta un limite di utilizzo, in numero di ore.
5. Impostare l'azione. Scegliere tra le seguenti:
  - Accedi alla tabella di sistema: aggiunge un record alla vista di sistema [SYS\\_QUERY\\_HISTORY](#). È possibile interrogare la `usage_limit` colonna in questa vista per determinare se una query ha superato il limite.
  - Avviso: utilizza Amazon SNS per configurare gli abbonamenti alle notifiche e inviare notifiche in caso di violazione di un limite. Puoi scegliere un argomento Amazon SNS esistente o crearne uno nuovo.
  - Disattiva le query utente: disabilita le query per interrompere l'utilizzo di Amazon Redshift Serverless. Inoltre invia una notifica.

Le prime due azioni sono informative, ma l'ultima disattiva l'elaborazione delle query.

6. Eventualmente, è possibile impostare un Limite di utilizzo della condivisione dei dati tra regioni, che limita la quantità di dati trasferiti dalla regione produttore ai consumatori della regione dei consumatori possono interrogare. A questo scopo, scegliere Aggiungi limite e seguire i passaggi.

7. Scegli Salva le modifiche nella parte inferiore della pagina per salvare il limite.
8. Se necessario, imposta gli altri tre limiti.

Per informazioni sulle RPU e sulla fatturazione, consulta [Fatturazione per Amazon Redshift serverless](#).

## Gestione dei limiti delle query

Nella scheda Limits (Limiti) per un gruppo di lavoro, è possibile aggiungere un limite per il monitoraggio delle prestazioni e dei limiti. Per ulteriori informazioni sui limiti di monitoraggio delle query, consulta [Regole di monitoraggio delle query WLM](#).

1. Scegliere Gestione dei limiti delle query. Scegli Add new limit (Aggiungi nuovo limite) nella finestra di dialogo Manage query limits (Gestisci limiti delle query).
2. Scegli il tipo di limite che desideri impostare e inserisci un valore per il limite corrispondente.
3. Per salvare il limite, scegliere Save Changes (Salva modifiche).

Quando modificate il limite di query e i parametri di configurazione, il database verrà riavviato.

## Filtro delle query

È possibile utilizzare i filtri disponibili nel pannello di controllo serverless. Per filtrare le query, procedere nel seguente modo:

1. A sinistra del pannello Riepilogo delle query, selezionare l'elenco a discesa per filtrare le query completate, le query non riuscite o entrambe.
2. A destra del pannello Riepilogo delle query, selezionare l'elenco a discesa per filtrare le query in esecuzione, le query in coda o entrambe.

## Modifica della password di amministratore

1. Scegli Namespace configuration (Configurazione dello spazio dei nomi). Seleziona Change admin password (Modifica password amministratore). Viene visualizzata una finestra di dialogo.
2. Puoi specificare un Nuovo nome utente amministratore e una Nuova password utente amministratore.
3. Selezionare Salva.

## Controllo dei dati di riepilogo di Amazon Redshift serverless utilizzando il pannello di controllo

La dashboard di Amazon Redshift Serverless contiene una raccolta di pannelli che mostrano at-a-glance metriche e informazioni sul gruppo di lavoro e sul namespace. Questi pannelli includono i seguenti:

- Riepilogo risorse: visualizza informazioni di alto livello su Amazon Redshift Serverless, come lo spazio di archiviazione utilizzata e altri parametri.
- Riepilogo delle query - Visualizza informazioni sulle query, incluse le query completate e le query in esecuzione. Scegli View details (Visualizza i dettagli) per accedere a uno schermo con filtri aggiuntivi.
- Capacità RPU utilizzata - Visualizza la capacità complessiva utilizzata in un determinato periodo di tempo, ad esempio nelle dieci ore precedenti.
- Unità di condivisione dati - Mostra il numero di unità di condivisione dati, che vengono utilizzate per condividere i dati tra, ad esempio, account AWS . I parametri mostrano quali unità di condivisione dati richiedono l'autorizzazione e altre informazioni.
- Utilizzo del calcolo totale: mostra le ore RPU totali utilizzate dal gruppo di lavoro selezionato in un intervallo di tempo selezionato, fino agli ultimi 7 giorni.

Dal pannello di controllo è possibile approfondire rapidamente questi parametri disponibili per verificare i dettagli relativi ad Amazon Redshift Serverless, esaminare le query o tenere traccia degli elementi di lavoro.

## Monitoraggio di query e carichi di lavoro con Amazon Redshift Serverless

### Monitoraggio di query e carichi di lavoro con Amazon Redshift Serverless

È possibile monitorare le query di Amazon Redshift Serverless e il carico di lavoro con le visualizzazioni di sistema fornite.

### Concessione dell'accesso alle query di monitoraggio

Un utente con privilegi avanzati può fornire accesso agli utenti che non hanno questi privilegi in modo che possano eseguire il monitoraggio delle query per tutti gli utenti. Per fornire l'accesso al

monitoraggio delle query, è innanzitutto necessario aggiungere una policy per un utente o un ruolo. Quindi, va concessa l'autorizzazione per il monitoraggio delle query all'utente o al ruolo.

### Aggiunta della policy di monitoraggio delle query

1. Scegliere <https://console.aws.amazon.com/iam/>.
2. In Gestione accessi scegli Policy.
3. Scegliere Create Policy (Crea policy).
4. Scegliere la scheda JSON e incollare la seguente definizione di policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift-data:ExecuteStatement",
        "redshift-data:DescribeStatement",
        "redshift-data:GetStatementResult",
        "redshift-data:ListDatabases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": "*"
    }
  ]
}
```

5. Scegli Verifica policy.
6. In Name (Nome), inserire un nome per la policy, ad esempio query-monitoring.
7. Scegli Crea policy.

Dopo aver creato la policy, puoi assegnare le autorizzazioni appropriate.

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- AWS IAM Identity Center Utenti e gruppi in:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creating a role for a third-party identity provider \(federation\)](#) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina [Creating a role for an IAM user](#) (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente di IAM.

### Concessione dell'autorizzazione per il monitoraggio delle query a un utente

Gli utenti con autorizzazione `sys:monitor` possono visualizzare tutte le query. Inoltre, gli utenti con l'autorizzazione `sys:operator` possono cancellare le query, analizzare la loro cronologia ed eseguire operazioni di vacuum.

1. Immettere il seguente comando per fornire l'accesso al monitoraggio del sistema, dove `user-name` è il nome dell'utente per il quale si desidera fornire l'accesso.

```
grant role sys:monitor to "IAM:user-name";
```

2. (Facoltativo) Immettere il seguente comando per fornire l'accesso alle operazioni di sistema, dove `user-name` è il nome dell'utente per il quale si desidera fornire l'accesso.

```
grant role sys:operator to "IAM:user-name";
```

### Concessione dell'autorizzazione per il monitoraggio delle query a un ruolo

Gli utenti con un ruolo con autorizzazione `sys:monitor` possono visualizzare tutte le query. Inoltre, gli utenti con un ruolo che dispone dell'autorizzazione `sys:operator` possono cancellare le query, analizzare la loro cronologia ed eseguire operazioni di vacuum.

1. Immettere il seguente comando per fornire l'accesso al monitoraggio del sistema, dove `role-name` è il nome del ruolo per il quale si desidera fornire l'accesso.

```
grant role sys:monitor to "IAMR:role-name";
```

2. (Facoltativo) Immettere il seguente comando per fornire l'accesso alle operazioni di sistema, dove `role-name` è il nome del ruolo per il quale si desidera fornire l'accesso.

```
grant role sys:operator to "IAMR:role-name";
```

## Viste di monitoraggio

Viste di monitoraggio sono viste di sistema in Amazon Redshift Serverless utilizzate per monitorare l'utilizzo di query e carichi di lavoro. Queste viste sono situate nello schema `pg_catalog`. Le viste di sistema disponibili sono state progettate per fornire le informazioni necessarie per monitorare Amazon Redshift Serverless, che è molto più semplice di quanto necessario per i cluster sottoposti a provisioning. Le viste di sistema SYS sono state progettate per funzionare con Amazon Redshift Serverless. Per visualizzare le informazioni fornite da queste visualizzazioni, eseguire istruzioni SQL `SELECT`.

Le viste di sistema sono definite per supportare i seguenti obiettivi di monitoraggio.

### Monitoraggio del carico di lavoro

È possibile monitorare le attività di query nel corso del tempo per:

- Comprendi i modelli di carico di lavoro, in modo da sapere cosa è normale (baseline) e cosa si trova all'interno degli SLA (Business Service Level Agreements).
- Identifica rapidamente la deviazione dal normale, che potrebbe essere un problema transitorio o qualcosa che giustifichi ulteriori azioni.

### Dati di monitoraggio del carico e dello scarico

Lo spostamento dei dati in entrata e in uscita da Amazon Redshift Serverless è una funzione cruciale. L'utente utilizza `COPY` e `UNLOAD` per caricare o scaricare i dati e monitorare attentamente i progressi in termini di byte/righe trasferite e di file completati per tenere traccia dell'aderenza agli SLA aziendali. Questo viene normalmente fatto eseguendo frequentemente query sulle tabelle di sistema (cioè ogni minuto) per monitorare i progressi e generare avvisi per indagini/azioni correttive se vengono rilevate deviazioni significative.

## Diagnostica guasti e problemi

Esistono casi in cui è necessario intervenire per errori di query o tempo di esecuzione. Gli sviluppatori si affidano alle tabelle di sistema per diagnosticare autonomamente i problemi e determinare i rimedi corretti.

## Ottimizzazione prestazioni

Potrebbe essere necessario ottimizzare le query che non soddisfano i requisiti SLA fin dall'inizio o che sono state degradate nel tempo. Per ottimizzare, è necessario disporre di dettagli di tempo di esecuzione, inclusi piano di esecuzione, statistiche, durata e consumo di risorse. Sono necessari dati di base per le query offensive per determinare la causa della deviazione e offrire una guida su come apportare miglioramenti.

## Monitoraggio eventi oggetti utente

È necessario monitorare le azioni e le attività sugli oggetti utente come l'aggiornamento delle viste materializzate, il vuoto e l'analisi. Ciò include eventi gestiti dal sistema come l'aggiornamento automatico per le viste materializzate. È importante monitorare quando termina un evento se è stato avviato dall'utente o l'ultima esecuzione riuscita se il sistema è stato avviato.

## Tracciamento dell'utilizzo per la fatturazione

Puoi monitorare le tendenze di utilizzo nel tempo per:

- Informare le stime della pianificazione del budget e dell'espansione aziendale.
- Identifica potenziali opportunità di risparmio sui costi, come la rimozione di dati freddi.

Utilizza le viste di sistema SYS per monitorare Amazon Redshift serverless. Per ulteriori informazioni sulle viste di monitoraggio SYS, consulta [Viste di monitoraggio SYS](#).

# Registrazione di verifiche per Amazon Redshift Serverless

## Esportazione dei log

Puoi configurare Amazon Redshift Serverless per esportare i dati di log di connessione, utente e attività degli utenti in un gruppo di log in Amazon Logs. CloudWatch Con Amazon CloudWatch Logs, puoi eseguire analisi in tempo reale dei dati di log e utilizzarli CloudWatch per creare allarmi e visualizzare i parametri. Puoi usare CloudWatch Logs per archiviare i tuoi record di log in uno spazio di archiviazione durevole.

Puoi creare CloudWatch allarmi per tenere traccia delle tue metriche utilizzando la console Amazon Redshift. Per ulteriori informazioni sulla creazione di allarmi, consulta [Gestione degli allarmi](#).

Per esportare i dati di log generati in Amazon CloudWatch Logs, i rispettivi log devono essere selezionati per l'esportazione nelle impostazioni di configurazione di Amazon Redshift Serverless, sulla console. È possibile farlo scegliendo le impostazioni di Configurazione dello spazio dei nomi, in Sicurezza e crittografia.

## Monitoraggio degli eventi di registro in CloudWatch

Dopo aver selezionato i log di Redshift da esportare, puoi monitorare gli eventi in Amazon Logs. CloudWatch Un nuovo gruppo di log viene creato automaticamente per Amazon Redshift serverless, in cui `log_type` rappresenta il tipo di log.

```
/aws/redshift/<namespace>/<log_type>
```

Quando crei il primo gruppo di lavoro e il primo spazio dei nomi, predefinito è il nome dello spazio dei nomi. Il nome del gruppo di log varia in base al nome dello spazio dei nomi.

Ad esempio, se scegli di esportare il log di connessione, i dati di log vengono archiviati nel seguente gruppo di log.

```
/aws/redshift/default/connectionlog
```

Gli eventi di log vengono esportati in un gruppo di log utilizzando il flusso di log serverless. Il comportamento dipende da quale delle seguenti condizioni sono vere:

- Esiste un gruppo di registri con il nome specificato. Redshift esporta i dati di log utilizzando il gruppo di log esistente. Per creare gruppi di log con periodi di conservazione dei log predefiniti, filtri metrici e accesso dei clienti, puoi utilizzare la configurazione automatizzata, come quella fornita da AWS CloudFormation
- Non esiste un gruppo di registri con il nome specificato. Quando viene rilevata una voce di log corrispondente nel log dell'istanza, Amazon Redshift Serverless crea automaticamente un nuovo gruppo di log in Amazon CloudWatch Logs. Il gruppo di log utilizza il periodo di conservazione-log predefinito di Never Expire (Nessuna scadenza). Per modificare il periodo di conservazione dei log, usa la console Amazon CloudWatch Logs, o l' AWS CLI API Amazon CloudWatch Logs. Per ulteriori informazioni sulla modifica dei periodi di conservazione dei log in CloudWatch Logs, consulta [Change log data retention in Working with log groups and log stream](#).

Per cercare informazioni all'interno degli eventi di registro, usa la console Amazon CloudWatch Logs AWS CLI, o l'API Amazon CloudWatch Logs. Per ulteriori informazioni sulla ricerca e l'applicazione di filtri per i dati di log, consultare [Ricerca e filtraggio dei dati di log](#).

## Parametri di Amazon Redshift Serverless

Le metriche serverless di Amazon Redshift sono suddivise in metriche di calcolo e metriche di dati e storage, che rientrano rispettivamente nei set di dimensioni del gruppo di lavoro e dello spazio dei nomi. Per ulteriori informazioni sui gruppi di lavoro e gli spazi dei nomi, consulta [Panoramica dei gruppi di lavoro di Amazon Redshift Serverless](#).

CloudWatch le metriche di calcolo sono le seguenti:

CloudWatch metriche di calcolo

Nome parametro	Unità	Descrizione	Set di dimensioni
QueriesCompletedPerSecond	Numero di query	Il numero medio di query completate al secondo.	{Database LatencyRange, Gruppo di lavoro}, {LatencyRange, Gruppo di lavoro}
QueryDuration	Microsecondi	Il tempo medio necessario per il completamento di una query.	{Database LatencyRange, Gruppo di lavoro}, {LatencyRange, Gruppo di lavoro}
QueriesRunning	Numero di query	Il numero di query in esecuzione in un determinato momento.	{Database QueryType, Gruppo di lavoro}, {QueryType, Gruppo di lavoro}
QueriesQueued	Numero di query	Il numero di query in coda in un determinato momento.	{Database QueryType, Gruppo di lavoro}, {QueryType, Gruppo di lavoro}

Nome parametro	Unità	Descrizione	Set di dimensioni
DatabaseConnections	Numero di connessioni	Il numero di connessioni a un database in un determinato momento.	{Database, gruppo di lavoro}, {Gruppo di lavoro}
QueryRuntimeBreakdown	Millisecondi	Il tempo totale di esecuzione delle query, per fase di query.	{Database, Stage, Gruppo di lavoro}, {Stage, Gruppo di lavoro}
ComputeCapacity	RPU	Numero medio di unità di calcolo allocate negli ultimi 30 minuti, arrotondato al numero intero più vicino.	{Workgroup}
ComputeSeconds	RPU-secondi	Secondi di unità di calcolo accumulati utilizzati negli ultimi 30 minuti.	{Workgroup}
QueriesSucceeded	Numero di query	Il numero di query che sono riuscite negli ultimi 5 minuti.	{Database QueryType, Gruppo di lavoro}, {QueryType e, Gruppo di lavoro}
QueriesFailed	Numero di query	Il numero di query che non sono riuscite negli ultimi 5 minuti.	{Database QueryType, Gruppo di lavoro}, {QueryType e, Gruppo di lavoro}

Nome parametro	Unità	Descrizione	Set di dimensioni
UsageLimitAvailable	Ore RPU o TB	<p>A seconda di UsageType , UsageLimitAvailable restituisce quanto segue:</p> <ul style="list-style-type: none"> <li>• Se UsageType è SERVERLESS_COMPUTE , UsageLimitAvailable restituisce il numero rimanente di ore RPU che il gruppo di lavoro può interrogare entro il limite specificato.</li> <li>• Se UsageType è CROSS_REGION_DATASHARING, UsageLimitAvailable restituisce il numero rimanente di TB che il cliente può scansionare</li> </ul>	{, Gruppo di lavoro} UsageLimitId UsageType

Nome parametro	Unità	Descrizione	Set di dimensioni
		entro il limite specificato.	

Nome parametro	Unità	Descrizione	Set di dimensioni
UsageLimitConsumed	Ore RPU o TB	<p>A seconda di UsageType , UsageLimitConsumed restituisce quanto segue:</p> <ul style="list-style-type: none"> <li>• Se UsageType è SERVERLESS_COMPUTE , UsageLimitConsumed restituisce il numero di ore RPU che il gruppo di lavoro ha già richiesto entro il limite specificato.</li> <li>• Se UsageType è CROSS_REGION_DATASHARING , UsageLimitConsumed restituisce il numero di TB che il cliente ha già utilizzato per la scansione</li> </ul>	{, Gruppo di lavoro} UsageLimitId UsageType

Nome parametro	Unità	Descrizione	Set di dimensioni
		entro il limite specificato.	

CloudWatch le metriche relative ai dati e allo storage sono le seguenti:

CloudWatch metriche relative ai dati e allo storage

Nome parametro	Unità	Descrizione	Set di dimensioni
TotalTableCount	Numero di tabelle	Il numero di tabelle utente esistenti in un particolare momento. Questo totale non include le tabelle di Amazon Redshift Spectrum.	{Database, namespace}
DataStorage	Megabyte	Il numero di megabyte utilizzati, nello spazio su disco o di archiviazione, per i dati Redshift.	{Namespace}

La SnapshotStorage metrica è indipendente dal namespace e dal gruppo di lavoro. CloudWatch la SnapshotStorage metrica è la seguente:

## CloudWatch SnapshotStorage metrica

Nome parametro	Unità	Descrizione	Set di dimensioni
SnapshotStorage	Megabyte	Il numero di megabyte utilizzati, nello spazio su disco o di archiviazione, per Snapshot.	{}

I set di dimensioni sono le dimensioni di raggruppamento applicate ai parametri. È possibile utilizzare questi gruppi di dimensioni per specificare come vengono recuperate le statistiche.

La tabella seguente riporta in dettaglio le dimensioni e i valori delle dimensioni per parametri specifici:

## CloudWatch dimensioni e valori delle dimensioni

Dimensione	Descrizione e valori
DatabaseName	Nome del database. Un valore personalizzato.
Latency	I valori possibili sono i seguenti: <ul style="list-style-type: none"> <li>Breve: meno di 10 secondi</li> <li>Media: tra 10 secondi e 10 minuti</li> <li>Lunga: più di 10 minuti</li> </ul>
QueryType	I valori possibili sono INSERT, DELETE, UPDATE, UNLOAD, LOAD, SELECT, CTAS e OTHER.
stage	Le fasi dell'esecuzione per una query. I valori possibili sono i seguenti: <ul style="list-style-type: none"> <li>QueryPlanning: Tempo impiegato per l'analisi e l'ottimizzazione delle istruzioni SQL.</li> </ul>

Dimensione	Descrizione e valori
	<ul style="list-style-type: none"> <li>• QueryWaiting: Tempo di attesa nella coda WLM.</li> <li>• QueryExecutingRead: Tempo impiegato per l'esecuzione di interrogazioni di lettura.</li> <li>• QueryExecutingInsert: Tempo impiegato per l'esecuzione delle interrogazioni di inserimento.</li> <li>• QueryExecutingDelete: tempo impiegato per l'esecuzione delle interrogazioni di eliminazione.</li> <li>• QueryExecutingUpdate: tempo impiegato per l'esecuzione delle interrogazioni di aggiornamento.</li> <li>• QueryExecutingCtas: tempo impiegato per l'esecuzione della creazione della tabella come query.</li> <li>• QueryExecutingUnload: tempo impiegato per l'esecuzione delle interrogazioni di scaricamento.</li> <li>• QueryExecutingCopy: tempo impiegato per l'esecuzione di interrogazioni di copia.</li> <li>• QueryCommit: tempo impiegato a impegnarsi.</li> </ul>
Namespace	Il nome dello spazio dei nomi. Un valore personalizzato.
Workgroup	Il nome del gruppo di lavoro. Un valore personalizzato.
UsageLimitId	Identificatore del limite di utilizzo.

Dimensione	Descrizione e valori
UsageType	La funzionalità Serverless di Amazon Redshift è limitata. I valori possibili sono i seguenti: <ul style="list-style-type: none"><li>• SERVERLESS_COMPUTING</li><li>• CONDIVISIONE DI DATI CROSS_REGION_</li></ul>

## Utilizzo di snapshot e punti di ripristino

Un backup in Amazon Redshift Serverless è una point-in-time rappresentazione degli oggetti e dei dati nel tuo spazio dei nomi. Esistono due tipi di backup: snapshot creati manualmente e punti di ripristino creati automaticamente da Amazon Redshift serverless. I punti di ripristino vengono creati ogni 30 minuti e conservati per 24 ore.

Se desideri recuperare i dati in uno snapshot o un punto di ripristino, puoi ripristinare lo snapshot in uno spazio dei nomi serverless o in un cluster con provisioning. Sono disponibili tre scenari in cui è possibile ripristinare snapshot:

- Ripristina uno snapshot serverless in uno spazio dei nomi serverless.
- Ripristinare uno snapshot serverless in un cluster con provisioning.
- Ripristina uno snapshot cluster con provisioning in uno spazio dei nomi serverless.

Quando ripristini uno snapshot serverless in un cluster con provisioning, devi scegliere il tipo di nodo da utilizzare, ad esempio RA3, e il numero di nodi, consentendoti di controllare le impostazioni a livello di cluster o nodo.

Per ripristinare uno snapshot cluster con provisioning in uno spazio dei nomi serverless, iniziare dalla console con provisioning di Redshift, scegliere lo snapshot da ripristinare, quindi scegliere Ripristino da snapshot, Ripristino dello spazio dei nomi serverless. Amazon Redshift converte le tabelle con chiavi interlacciate in chiavi di ordinamento composte quando si ripristina uno snapshot di cluster con provisioning in uno spazio dei nomi serverless. Per ulteriori informazioni sulle chiavi di ordinamento, consulta [Utilizzo delle chiavi di ordinamento](#).

Se desideri aggiungere ulteriore contesto, puoi applicare tag a snapshot e a punti di ripristino con coppie chiave-valore che forniscono metadati e informazioni. Per ulteriori informazioni sull'aggiunta di tag alle risorse, consulta [Panoramica delle risorse di tagging](#).

Infine, puoi anche condividere snapshot con altri account AWS, che consente loro di accedere ai dati all'interno dello snapshot ed eseguire query.

## Snapshot

Puoi ripristinare uno snapshot creato sulla console Amazon Redshift Serverless in uno spazio dei nomi disponibile associato a un gruppo di lavoro. Uno spazio dei nomi è disponibile una volta pronto per la query e/o la modifica. È possibile ripristinare uno snapshot crittografato con una chiave KMS gestita da AWS per uno spazio dei nomi serverless.

Per visualizzare un elenco di tutte le snapshot, sulla console di Amazon Redshift Serverless, scegli la console di Amazon Redshift Serverless Backup dei dati.

Per creare una snapshot

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegli Create snapshot (Crea snapshot).
3. Scegli uno spazio dei nomi di cui creare una snapshot.
4. Immetti un identificatore di snapshot.
5. (Facoltativo) Scegli un periodo di conservazione. Se scegli Valore personalizzato, scegli il numero di giorni. L'importo scelto deve essere compreso tra 1-3653 giorni. Il valore predefinito è conservato a tempo indeterminato.
6. Scegli Crea.

Per creare uno snapshot dalla configurazione dello spazio dei nomi

1. Nella console Amazon Redshift Serverless scegli Configurazione dello spazio dei nomi.
2. Scegli lo spazio dei nomi di cui creare una snapshot. È possibile creare solo snapshot di spazi dei nomi associati a un gruppo di lavoro e i cui stati sono disponibili.
3. Seleziona la scheda Backup dei dati.
4. Scegli Create snapshot (Crea snapshot).
5. Immetti un identificatore di snapshot.
6. (Facoltativo) Scegli un periodo di conservazione. Se scegli Valore personalizzato, scegli il numero di giorni. L'importo scelto deve essere compreso tra 1-3653 giorni.
7. Scegli Crea.

## Per aggiornare il periodo di conservazione di un'istantanea

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegliere uno snapshot da aggiornare.
3. Scegliere Operazioni, Imposta le impostazioni manuali dello snapshot.
4. Selezionare un periodo di conservazione. Se scegli Valore personalizzato, scegli il numero di giorni.
5. Seleziona Salvataggio delle modifiche.

## Per eliminare uno snapshot

### Note

Non puoi eliminare un'istantanea che è stata condivisa con un altro account. È necessario rimuovere l'accesso dell'account all'istantanea prima di eliminare l'istantanea.

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegliere uno snapshot da eliminare.
3. Scegliere Actions (Operazioni), Delete (Elimina).
4. Scegliere Delete (Elimina).

Per creare un'istantanea finale di tutti i dati all'interno di uno spazio dei nomi prima di eliminare lo spazio dei nomi.

1. Nella console Amazon Redshift Serverless scegli Configurazione dello spazio dei nomi.
2. Selezionare lo spazio dei nomi da eliminare.
3. Scegli Operazioni > Elimina.
4. Scegliere Creare uno snapshot finale.
5. Inserire un nome per lo snapshot.
6. Immetti delete.
7. Scegli Elimina.

Per condividere un'istantanea con un altro account AWS o rimuovere l'accesso di un account a un'istantanea

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegliere uno snapshot da condividere.
3. Scegliere Operazioni, Gestione degli accessi.
4. Per condividere uno snapshot con un altro account, inserire un Account AWS ID. Per rimuovere l'accesso da un account, scegli Rimuovi.
5. Seleziona Salvataggio delle modifiche.

## Ripristino di uno snapshot

Il ripristino di uno snapshot in uno spazio dei nomi serverless sostituisce il database corrente con il database presente nello snapshot.

Il ripristino di un'istantanea in uno spazio dei nomi serverless viene completato in due fasi. La prima fase viene completata in pochi minuti, ripristina i dati nello spazio dei nomi e li rende disponibili per le query. La seconda fase del ripristino è il punto in cui il database è sintonizzato, il che può causare piccoli problemi di prestazioni. La seconda fase può durare da poche ore a diversi giorni e, in alcuni casi, un paio di settimane. Il tempo dipende dalle dimensioni dei dati. Le prestazioni però migliorano progressivamente con l'ottimizzazione del database. Alla fine di questa fase, lo spazio dei nomi serverless è completamente sintonizzato e puoi inviare query senza problemi di prestazioni.

Per ripristinare una snapshot in uno spazio dei nomi serverless

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegli l'istantanea da ripristinare. È possibile ripristinare un solo snapshot per volta.
3. Scegliere Operazioni, Ripristino dello spazio dei nomi serverless.
4. Scegli uno spazio dei nomi disponibile su cui eseguire il ripristino. È possibile ripristinare solo gli spazi dei nomi i cui stati sono disponibili.
5. Scegli Restore (Ripristina).

Per ripristinare una snapshot in un cluster con provisioning

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegli un'istantanea da ripristinare.

3. Scegliere Operazione, Ripristino sul cluster con provisioning.
4. Digitare l'identificatore del cluster.
5. Selezionare un tipo di nodo. Il numero di nodi dipende dal tipo di nodo.
6. Segui le istruzioni sulla pagina della console per inserire le proprietà della Cluster configuration (Configurazione del cluster). Per ulteriori informazioni, consulta [Creazione di un cluster](#).

Per ulteriori informazioni sugli snapshot dei cluster con provisioning, consulta [Snapshot e backup di Amazon Redshift](#).

## Punti di ripristino

I punti di ripristino in Amazon Redshift serverless vengono creati ogni 30 minuti circa e salvati per 24 ore.

Sulla console di Amazon Redshift Serverless, scegli Backup dei dati per gestire i punti di ripristino. È possibile effettuare le seguenti operazioni:

- Ripristina un punto di ripristino su uno spazio dei nomi serverless.
- Convertire un punto di ripristino in uno snapshot.

Ripristinare un punto di ripristino su uno spazio dei nomi serverless

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. In Punti di ripristino, scegli l'Orario di creazione del punto di ripristino che si desidera ripristinare.
3. Scegli Restore (Ripristina). È possibile ripristinare solo gli spazi dei nomi i cui stati sono disponibili.
4. Inserisci restore (ripristina) nel campo di immissione del testo e scegli Restore (Ripristina).

Convertire un punto di ripristino in uno snapshot

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. In Punti di ripristino, scegli l'Orario di creazione del punto di ripristino che desideri convertire in uno snapshot.
3. Scegli Creazione di snapshot dal punto di ripristino.
4. Immetti un Elemento identificatore snapshot.

## 5. Scegli Crea.

### Pianificazione degli snapshot

Per controllare con precisione quando acquisire uno snapshot, puoi creare la pianificazione degli snapshot per spazi dei nomi specifici. In tal caso, puoi creare un evento una tantum o utilizzare le espressioni cron Unix per creare una pianificazione ricorrente. Le espressioni cron supportano tre campi e sono separati da uno spazio.

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Campi	Valori	Caratteri jolly
Minuti	0-59	, - * /
Ore	0-23	, - * /
Day-of-month	1-31	, - * ? / L W
Mese	1-12 o JAN-DEC	, - * /
Day-of-week	1-7 o SUN-SAT	, - * ? L #
Anno	1970–2199	, - * /

#### Caratteri jolly

- Il carattere jolly , (virgola) include valori aggiuntivi. Nel campo Day-of-week, MON, WED, FRI includono lunedì, mercoledì e venerdì. I valori totali sono limitati a 24 per campo.
- Il carattere jolly - (trattino) specifica gli intervalli. Nel campo Hour, 1-15 include le ore dall'1 alle 15 del giorno specificato.
- Il carattere jolly \* (asterisco) include tutti i valori nel campo. Nel campo Hours, \* include ogni ora.
- Il carattere jolly / (barra) specifica gli incrementi. Nel campo Hours puoi immettere **1/10** per specificare ogni decima ora, a partire dalla prima ora del giorno (ad esempio, 01:00, 11:00 e 21:00).

- Il carattere jolly ? (punto interrogativo) specifica un valore. Nel **Day-of-month** campo puoi inserire 7, e se non ti interessa in che giorno della settimana è il settimo, puoi inserire? nel ay-of-week campo D.
- Il carattere jolly L nel campo Day-of-month o Day-of-week specifica l'ultimo giorno del mese o della settimana.
- Il carattere jolly W nel campo Day-of-month specifica un giorno feriale. Nel campo Day-of-month, 3W specifica il giorno più vicino al terzo giorno feriale del mese.
- Il carattere jolly # nel ay-of-week campo D specifica una determinata istanza del giorno della settimana specificato nell'arco di un mese. Ad esempio, 3#2 sarebbe il secondo martedì del mese: il 3 fa riferimento a martedì perché è il terzo giorno di ogni settimana e il 2 fa riferimento al secondo giorno di questo tipo in un mese.

#### Note

Se si utilizza un carattere '#', è possibile definire solo un'espressione nel day-of-week campo. Ad esempio, "3#1,6#3" non è valido perché viene interpretato come due espressioni.

## Limiti

- Non puoi specificare i campi Day-of-month e Day-of-week nella stessa espressione cron. Se specifichi un valore in uno dei campi, devi usare un carattere ? nell'altro campo.
- Le pianificazioni degli snapshot non supportano le seguenti frequenze:
  - Snapshot pianificati più frequentemente di uno all'ora.
  - Snapshot pianificati meno frequentemente di uno al giorno (24 ore).

Se sono presenti pianificazioni sovrapposte che determinano la pianificazione di snapshot nell'arco di un'ora, viene generato un errore di convalida.

La tabella seguente illustra alcuni esempi di stringhe cron.

Minuti	Ore	Giorno della settimana	Significato
0	14-20/1	TUE	Ogni ora tra le 14:00 e le 20:00 di martedì.
0	21	MON-FRI	Tutte le sere alle 21, dal lunedì al venerdì.
30	0/6	SAT-SUN	Ogni 6 ore di incremento il sabato e la domenica a partire da 30 minuti dopo la mezzanotte (00:30) di quel giorno. Ciò restituisce uno snapshot alle [00:30, 06:30, 12:30 e 18:30] ogni giorno.
30	12/4	*	Ogni 4 ore di incremento a partire dalle 12:30 ogni giorno. Pertanto, il risultato restituito è [12:30, 16:30, 20:30].

L'esempio seguente illustra come creare una pianificazione che viene eseguita ogni giorno in incrementi di 2 ore a partire dalle 15:15.

```
cron(15 15/2 *)
```

Al momento, puoi utilizzare solo l'API Amazon Redshift serverless o la AWS CLI per creare una pianificazione degli snapshot. Per ulteriori informazioni su queste operazioni, consulta [Utilizzo della AWS CLI e dell'API Amazon Redshift serverless](#).

## Copia dei backup in un'altra Regione AWS

Puoi configurare Amazon Redshift serverless per copiare automaticamente snapshot e punti di ripristino in un'altra Regione AWS. Quando crei uno snapshot nella Regione AWS di origine, questo viene copiato in una regione di destinazione. È possibile configurare lo spazio dei nomi in modo che copi solo gli snapshot e i punti di ripristino su una Regione AWS di destinazione alla volta. Per l'elenco delle Regioni AWS in cui Amazon Redshift serverless è disponibile, consulta gli endpoint indicati per l'[API Redshift serverless](#) in Riferimenti generali di Amazon Web Services.

Quando configuri la copia dei backup puoi specificare anche un periodo di conservazione per stabilire per quanto tempo Amazon Redshift serverless deve conservare lo snapshot copiato. Non è possibile modificare i periodi di conservazione dei punti di ripristino, che devono essere di 1 giorno. I periodi di conservazione degli snapshot nella regione di destinazione sono separati dal periodo di conservazione degli snapshot nella regione di origine. Per impostazione predefinita, il periodo di conservazione stabilisce di conservare lo snapshot per un tempo illimitato. Se scegli Valore personalizzato seleziona il numero di giorni. Il valore scelto deve essere compreso tra 1 e 3653 giorni.

Per modificare la regione di destinazione in cui copiare gli snapshot, disabilita innanzitutto la copia dei backup, quindi specifica la nuova regione di destinazione quando riabiliti la copia.

Una volta copiato uno snapshot o un punto di ripristino in una regione di destinazione, è possibile utilizzarlo per ripristinare i dati nella regione.

Per impostazione predefinita, i dati vengono crittografati con una chiave gestita da AWS. Per utilizzare una chiave diversa, scegli la chiave che desideri utilizzare per configurare la copia dei backup nella Regione AWS di origine e Amazon Redshift serverless crea automaticamente un'autorizzazione che abilita la crittografia degli snapshot nella Regione AWS di destinazione.

Per copiare i backup in un'altra regione, assicurati di disporre delle seguenti autorizzazioni IAM:

```
redshift-serverless:CreateSnapshotCopyConfiguration
redshift-serverless:UpdateSnapshotCopyConfiguration
redshift-serverless:ListSnapshotCopyConfigurations
redshift-serverless>DeleteSnapshotCopyConfiguration
```

Se utilizzi la tua chiave KMS per crittografare i backup, hai bisogno anche delle seguenti autorizzazioni:

```
kms:CreateGrant
```

```
kms:DescribeKey
```

Per configurare la copia degli snapshot o dei punti di ripristino in un'altra Regione AWS

1. Sulla console Amazon Redshift serverless scegli lo spazio dei nomi per cui desideri configurare la copia di snapshot o punti di ripristino.
2. Scegli Operazioni, quindi Configurazione del backup tra Regioni.
3. Scegli la Regione AWS di destinazione in cui copiare lo snapshot.
4. (Facoltativo) Scegli per quanto tempo conservare lo snapshot. Se scegli Valore personalizzato seleziona il numero di giorni. Il valore scelto deve essere compreso tra 1 e 3653 giorni. Il periodo di conservazione predefinito stabilisce un tempo illimitato.
5. (Facoltativo) Scegli una chiave AWS KMS diversa da utilizzare per eseguire la crittografia nella regione di destinazione.
6. Seleziona Save configuration (Salva configurazione).

## Ripristino di una tabella

È possibile ripristinare una tabella specifica da uno snapshot o da un punto di ripristino. Per farlo, specifichi lo snapshot o il punto di ripristino di origine, il database, lo schema, la tabella, il database di destinazione, lo schema e il nome della nuova tabella. La nuova tabella non può avere lo stesso nome di una tabella esistente. Per sostituire una tabella esistente con una tabella ripristinata, devi innanzitutto rinominare o rilasciare la tabella esistente prima di ripristinare l'altra tabella.

La tabella di destinazione viene creata usando le definizioni di colonna, gli attributi di tabella e gli attributi di colonna della tabella di origine, a esclusione delle chiavi esterne. Per impedire conflitti dovuti alle dipendenze, la tabella di destinazione non eredita le chiavi estere dalla tabella di origine. Eventuali dipendenze, come viste o autorizzazioni concesse nella tabella di origine, non vengono applicate alla tabella di destinazione.

Se il proprietario della tabella di origine esiste, tale utente diventa il proprietario della tabella ripristinata, a condizione che abbia autorizzazioni sufficienti per diventare il proprietario di una relazione nel database e nello schema specificati. In caso contrario, la tabella ripristinata è di proprietà dell'utente master creato all'avvio del cluster.

La tabella ripristinata torna allo stato in cui si trovava al momento dell'esecuzione del backup. Ciò include le regole di visibilità delle transazioni definite dall'applicazione in Amazon Redshift

dell'[isolamento serializzabile](#), che prevede che i dati siano immediatamente visibili per le transazioni in corso avviate dopo il backup.

Puoi utilizzare la console Amazon Redshift serverless per ripristinare le tabelle da uno snapshot.

Il ripristino di una tabella da un backup di dati prevede le limitazioni seguenti:

- Puoi ripristinare una sola tabella per volta.
- Eventuali dipendenze, come viste o autorizzazioni concesse nella tabella di origine, non vengono applicate alla tabella di destinazione.
- Se la sicurezza a livello di riga è attivata per il ripristino di una tabella, Amazon Redshift serverless ripristina la tabella con la sicurezza a livello di riga attivata.

Per ripristinare una tabella tramite la console Amazon Redshift serverless

1. Sulla console di Amazon Redshift Serverless, scegli Backup dei dati.
2. Scegli lo snapshot o il punto di ripristino che contiene la tabella da ripristinare.
3. Scegli Operazioni, Ripristina tabella da snapshot o Ripristina tabella da punto di ripristino.
4. Inserisci le informazioni sullo snapshot o sul punto di ripristino di origine e sulla tabella di destinazione, quindi scegli Ripristina tabella.

## Utilizzo della AWS Command Line Interface e dell'API Amazon Redshift serverless

Oltre a utilizzare la console AWS, è anche possibile utilizzare AWS CLI o l'API di Amazon Redshift Serverless per interagire con snapshot e punti di ripristino. La tabella seguente elenca le operazioni API e della CLI che è possibile usare per gestire snapshot e punti di ripristino.

Operazione API	Comando CLI	Descrizione
<a href="#">CreateSnapshot</a>	create-snapshot	Crea uno snapshot. Le istantanee devono essere associate a uno spazio dei nomi, pertanto è necessari o includere il nome di uno spazio dei nomi nella richiesta

Operazione API	Comando CLI	Descrizione
		<p>. Per impostazione predefinita, Amazon Redshift serverless conserva gli snapshot per un periodo illimitato, ma puoi specificare un periodo di conservazione.</p>
<a href="#">RestoreFromSnapshot</a>	<code>restore-from-snapshot</code>	<p>Ripristina i database di uno snapshot nello spazio dei nomi. Se esegui il ripristino di uno snapshot da Amazon Redshift Serverless in un cluster con provisioning, devi specificare il parametro <code>snapshotArn</code> per il snapshot che stai ripristinando. In alternativa, se stai eseguendo il ripristino da serverless a serverless, puoi specificare <code>snapshotArn</code> o <code>snapshotName</code>, ma non entrambi.</p>
<a href="#">RestoreTableFromSnapshot</a>	<code>restore-table-from-snapshot</code>	<p>Ripristina una tabella da uno snapshot nello spazio dei nomi Amazon Redshift serverless. Non è possibile utilizzare questa operazione per ripristinare le tabelle con chiavi di ordinamento interleaved.</p>
<a href="#">GetSnapshot</a>	<code>get-snapshot</code>	<p>Recupera le informazioni su uno snapshot.</p>
<a href="#">ListSnapshots</a>	<code>list-snapshots</code>	<p>Recupera le informazioni su più snapshot.</p>

Operazione API	Comando CLI	Descrizione
<a href="#">DeleteSnapshot</a>	delete-snapshot	Elimina uno snapshot.
<a href="#">RestoreFromRecoveryPoint</a>	restore-from-recovery-point	Ripristina i dati di un punto di ripristino nello spazio dei nomi.
<a href="#">RestoreTableFromRecoveryPoint</a>	restore-table-from-recovery-punto	Ripristina una tabella da un punto di ripristino nello spazio dei nomi Amazon Redshift serverless. Non è possibile utilizzare questa operazione per ripristinare le tabelle con chiavi di ordinamento interleaved.
<a href="#">ConvertRecoveryPointToSnapshot</a>	convert-recovery-point-to-instantanea	Converte un punto di ripristino in uno snapshot.
<a href="#">GetRecoveryPoint</a>	get-recovery-point	Recupera le informazioni su un punto di ripristino.
<a href="#">ListRecoveryPoints</a>	list-recovery-points	Recupera le informazioni su più punti di ripristino.

Per pianificare la creazione di snapshot, utilizza le operazioni API seguenti.

Operazione API	Comando CLI	Descrizione
<a href="#">CreateScheduledAction</a>	create-scheduled-action	Crea un'azione pianificata contenente una pianificazione e un'azione Amazon Redshift serverless. Ad esempio, puoi programmare l'esecuzione dell'operazione API <code>CreateSnapshot</code> .

Operazione API	Comando CLI	Descrizione
<a href="#">DeleteScheduledAction</a>	delete-scheduled-action	Elimina un'azione pianificata.
<a href="#">GetScheduledAction</a>	get-scheduled-action	Recupera le informazioni su un'azione pianificata.
<a href="#">ListScheduledActions</a>	list-scheduled-actions	Recupera le informazioni su un elenco di azioni pianificate.
<a href="#">UpdateScheduledAction</a>	update-scheduled-action	Aggiorna un'azione pianificata.

## Condivisione dei dati in Amazon Redshift Serverless

Usa la condivisione dei dati per condividere le informazioni più consistenti up-to-date e coerenti man mano che vengono aggiornate in Amazon Redshift Serverless.

### Condivisione dei dati in Amazon Redshift Serverless

Con la condivisione dei dati, hai accesso in tempo reale ai dati in modo che i tuoi utenti possano vedere le informazioni più consistenti up-to-date e coerenti man mano che vengono aggiornate in Amazon Redshift Serverless.

### Guida introduttiva alla condivisione dei dati in Amazon Redshift Serverless

È possibile condividere i dati a scopo di lettura tra diversi endpoint Amazon Redshift Serverless all'interno o tra un account Account AWS.

È possibile iniziare a condividere i dati utilizzando l'interfaccia SQL o la console Amazon Redshift. Per ulteriori informazioni, consultare [Guida introduttiva alla condivisione dei dati utilizzando l'interfaccia SQL](#) oppure [Informazioni di base sulla condivisione dei dati utilizzando la console](#) nella Guida per sviluppatori di database Amazon Redshift nella Guida per sviluppatori di database Amazon Redshift.

Grazie alla condivisione dei dati, i namespace di Amazon Redshift Serverless e i cluster con provisioning possono condividere dati in tempo reale tra loro, indipendentemente dal fatto che si trovino all'interno o all'esterno. Account AWS Account AWS Regioni AWS Per ulteriori informazioni, consulta [Regioni in cui è disponibile la condivisione dei dati](#).

Per iniziare a condividere dati all'interno di un Account AWS, apri e scegli la console Amazon Redshift. AWS Management Console Scegliere Configurazione spazio dei nomi e poi Unità di condivisione dati. Seguire le procedure indicate in [Informazioni di base sulla condivisione dei dati utilizzando la console](#) nella Guida per sviluppatori di database Amazon Redshift.

Per iniziare a condividere dati Account AWS, apri la console AWS Management Console Amazon Redshift e scegli la console Amazon Redshift. Scegliere Unità di condivisione dati. Seguire le procedure indicate in [Informazioni di base sulla condivisione dei dati utilizzando la console](#) nella Guida per sviluppatori di database Amazon Redshift.

Per iniziare a interrogare i dati in una unità di condivisione dati, creare database in uno spazio dei nomi a cui è associato un gruppo di lavoro. Da una condivisione di dati specificata, scegliere uno spazio dei nomi a cui è associato un gruppo di lavoro e creare un database per interrogare i dati. Seguire le procedure indicate in [Creazione di database da unità di condivisione dati](#).

## Concessione dell'accesso per visualizzare unità di condivisione dati utilizzando la console

Un utente con privilegi avanzati può fornire accesso agli utenti con privilegi inferiori in modo che possano visualizzare le unità di condivisione dati create da tutti gli utenti.

Per fornire l'accesso a un'unità di condivisione dati a un utente, utilizza il seguente comando, in cui `datashare_name` è il nome dell'unità di condivisione dati e `user-name` è il nome dell'utente al quale si desidera fornire l'accesso.

```
grant share on datashare datashare_name to "IAM:test_user";
```

Per fornire l'accesso a un'unità di condivisione dati a un gruppo di utenti, crea innanzitutto un gruppo di utenti. Per informazioni su come creare gruppi di utenti, consulta [CREATE GROUP](#). Quindi, fornisci l'accesso all'unità di condivisione dati a un utente utilizzando il seguente comando, in cui `datashare_name` è il nome dell'unità di condivisione dati e `user-group` è il nome del gruppo di utenti al quale si desidera fornire l'accesso.

```
grant share on datashare datashare_name to group user_group;
```

Per informazioni su come utilizzare l'istruzione GRANT, consulta [GRANT](#).

## Considerazioni sulla condivisione dei dati in Amazon Redshift Serverless

Di seguito sono riportate le considerazioni sull'utilizzo della condivisione dei dati in Amazon Redshift Serverless:

- Amazon Redshift supporta solo cluster con provisioning di istanze di tipo ra3.16xlarge, ra3.4xlarge e ra3.xlplus ed endpoint serverless come producer e consumer per la condivisione dei dati.
- Amazon Redshift Serverless

Per un elenco delle limitazioni delle unità di condivisione dati, inclusi gli oggetti di database supportati, i requisiti di crittografia e i requisiti delle chiavi di ordinamento, consulta [Considerazioni sull'utilizzo della condivisione dei dati in Amazon Redshift](#) nella Guida per sviluppatori di database di Amazon Redshift.

## Panoramica delle risorse di tagging

In AWS, i tag sono etichette definite dall'utente costituite da coppie chiave-valore. Amazon Redshift Serverless supporta l'assegnazione di tag per fornire i metadati sulle risorse in modo immediato.

I tag non sono obbligatori per le risorse, ma sono utili per fornire il contesto. È possibile applicare tag alle risorse con metadati con informazioni correlate alla risorsa. Supponi, ad esempio, di voler tenere traccia delle risorse che appartengono a un ambiente di test e di quelle che appartengono a un ambiente di produzione. Puoi creare un ambiente chiave denominato e specificare il valore o per identificare le risorse usate in ogni ambiente. Se usi il tagging in altri servizi AWS o nella tua azienda vengono usate categorie standard, per coerenza è consigliabile creare le stesse coppie chiave-valore per le risorse.

Se elimini una risorsa, i tag associati vengono eliminati. Puoi utilizzare sia l'AWS CLI e la console di Amazon Redshift Serverless per applicare tag alle risorse serverless. Le operazioni API disponibili sono `TagResource`, `UntagResource` e `ListTagsForResource`.

Ogni risorsa dispone di un set di tag, ovvero una raccolta di uno o più tag assegnati alla risorsa. Ogni risorsa può avere fino a 50 tag per set di tag. Puoi aggiungere tag quando crei una risorsa e dopo che la risorsa è stata creata. Puoi aggiungere tag ai tipi di risorse serverless seguenti:

- Gruppi di lavoro
- Spazi dei nomi
- Snapshot

- Punti di ripristino

I tag hanno i requisiti seguenti:

- Alle chiavi non può essere anteposto il prefisso aws : .
- Le chiavi devono essere univoche per un set di tag.
- Una chiave deve essere costituita da un numero di caratteri compreso tra 1 e 128.
- Un valore deve essere costituito da un numero di caratteri compreso tra 0 e 256.
- Non è necessario che i valori siano univoci per un set di tag.
- I caratteri consentiti per le chiavi e i valori sono lettere Unicode, cifre, spazi e uno qualsiasi dei simboli seguenti: \_ . : / = + - @.
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole.

#### Gestione dei tag delle risorse di Amazon Redshift Serverless

1. Sulla console di Amazon Redshift Serverless, scegli Manage Tags (Gestisci tag).
2. Inserire il tipo di risorsa da cercare e scegliere Search resources (Cerca risorse). Scegli le risorse per le quali desideri gestire i tag, quindi seleziona Manage tags (Gestisci tag).
3. Specifica le chiavi e i valori opzionali che desideri aggiungere alla risorsa. Quando si modifica un tag, è possibile modificare il valore del tag, ma non la chiave.
4. Dopo aver aggiunto, rimosso o modificato i tag, scegliere Save changes (Salva modifiche), quindi scegliere Apply (Applica) per salvare le modifiche.

# Cluster con provisioning di Amazon Redshift

Nelle seguenti sezioni sono riportate le informazioni di base sulla creazione di un data warehouse mediante l'avvio di un set di nodi di calcolo denominato cluster di Amazon Redshift.

## Argomenti

- [Panoramica di Amazon Redshift](#)
- [Utilizzo di EC2-VPC durante la creazione del cluster](#)
- [Allarme predefinito dello spazio su disco](#)
- [Stato del cluster](#)
- [Considerazioni sull'utilizzo dei cluster con provisioning di Amazon Redshift](#)
- [Operazioni del cluster](#)
- [Configurazione dell'implementazione multi-AZ](#)
- [Gestione dei cluster con la console](#)
- [Gestione dei cluster utilizzando l'API AWS CLI Amazon Redshift](#)
- [Gestione dei cluster in un VPC](#)
- [Cronologia delle versioni del cluster](#)

## Panoramica di Amazon Redshift

Un data warehouse Amazon Redshift è costituito da un insieme di risorse di calcolo denominate nodi, strutturate in un gruppo denominato cluster. Ciascun cluster esegue un motore Amazon Redshift e contiene uno o più database.

### Note

Al momento è disponibile il motore Amazon Redshift versione 1.0. Tuttavia, poiché il motore viene costantemente aggiornato, è possibile che siano disponibili più versioni del motore Amazon Redshift.

## Cluster e nodi in Amazon Redshift

Un cluster Amazon Redshift è costituito da nodi. Ogni cluster include un nodo principale e uno o più nodi di calcolo. Il nodo principale riceve le query dalle applicazioni client, analizza le query e quindi genera i piani di esecuzione delle query. Il nodo principale coordina quindi l'esecuzione parallela di questi piani con i nodi di calcolo e aggrega i risultati intermedi da tali nodi. Restituisce infine i risultati alle applicazioni client.

I nodi di calcolo eseguono i piani di esecuzione delle query e si scambiano i dati necessari per elaborare tali query. I risultati intermedi vengono quindi inviati al nodo principale per l'aggregazione prima di essere reinviati alle applicazioni client. Per ulteriori informazioni sui nodi principali e sui nodi di calcolo, consultare [Architettura del sistema di data warehouse](#) nella Guida per gli amministratori di database di Amazon Redshift.

### Note

Quando crei un cluster sulla console Amazon Redshift (<https://console.aws.amazon.com/redshiftv2/>), puoi ricevere consigli sulla configurazione del cluster in base alla dimensione dei dati e alle caratteristiche delle query. Per utilizzare questo calcolatore di dimensionamento, cerca Help me choose sulla console nelle AWS regioni che supportano i tipi di nodi RA3. Per ulteriori informazioni, consultare [Creazione di un cluster](#).

Quando si avvia un cluster, una delle opzioni da specificare è il tipo di nodo. Il tipo di nodo determina la CPU, la RAM, la capacità di storage e il tipo di unità di storage per ciascun nodo.

Amazon Redshift offre diversi tipi di nodo per accogliere i carichi di lavoro. Consigliamo di scegliere RA3 o DC2 a seconda delle prestazioni necessarie, delle dimensioni dei dati e della relativa crescita prevista.

I nodi RA3 con storage gestito consentono di ottimizzare il data warehouse dimensionando e pagando le capacità di calcolo e storage gestito separatamente. Con RA3, basta scegliere il numero di nodi in base alle prestazioni necessarie e verrà fatturato solo lo storage gestito utilizzato. Dimensiona il cluster RA3 in base della quantità di dati elaborata quotidianamente. Puoi avviare i cluster che utilizzano i tipi di nodo RA3 in un virtual private cloud (VPC). Non è possibile avviare cluster RA3 in EC2-Classic. Per ulteriori informazioni, consultare [Creazione di un cluster in un VPC](#).

L'archiviazione gestita di Amazon Redshift utilizza SSD di grandi dimensioni e ad alte prestazioni in ogni nodo RA3 per un'archiviazione locale rapida e Amazon S3 per l'archiviazione durevole a lungo

termine. Se i dati in un nodo crescono superando la dimensione degli SSD locali, l'archiviazione gestita di Amazon Redshift trasferisce automaticamente tali dati su Amazon S3. A prescindere che i dati si trovino in SSD a elevate prestazioni o in Amazon S3, la tariffa pagata per l'archiviazione gestita di Amazon Redshift non cambia e rimane bassa. Per i carichi di lavoro che richiedono uno storage in continua crescita, lo storage gestito consente di scalare automaticamente la capacità di archiviazione del data warehouse separatamente dai nodi di elaborazione.

I nodi DC2 consentono di creare data warehouse per calcoli intensivi con storage SSD locale incluso. Puoi scegliere il numero di nodi di cui hai bisogno in base alla dimensione dei dati e ai requisiti di prestazioni. I nodi DC2 archiviano i dati a livello locale per garantire prestazioni elevate e, al crescere delle dimensioni dei dati, puoi aggiungere altri nodi di calcolo per aumentare la capacità di storage del cluster. Nel caso di set di dati inferiori a 1 TB (compressi), consigliamo i nodi DC2, così da avere prestazioni ottimali con prezzi minimi. Se prevedi una crescita dei dati, ti consigliamo di utilizzare i nodi RA3, in modo da poter dimensionare il calcolo e lo storage in modo indipendente per ottenere prezzi e prestazioni ottimali. Puoi avviare i cluster che utilizzano i tipi di nodo DC2 in un VPC (virtual private cloud). Non è possibile avviare cluster DC2 in modalità EC2-Classical. Per ulteriori informazioni, consulta [Creazione di un cluster in un VPC](#).

I tipi di nodo sono disponibili in diverse dimensioni. Le dimensioni e il numero dei nodi determinano lo storage totale di un cluster. Per ulteriori informazioni, consultare [Dettagli relativi ai tipi di nodo](#).

Alcuni tipi di nodo consentono un solo nodo (a nodo singolo) o due o più nodi (a più nodi). Il numero minimo di nodi per i cluster di alcuni tipi di nodo è due. In un cluster a nodo singolo, il nodo condivide le funzionalità del nodo principale e del nodo di calcolo. I cluster a nodo singolo non sono consigliati per l'esecuzione di carichi di lavoro di produzione. In un cluster a più nodi, il nodo principale è distinto dai nodi di calcolo. Il tipo del nodo principale è identico a quello dei nodi di calcolo. Paghi solo per i nodi di calcolo.

Amazon Redshift applica quote alle risorse per ogni AWS account in ogni regione. AWS Una quota limita il numero di risorse che il tuo account può creare per un determinato tipo di risorsa, come nodi o istantanee, all'interno di una regione. AWS Per ulteriori informazioni sulle quote predefinite valide per le risorse Amazon Redshift, consulta [Limiti di Amazon Redshift](#) nei Riferimenti generali di Amazon Web Services. Per richiedere un aumento, inviare un [modulo di richiesta di aumento del limite di Amazon Redshift](#).

Il costo del cluster dipende dalla AWS regione, dal tipo di nodo, dal numero di nodi e dal fatto che i nodi siano prenotati in anticipo. Per ulteriori informazioni sui costi dei nodi, consultare la pagina dei [prezzi di Amazon Redshift](#).

## Dettagli relativi ai tipi di nodo

Nelle tabelle seguenti sono riepilogate le specifiche dei nodi per ogni tipo e dimensione di nodo. Le intestazioni delle tabelle hanno i seguenti significati:

- vCPU è il numero di CPU virtuali per ogni nodo.
- RAM è la quantità di memoria, espressa in gibibyte (GiB), per ogni nodo.
- Sezioni di default per nodo è il numero di sezioni in cui un nodo di calcolo viene partizionato quando un cluster viene creato o ridimensionato con ridimensionamento classico.

Il numero di sezioni per nodo potrebbe cambiare se al cluster viene applicato il ridimensionamento elastico. Tuttavia, il numero totale di sezioni in tutti i nodi di calcolo nel cluster rimane lo stesso dopo il ridimensionamento elastico.

Quando si crea un cluster con l'operazione di ripristino da snapshot, il numero di sezioni del cluster risultante potrebbe cambiare rispetto al cluster originale se si modifica il tipo di nodo.

- Storage è la capacità e il tipo di storage per ogni nodo.
- L'intervallo di nodi è il numero minimo e massimo di nodi supportato da Amazon Redshift per il tipo e la dimensione del nodo.

### Note

Potresti essere limitato a un numero inferiore di nodi a seconda della quota applicata al tuo AWS account nella AWS regione selezionata. Per richiedere un aumento, inviare un [modulo di richiesta di aumento del limite di Amazon Redshift](#).

- La capacità totale è la capacità di archiviazione totale per il cluster se distribuisce il numero massimo di nodi specificati nell'intervallo di nodi.

## Tipi di nodo RA3

Tipo di nodo	VPCU	RAM (GiB)	Sezioni predefinite per nodo	Limite dell'archiviazione gestita per nodo <sup>1</sup>	Intervallo di nodi con creazione cluster	Capacità totale di archiviazione gestita <sup>2</sup>
ra3.xlplus (nodo singolo)	4	32	2	4 TB	1	4 TB <sup>3</sup>
ra3.xlplus (multinodo)	4	32	2	32 TB	2–16 <sup>4</sup>	1024 TB <sup>4</sup>
ra3.4xlarge	12	96	4	128 TB	2–32 <sup>5</sup>	8192 TB <sup>5</sup>
ra3.16xlarge	48	384	16	128 TB	2–128	16.384 TB <sup>4</sup>

<sup>1</sup> Il limite di l'archiviazione gestita per Amazon Redshift. Questo è un limite insuperabile.

<sup>2</sup> Il limite di archiviazione gestita totale è il numero massimo di nodi per il limite di archiviazione gestita per nodo.

<sup>3</sup> Per ridimensionare un cluster a nodo singolo su più nodi, è supportato solo il ridimensionamento classico.

<sup>4</sup> È possibile creare un cluster con il tipo di nodo ra3.xlplus (multinodo) contenente un massimo di 16 nodi. Per i cluster a più nodi, è possibile ridimensionare con il ridimensionamento elastico fino a un massimo di 32 nodi.

<sup>5</sup> È possibile creare cluster con il tipo di nodo ra3.4xlarge contenente un massimo di 32 nodi. È possibile ridimensionarlo con un ridimensionamento elastico fino a un massimo di 64 nodi.

## Tipi di nodo DC (Dense Compute)

Tipo di nodo	VPCU	RAM (GiB)	Sezioni predefinite per nodo	Archiviazione per nodo	Intervallo di nodi	Capacità totale
dc2.large	2	15	2	160 GB (NVMe-SSD)	1-32	5.12 TB
dc2.8xlarge	32	244	16	2,56 TB (NVMe-SSD)	2-128	326 TB

### Note

I tipi di nodi Dense Storage (DS2) non sono più disponibili.

## Nomi precedenti dei tipi di nodo

Nelle versioni precedenti di Amazon Redshift alcuni tipi di nodo hanno nomi diversi. Puoi utilizzare i nomi precedenti nell'API Amazon Redshift e. AWS CLI Tuttavia, ti consigliamo di aggiornare gli script che fanno riferimento a tali nomi in modo che utilizzino invece i nomi correnti. I nomi correnti e i rispettivi nomi precedenti sono riportati di seguito.

Nome corrente	Nomi precedenti
ds2.xlarge	ds1.xlarge, dw.hs1.xlarge, dw1.xlarge
ds2.8xlarge	ds1.8xlarge, dw.hs1.8xlarge, dw1.8xlarge
dc1.large	dw2.large
dc1.8xlarge	dw2.8xlarge

## Determinazione del numero di nodi

Dal momento che Amazon Redshift distribuisce ed esegue le query in parallelo tra tutti i nodi di calcolo di un cluster, è possibile ottimizzare le prestazioni delle query mediante l'aggiunta di nodi al cluster. Quando esegui un cluster che include almeno due nodi di calcolo, viene sempre eseguito il mirroring dei dati di ciascun nodo sui dischi di un altro nodo per ridurre il rischio di perdita dei dati.

Puoi monitorare le prestazioni delle query nella console Amazon Redshift e con i parametri di Amazon CloudWatch . Puoi inoltre aggiungere o rimuovere nodi in base alle esigenze per ottenere l'equilibrio tra prezzo e prestazioni per il cluster. Quando si richiede un nodo aggiuntivo, Amazon Redshift gestisce tutti i dettagli relativi a distribuzione, bilanciamento del carico e manutenzione dei dati. Per ulteriori informazioni sulle prestazioni dei cluster, consultare [Monitoraggio delle prestazioni del cluster Amazon Redshift](#).

Nodi riservati sono ideali per carichi di lavoro in ambienti di produzione a stato costante, poiché i costi sono molto inferiori rispetto ai prezzi on demand. Puoi acquistare nodi riservati dopo aver eseguito esperimenti e aver convalidato proof-of-concepts la configurazione di produzione. Per ulteriori informazioni, consulta [Acquisto di nodi riservati di Amazon Redshift](#).

La sospensione di un cluster comporta anche la sospensione della fatturazione on demand durante il periodo in cui il cluster è sospeso. Durante questo tempo di pausa, si paga per lo storage di backup. In questo modo non sarà necessario pianificare né acquistare in anticipo capacità del data warehouse e sarà possibile gestire ambienti di sviluppo o di test a costi ridotti.

Per informazioni sui prezzi dei nodi on demand e riservati, consultare [Prezzi di Amazon Redshift](#).

## Utilizzo di EC2-VPC durante la creazione del cluster

I cluster Amazon Redshift vengono eseguiti in istanze Amazon EC2 configurate per il tipo di nodo Amazon Redshift e le dimensioni selezionati. Crea il cluster utilizzando EC2-VPC. Se utilizzi ancora EC2-Classic, ti consigliamo di utilizzare EC2-VPC per ottenere prestazioni e sicurezza migliorate. Per ulteriori informazioni su queste piattaforme di rete, consulta [Supported Platforms](#) nella Amazon EC2 User Guide. Le impostazioni AWS dell'account determinano se EC2-VPC o EC2-Classic sono disponibili per te.

### Note

Per evitare problemi di connessione tra gli strumenti client SQL e il database Amazon Redshift, consigliamo di eseguire una delle due operazioni seguenti. Puoi configurare una

regola in entrata che autorizzi gli host a negoziare le dimensioni dei pacchetti. In alternativa, è possibile disabilitare i frame jumbo TCP/IP impostando l'unità massima di trasmissione (MTU) su 1500 sull'interfaccia di rete (NIC) delle istanze Amazon EC2. Per ulteriori informazioni su questi approcci, consultare [Query bloccate e talvolta impossibilitate a raggiungere il cluster](#).

## EC2-VPC

Quando si utilizza EC2-VPC, il cluster viene eseguito in un cloud privato virtuale (VPC) logicamente isolato dal proprio account. AWS Se si effettua il provisioning del cluster in EC2-VPC, per controllare l'accesso al cluster è necessario associare uno o più gruppi di sicurezza del VPC al cluster. Per ulteriori informazioni, consultare [Gruppi di sicurezza per il VPC](#) nella Guida per l'utente di Amazon VPC.

Per creare un cluster in un VPC, è necessario creare innanzitutto un gruppo di sottoreti del cluster Amazon Redshift immettendo le informazioni sulla sottorete del VPC in uso, quindi fornendo il gruppo di sottoreti all'avvio del cluster. Per ulteriori informazioni, consultare [Gruppi di sottoreti dei cluster Amazon Redshift](#).

Per ulteriori informazioni su Amazon Virtual Private Cloud (Amazon VPC), consultare la [pagina dei dettagli del prodotto di Amazon VPC](#).

## Allarme predefinito dello spazio su disco

Quando crei un cluster Amazon Redshift, puoi facoltativamente configurare un CloudWatch allarme Amazon per monitorare la percentuale media di spazio su disco utilizzata su tutti i nodi del cluster. Questo allarme viene definito allarme predefinito dello spazio su disco.

Questo tipo di allarme ha lo scopo di monitorare la capacità di storage del cluster. Puoi configurare questo allarme in base alle specifiche esigenze del data warehouse in uso. Ad esempio, puoi utilizzare l'avviso come indicatore per l'eventuale necessità di dimensionare il cluster. Puoi decidere di eseguire il dimensionamento utilizzando un tipo di nodo diverso, aggiungendo nodi oppure acquistando nodi prenotati da utilizzare nelle espansioni future.

L'allarme predefinito dello spazio su disco viene attivato quando l'utilizzo del disco raggiunge o supera una percentuale specificata per un determinato numero di volte e con una durata specificata. Per impostazione predefinita, questo allarme viene attivato quando la percentuale specificata viene raggiunta per cinque minuti o più oppure viene superata per la stessa durata di tempo. Puoi modificare i valori predefiniti dopo aver avviato il cluster.

Quando si attiva l' CloudWatch allarme, Amazon Simple Notification Service (Amazon SNS) invia una notifica a destinatari specifici per avvisarli del raggiungimento della soglia percentuale. Amazon SNS utilizza un argomento per specificare i destinatari e il messaggio inviato in una notifica. È possibile utilizzare un argomento Amazon SNS esistente. In caso contrario, viene creato un argomento in base alle impostazioni specificate all'avvio del cluster. Puoi modificare l'argomento dell'allarme corrente dopo aver avviato il cluster. Per ulteriori informazioni sulla creazione di argomenti Amazon SNS, consultare in [Nozioni di base di Amazon Simple Notification Service](#).

Dopo aver avviato il cluster, puoi visualizzare e modificare l'allarme dalla finestra di stato del cluster in Allarmi. CloudWatch Il nome è `percentage-disk-space-used-default-<stringa>`. È possibile aprire l'allarme per visualizzare l'argomento Amazon SNS associato e modificare le impostazioni dell'allarme. ***Se non hai selezionato un argomento Amazon SNS esistente da utilizzare, quello creato per te si chiama `< clustername >-default-alarms (< destinatario >); ad esempio, (notify@example.com). examplecluster-default-alarms`***

Per ulteriori informazioni sulla configurazione e modifica dell'allarme predefinito dello spazio su disco, consultare [Creazione di un cluster](#) e [Creazione o modifica dell'allarme dello spazio su disco](#).

#### Note

Se elimini il cluster, l'allarme associato non verrà eliminato, ma non verrà mai attivato. Puoi eliminare l'allarme dalla console se non ti serve più. CloudWatch

## Stato del cluster

Lo stato del cluster indica lo stato corrente del cluster. La tabella seguente fornisce una descrizione di ciascuno stato del cluster.

Stato	Descrizione
available	Il cluster è in esecuzione e disponibile.
available, prep-for-resize	Il cluster viene preparato per il ridimensionamento elastico. Il cluster è in esecuzione ed è disponibile per query in lettura e scrittura, anche se le operazioni del cluster, come la creazione di uno snapshot, non sono disponibili.

Stato	Descrizione
available, resize-cleanup	Un'operazione di ridimensionamento elastico sta completando il trasferimento dati sui nuovi nodi del cluster. Il cluster è in esecuzione ed è disponibile per query in lettura e scrittura, anche se le operazioni del cluster, come la creazione di uno snapshot, non sono disponibili.
cancelling- resize	L'operazione di dimensionamento viene annullata.
creating	Amazon Redshift sta creando il cluster. Per ulteriori informazioni, consultare <a href="#">Creazione di un cluster</a> .
deleting	Amazon Redshift sta eliminando il cluster. Per ulteriori informazioni, consultare <a href="#">Eliminazione di un cluster</a> .
final-snapshot	Amazon Redshift sta creando uno snapshot finale del cluster prima di eliminarlo. Per ulteriori informazioni, consultare <a href="#">Eliminazione di un cluster</a> .
hardware- failure	Nel cluster si è verificato un errore a livello di hardware.  Se si tratta di un cluster a nodo singolo, il nodo non può essere sostituito. Per recuperare il cluster, ripristina uno snapshot. Per ulteriori informazioni, consultare <a href="#">Snapshot e backup di Amazon Redshift</a> .
incompatible- hsm	Amazon Redshift non può connettersi al modulo di sicurezza hardware (HSM, Hardware Security Module). Controlla la configurazione HSM tra il cluster e HSM. Per ulteriori informazioni, consultare <a href="#">Crittografia per Amazon Redshift tramite moduli di sicurezza hardware (HSM)</a> .
incompatible- network	Si è verificato un problema nella configurazione della rete sottostante. Verifica che il VPC in cui hai avviato il cluster esista e che le relative impostazioni siano corrette. Per ulteriori informazioni, consultare <a href="#">Gestione dei cluster in un VPC</a> .

Stato	Descrizione
<code>incompatible-parameters</code>	Si è verificato un problema con uno o più valori di parametro nel gruppo di parametri associato e il valore o i valori di parametro non possono essere applicati. Modificare il gruppo di parametri e aggiorna i valori non validi. Per ulteriori informazioni, consultare <a href="#">Gruppi di parametri di Amazon Redshift</a> .
<code>incompatible-restore</code>	Si è verificato un problema durante il ripristino del cluster dallo snapshot. Prova a ripristinare di nuovo il cluster con uno snapshot diverso. Per ulteriori informazioni, consultare <a href="#">Snapshot e backup di Amazon Redshift</a> .
<code>modifying</code>	Amazon Redshift sta applicando le modifiche al cluster. Per ulteriori informazioni, consultare <a href="#">Modifica di un cluster</a> .
<code>paused</code>	Il cluster è in pausa. Per ulteriori informazioni, consultare <a href="#">Sospensione e ripristino dei cluster</a> .
<code>rebooting</code>	Amazon Redshift sta riavviando il cluster. Per ulteriori informazioni, consultare <a href="#">Riavvio di un cluster</a> .
<code>renaming</code>	Amazon Redshift sta applicando un nuovo nome al cluster. Per ulteriori informazioni, consultare <a href="#">Ridenominazione dei cluster</a> .
<code>resizing</code>	Amazon Redshift sta ridimensionando il cluster. Per ulteriori informazioni, consultare <a href="#">Ridimensionamento di un cluster</a> .
<code>rotating-keys</code>	Amazon Redshift sta ruotando le chiavi di crittografia del cluster. Per ulteriori informazioni, consultare <a href="#">Rotazione delle chiavi di crittografia in Amazon Redshift</a> .
<code>storage-full</code>	Il cluster ha raggiunto la relativa capacità di storage. Ridimensiona il cluster aggiungendo nodi o scegliendo una dimensione di nodo diversa. Per ulteriori informazioni, consultare <a href="#">Ridimensionamento di un cluster</a> .
<code>updating-hsm</code>	Amazon Redshift sta aggiornando la configurazione HSM.

# Considerazioni sull'utilizzo dei cluster con provisioning di Amazon Redshift

Dopo la creazione del cluster, in questa sezione puoi trovare informazioni sulle regioni in cui sono disponibili funzionalità, attività di manutenzione, tipi di nodi e limiti di utilizzo.

## Argomenti

- [Considerazioni su regioni e zone di disponibilità](#)
- [Manutenzione del cluster](#)
- [Gestione dei limiti di utilizzo in Amazon Redshift](#)
- [Funzionalità di rete supportate dai nodi RA3](#)
- [Tipi di nodo](#)

## Considerazioni su regioni e zone di disponibilità

Amazon Redshift è disponibile in diverse AWS regioni. Per impostazione predefinita, Amazon Redshift effettua il provisioning del cluster in una zona di disponibilità (AZ) selezionata casualmente all'interno della AWS regione scelta. Viene effettuato il provisioning di tutti i nodi del cluster nella stessa zona di disponibilità.

Facoltativamente, è possibile richiedere una zona di disponibilità specifica se Amazon Redshift è disponibile in tale zona. Ad esempio, se si dispone già di un'istanza Amazon EC2 in esecuzione in una zona di disponibilità, potrebbe essere necessario creare il proprio cluster Amazon Redshift nella stessa zona per ridurre la latenza. D'altra parte, potrebbe essere necessario scegliere un'altra zona di disponibilità con una maggiore disponibilità. Amazon Redshift potrebbe non essere disponibile in tutte le zone di disponibilità all'interno di una AWS regione.

Per un elenco delle AWS regioni supportate in cui è possibile effettuare il provisioning di un cluster Amazon Redshift, consulta gli [endpoint Amazon Redshift](#) nel. Riferimenti generali di Amazon Web Services

## Manutenzione del cluster

Amazon Redshift esegue periodicamente la manutenzione per applicare aggiornamenti al cluster. Durante questi aggiornamenti, il cluster Amazon Redshift non è disponibile per le operazioni normali.

Esistono diversi modi per controllare come poter effettuare la manutenzione del cluster. Ad esempio, puoi controllare come distribuire gli aggiornamenti sui cluster. Puoi anche scegliere se il cluster esegue sempre la versione di rilascio più recente o quella precedente alla più recente. Infine, puoi anche decidere di posticipare gli aggiornamenti di manutenzione non obbligatori.

## Argomenti

- [Finestre di manutenzione](#)
- [Posticipazione della manutenzione](#)
- [Selezione delle tracce di manutenzione del cluster](#)
- [Gestione delle versioni del cluster](#)
- [Rollback della versione cluster](#)
- [Determinazione della versione di manutenzione del cluster](#)

## Finestre di manutenzione

Amazon Redshift assegna una finestra di manutenzione di 30 minuti a caso su un periodo di 8 ore per AWS regione, in un giorno casuale della settimana (dal lunedì alla domenica, inclusi).

### Finestre di manutenzione predefinite

L'elenco seguente mostra i blocchi temporali per ciascuna AWS regione a partire dai quali vengono assegnate le finestre di manutenzione predefinite:

- Regione Stati Uniti orientali (Virginia settentrionale): 03:00-11:00 UTC
- Regione Stati Uniti orientali (Ohio): 03:00 - 11:00 UTC
- Regione Stati Uniti occidentali (California settentrionale): 06:00-14:00 UTC
- Regione Stati Uniti occidentali (Oregon): 06:00 - 14:00 UTC
- Regione Africa (Città del Capo): 20:00 - 04:00 UTC
- Regione Asia Pacifico (Hong Kong): 13:00 - 21:00 UTC
- Regione Asia Pacifico (Hyderabad): 16:30-00:30 UTC
- Regione Asia Pacifico (Jakarta): 15:00 – 23:00 UTC
- Regione Asia Pacifico (Melbourne): 12:00 - 20:00 UTC
- Regione Asia Pacifico (Mumbai): 16:30 - 00:30 UTC

- Regione Asia Pacifico (Tokyo): 13:00 – 21:00 UTC
- Regione Asia Pacifico (Seoul): 13:00 – 21:00 UTC
- Regione Asia Pacifico (Singapore): 14:00-22:00 UTC
- Regione Asia Pacifico (Sydney): 12:00 - 20:00 UTC
- Regione Asia Pacifico (Tokyo): 13:00-21:00 UTC
- Regione Canada (Centrale): 03:00 - 11:00 UTC
- Regione Canada occidentale (Calgary): 04:00 - 12:00 UTC
- Regione Cina (Pechino): 13:00 - 21:00 UTC
- Regione Cina (Ningxia): 13:00 - 21:00 UTC
- Regione Europa (Francoforte): 06:00 - 14:00 UTC
- Regione Europa (Irlanda): 22:00-06:00 UTC
- Regione Europa (Londra): 22:00 - 06:00 UTC
- Regione Europa (Milano): 21:00 - 05:00 UTC
- Regione Europa (Parigi): 23:00 - 07:00 UTC
- Regione Europa (Stoccolma): 23:00 - 07:00 UTC
- Regione Europa (Zurigo): 22:00-04:00 UTC
- Regione di Israele (Tel Aviv): 20:00 — 04:00 UTC
- Regione Europa (Spagna): 21:00-05:00 UTC
- Regione Medio Oriente (Bahrein): 13:00 - 21:00 UTC
- Regione Medio Oriente (EAU): 18:00–02:00 UTC
- Regione Sud America (San Paolo): 19:00 - 03:00 UTC

Se in una determinata settimana è pianificato un evento di manutenzione, tale evento viene avviato durante la finestra di manutenzione di 30 minuti assegnata. Mentre Amazon Redshift esegue la manutenzione, verranno terminate le query e tutte le altre operazioni in corso. La maggior parte del processo di manutenzione viene completato durante la finestra di manutenzione di 30 minuti, ma l'esecuzione di alcune attività di manutenzione potrebbe continuare anche dopo la chiusura della finestra. Se non sono previste attività di manutenzione da eseguire durante una finestra di manutenzione pianificata, il cluster continuerà a funzionare normalmente fino alla successiva finestra di manutenzione pianificata.

È possibile cambiare la finestra di manutenzione programmata modificando il cluster a livello di codice o utilizzando la console Amazon Redshift. È possibile trovare la finestra di manutenzione e impostare il giorno e l'ora in cui si verifica per il cluster nella scheda Manutenzione.

È possibile riavviare un cluster al di fuori di una finestra di manutenzione. Questo può avvenire per alcuni motivi. Un motivo più comune è che è stato rilevato un problema nel cluster e sono in corso operazioni di manutenzione per riportarlo a uno stato integro. Per ulteriori informazioni consulta l'articolo [Why did my Amazon Redshift cluster reboot outside of the maintenance window?](#), che fornisce dettagli sul motivo per cui ciò potrebbe verificarsi.

## Posticipazione della manutenzione

Per pianificare nuovamente la finestra di manutenzione del cluster, puoi posticipare la manutenzione fino a un massimo 45 giorni. Ad esempio, se la finestra di manutenzione del cluster è impostata a mercoledì 8:30 - 9:00 UTC ed è necessario accedere al cluster in quel periodo, puoi posticipare la manutenzione impostandola a un periodo successivo.

Se rinvii la manutenzione, Amazon Redshift continuerà ad applicare aggiornamenti hardware o altri aggiornamenti di sicurezza obbligatori al cluster. Durante questi aggiornamenti il cluster non è disponibile.

Se durante la prossima finestra di manutenzione è pianificato un aggiornamento hardware o un altro aggiornamento di sicurezza obbligatorio, Amazon Redshift ti invia notifiche anticipate nella categoria In sospeso. Per ulteriori informazioni sulle notifiche di eventi In sospeso, consulta [Notifiche di eventi Amazon Redshift](#).

Puoi anche scegliere di ricevere notifiche tramite SMS da Amazon Simple Notification Service (Amazon SNS). Per ulteriori informazioni sulla sottoscrizione alle notifiche eventi di Amazon SNS, consulta [Sottoscrizione alle notifiche degli eventi del cluster di Amazon Redshift](#).

Se posticipi la manutenzione del cluster, la finestra di manutenzione successiva al periodo di posticipazione non può essere posticipata.

### Note

Non è possibile posticipare la manutenzione dopo che è iniziata.

Per ulteriori informazioni sulla manutenzione dei cluster, consulta la documentazione seguente:

- [Finestre di manutenzione](#)
- [Gestione dei cluster con la console](#)
- [Modifica di un cluster](#)

## Selezione delle tracce di manutenzione del cluster

Quando è disponibile una nuova versione del cluster Amazon Redshift, il cluster viene aggiornato durante la relativa finestra di manutenzione. Puoi controllare se il cluster viene aggiornato alla versione aggiornata più recente o alla versione precedente.

La traccia di manutenzione controlla quale versione del cluster viene applicata durante una finestra di manutenzione. Quando Amazon Redshift rilascia una nuova versione del cluster, quella versione viene assegnata alla traccia corrente e la versione precedente viene assegnata alla traccia finale. Per impostare la traccia di manutenzione per il cluster, specifica uno dei seguenti valori:

- **Corrente:** utilizzare la versione del cluster approvata più recente.
- **Trailing:** utilizzare la versione del cluster prima della versione corrente.
- **Anteprima:** utilizzare la versione del cluster che contiene nuove funzionalità disponibili per l'anteprima.

Ad esempio, si assuma che il cluster al momento esegua la versione 1.0.2762 e la versione corrente di Amazon Redshift sia 1.0.3072. Se hai impostato il valore di traccia della manutenzione su Current (Corrente), il cluster viene aggiornato alla versione 1.0.3072 (la versione approvata successiva) durante la successiva finestra di manutenzione. Se invece il valore di traccia della manutenzione del cluster è impostato a Trailing (Finale), il cluster non viene aggiornato finché non è disponibile una nuova versione successiva alla versione 1.0.3072.

### Tracce anteprima

Una traccia Preview (Anteprima) potrebbe non essere sempre una delle scelte disponibili. Scegliendo una traccia Preview (Anteprima), deve anche essere selezionato un nome di traccia. Le tracce di anteprima e le relative risorse sono temporanee, presentano delle limitazioni funzionali e potrebbero non includere tutte le funzionalità correnti di Amazon Redshift disponibili in altre tracce. Utilizzando le tracce anteprima:

- Utilizzare la nuova console Amazon Redshift quando si lavora con le tracce di anteprima. Ad esempio, quando si crea un cluster da utilizzare con le funzionalità di anteprima.

- Non è possibile spostare un cluster da una traccia anteprima a un'altra.
- Non è possibile spostare un cluster su una traccia anteprima da una traccia corrente o finale.
- Non è possibile spostare un cluster da una traccia di anteprima su una traccia corrente o finale.
- Non è possibile eseguire un ripristino da uno snapshot creato a partire da una diversa traccia anteprima.
- È possibile utilizzare la traccia anteprima solo durante la creazione di un nuovo cluster o durante il ripristino da uno snapshot.
- Non è possibile eseguire un ripristino da uno snapshot creato a partire da una diversa traccia anteprima o con una versione di manutenzione del cluster successiva alla versione del cluster della traccia anteprima. Ad esempio, quando si ripristina un cluster in una traccia anteprima, è possibile utilizzare solo uno snapshot creato a partire da una versione di manutenzione del cluster precedente rispetto a quella della traccia anteprima.

### Passaggio da una traccia di manutenzione all'altra

La modifica delle tracce per un cluster è in genere una decisione occasionale. In tali casi, è consigliabile procedere con estrema prudenza. Se cambi la traccia di manutenzione da Trailing (Finale) a Current (Corrente), il cluster viene aggiornato alla versione di rilascio traccia Current (Corrente) durante la successiva finestra di manutenzione. Tuttavia, se cambi la traccia di manutenzione in Trailing (Finale), il cluster non viene aggiornato finché non è disponibile una nuova versione successiva alla versione di rilascio traccia Current (Corrente).

### Tracce di manutenzione e ripristino

Uno snapshot eredita la traccia di manutenzione dal cluster di origine. Se cambi la traccia di manutenzione del cluster di origine dopo aver creato uno snapshot, lo snapshot e il cluster di origine si trovano su tracce differenti. Quando esegui il ripristino dallo snapshot, il nuovo cluster avrà la traccia di manutenzione ereditata dal cluster di origine. Puoi modificare la traccia di manutenzione al completamento dell'operazione di ripristino. Il ridimensionamento di un cluster non ha impatto sulla traccia di manutenzione del cluster.

### Gestione delle versioni del cluster

Una traccia di manutenzione è costituita da una serie di rilasci. Puoi decidere se il cluster si trova sulla traccia Current (Corrente) o sulla traccia Trailing (Finale). Se hai impostato il cluster sulla traccia Current (Corrente), viene aggiornato alla versione di rilascio cluster più recente durante la relativa

finestra di manutenzione. Se hai impostato il cluster sulla traccia Trailing (Finale), viene aggiornato alla versione di rilascio cluster rilasciata immediatamente prima di quella più recente.

La colonna Stato del rilascio nell'elenco dei cluster della console Amazon Redshift indica se per qualcuno dei cluster è disponibile un aggiornamento.

## Rollback della versione cluster

Se il cluster è aggiornato con l'ultima versione del cluster, è possibile scegliere di eseguire il rollback alla versione precedente.

Per informazioni dettagliate sulle caratteristiche e sui miglioramenti inclusi in ogni versione del cluster, consultare [Cronologia delle versioni del cluster](#).

Per eseguire il rollback a una versione di cluster precedente

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster di cui desideri eseguire il rollback.
4. Alla voce Actions (Operazioni), scegli Roll back cluster version (Versione del cluster a cui eseguire il rollback). Appare la pagina Roll back cluster version (Versione del cluster a cui eseguire il rollback).
5. Se è disponibile una versione a cui eseguire il rollback, segui le istruzioni sulla pagina.
6. Scegli Roll back now (Esegui subito il rollback).

## Determinazione della versione di manutenzione del cluster

È possibile determinare la versione del motore Amazon Redshift e del database con la console Amazon Redshift.

Per trovare la versione di un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono

includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Unità di condivisione dati, Pianificazioni, Manutenzione e Proprietà.

3. Scegliere la scheda Manutenzione per maggiori dettagli.
4. Nella sezione Maintenance (Manutenzione) individua la voce Current cluster version (Versione attuale del cluster).

#### Note

Anche se nella console queste informazioni vengono visualizzate in un unico campo, si tratta di due parametri nell'API Amazon Redshift, `ClusterVersion` e `ClusterRevisionNumber`. Per ulteriori informazioni, consultare [Cluster](#) nella Documentazione di riferimento dell'API di Amazon Redshift.

## Gestione dei limiti di utilizzo in Amazon Redshift

È possibile definire limiti per monitorare e controllare l'utilizzo e il costo associato di alcune caratteristiche di Amazon Redshift. È possibile creare limiti di utilizzo giornalieri, settimanali e mensili e definire le operazioni eseguite automaticamente da Amazon Redshift se tali limiti vengono raggiunti. Le azioni includono elementi come la registrazione di un evento in una tabella di sistema per registrare l'utilizzo che supera i limiti definiti. Altre operazioni possibili includono la raccolta di avvisi con Amazon SNS e Amazon CloudWatch per inviare una notifica a un amministratore e la disabilitazione di ulteriori utilizzi per controllare i costi.

È possibile definire i limiti di utilizzo per ogni cluster. Dopo la creazione del cluster, è possibile definire i limiti di utilizzo per le seguenti caratteristiche:

- Amazon Redshift Spectrum
- Dimensionamento simultaneo di Amazon Redshift
- Sharing di dati in più regioni di Amazon Redshift

I limiti di utilizzo sono disponibili con la versione 1.0.14677 o successiva nelle regioni AWS in cui è possibile il ridimensionamento simultaneo di Amazon Redshift Spectrum e Amazon Redshift.

Un limite Redshift Spectrum specifica la soglia della quantità totale di dati analizzati con incrementi di 1 TB. Un limite di dimensionamento simultaneo specifica la soglia del tempo totale utilizzato dal

dimensionamento simultaneo in incrementi di 1 minuto. Un limite di condivisione di dati tra regioni specifica la soglia della quantità totale di dati analizzati con incrementi di 1 TB.

È possibile specificare un limite per un periodo giornaliero, settimanale o mensile (utilizzando UTC per determinare l'inizio e la fine del periodo). Se si crea un limite nel mezzo di un periodo, il limite viene misurato da quel punto alla fine del periodo. Ad esempio, se si crea un limite mensile il 15 marzo, il primo periodo mensile viene misurato dal 15 marzo al 31 marzo.

È possibile definire più limiti di utilizzo per ogni caratteristica. Ogni limite può avere un'operazione diversa. Le possibili operazioni includono quanto segue:

- **Accesso alla tabella di sistema:** questa è l'operazione di default. Le informazioni vengono registrate nella tabella `STL_USAGE_CONTROL`. La registrazione è utile quando si valuta l'utilizzo passato e si decide sui limiti di utilizzo futuri. Per ulteriori informazioni su cosa viene registrato, consultare [STL\\_USAGE\\_CONTROL](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- **Avviso:** Amazon Redshift emette parametri CloudWatch per l'utilizzo disponibile e consumato. È possibile definire fino a tre limiti di utilizzo per ciascuna caratteristica. Se si abilita l'operazione di allarme utilizzando la console Amazon Redshift, su questi parametri viene creato automaticamente un allarme CloudWatch. È possibile collegare facoltativamente un abbonamento Amazon SNS a tale allarme. Se si utilizza un'operazione API o la AWS CLI, assicurarsi di creare l'allarme CloudWatch manualmente. Quando viene raggiunta la soglia, anche gli eventi vengono registrati in una tabella di sistema.
- **Disabilita caratteristica:** quando viene raggiunta la soglia, Amazon Redshift disabilita la caratteristica fino a quando la quota non viene aggiornata per il periodo di tempo successivo (giornaliero, settimanale o mensile). Solo un limite per ogni caratteristica può avere l'azione di disattivazione. Gli eventi vengono inoltre registrati in una tabella di sistema e possono essere emessi avvisi.

I limiti di utilizzo persistono fino a quando la definizione del limite di utilizzo stessa o il cluster non viene eliminato.

È possibile definire e gestire i limiti di utilizzo con la nuova console Amazon Redshift, la AWS CLI o le operazioni API Amazon Redshift. Per definire un limite sulla console Amazon Redshift, passare al cluster e scegliere Configura limite di utilizzo per Operazioni. Per visualizzare i limiti di utilizzo definiti in precedenza per il cluster, passare al cluster e nella scheda Manutenzione selezionare la sezione Limiti di utilizzo. Per visualizzare la quantità di utilizzo disponibile e consumata per il cluster,

passare al cluster. Scegliere la scheda Prestazioni del cluster, quindi visualizzare i grafici per l'utilizzo consumato di una caratteristica.

Per gestire i limiti di utilizzo, è possibile utilizzare le operazioni della CLI di Amazon Redshift elencate di seguito. Per ulteriori informazioni, consultare la sezione relativa alle informazioni di riferimento ai comandi della AWS CLI.

- [create-usage-limit](#)
- [describe-usage-limits](#)
- [modify-usage-limit](#)
- [delete-usage-limit](#)

Per gestire i limiti di utilizzo, è possibile utilizzare le operazioni API di Amazon Redshift elencate di seguito. Per ulteriori informazioni, consultare la Documentazione di riferimento delle API di Amazon Redshift.

- [CreateUsageLimit](#)
- [DescribeUsageLimits](#)
- [ModifyUsageLimit](#)
- [DeleteUsageLimit](#)

Per apprendere come creare e monitorare i limiti di utilizzo usando la console Amazon Redshift, guardare il video [Controlli dei costi per Amazon Redshift Spectrum e il dimensionamento simultaneo](#).

## Funzionalità di rete supportate dai nodi RA3

I nodi RA3 supportano una raccolta di funzionalità di rete non disponibili per altri tipi di nodi. Questa sezione fornisce brevi descrizioni di ciascuna funzionalità e collegamenti a documentazione aggiuntiva:

- Endpoint VPC con cluster fornito: quando crei o ripristini un cluster RA3, Amazon Redshift utilizza una porta compresa tra 5431-5455 o 8191-8215. Quando il cluster è impostato su una porta in uno di questi intervalli, Amazon Redshift crea automaticamente un endpoint VPC nel tuo AWS account per il cluster e gli assegna un indirizzo IP privato. Se imposti il cluster come accessibile al pubblico, Redshift crea un indirizzo IP elastico nel tuo AWS account e lo collega all'endpoint VPC. Per ulteriori informazioni, consulta [Configurazione delle impostazioni di comunicazione dei gruppi di sicurezza per un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift Serverless](#).

- Cluster RA3 a sottorete singola: è possibile creare un cluster RA3 con una singola sottorete, ma non può utilizzare funzionalità di ripristino di emergenza. Si verifica un'eccezione se abiliti il riposizionamento del cluster quando la sottorete non ha più zone di disponibilità (AZ).
- Cluster e gruppi di sottoreti RA3 con più sottoreti: puoi creare un cluster RA3 con più sottoreti creando un gruppo di sottoreti quando esegui il provisioning del cluster nel tuo cloud privato virtuale (VPC). Un gruppo di sottoreti del cluster consente di specificare un set di sottoreti nel tuo VPC e Amazon Redshift crea il cluster in una di esse. Dopo aver creato un gruppo di sottoreti, puoi rimuovere le sottoreti aggiunte in precedenza o aggiungerne altre. Per ulteriori informazioni, consulta i gruppi di [sottoreti del cluster Amazon Redshift](#).
- Accesso agli endpoint su più account o più VPC: puoi accedere a un cluster o a un gruppo di lavoro Serverless Amazon Redshift fornito configurando un endpoint VPC gestito da Redshift. Puoi configurarlo come connessione privata tra un VPC che contiene un cluster o un gruppo di lavoro e un VPC in cui esegui uno strumento client, ad esempio. In questo modo, è possibile accedere al data warehouse senza utilizzare un indirizzo IP pubblico e senza instradare il traffico su Internet. Per ulteriori informazioni, consulta [Lavorare con gli endpoint VPC gestiti da Redshift](#).
- Trasferimento del cluster: è possibile spostare un cluster in un'altra zona di disponibilità (AZ) senza alcuna perdita di dati in caso di interruzione del servizio. Per attivarlo nella console Per ulteriori informazioni, consulta [Trasferimento del cluster](#).
- Nome di dominio personalizzato: puoi creare un nome di dominio personalizzato, noto anche come URL personalizzato, per il cluster Amazon Redshift. È un record easy-to-read DNS che indirizza le connessioni SQL-Client all'endpoint del cluster. Per ulteriori informazioni, consulta [Utilizzo di un nome di dominio personalizzato per le connessioni client](#).

## Tipi di nodo

Queste sezioni descrivono in dettaglio le attività disponibili per vari tipi di nodi.

### Argomenti

- [Nodi RA3](#)
- [Tipi di nodi DC2](#)

## Nodi RA3

Queste sezioni descrivono in dettaglio le attività disponibili per i nodi RA3.

### Argomenti

- [Panoramica](#)
- [Aggiornamento ai tipi di nodo RA3](#)

## Panoramica

I nodi RA3 offrono i seguenti vantaggi:

- Sono flessibili per aumentare la capacità di elaborazione senza aumentare i costi di storage. Ridimensionano lo storage senza un eccessivo provisioning della capacità di elaborazione.
- Utilizzano SSD ad alte prestazioni per i dati hot e Amazon S3 per i dati cold. Pertanto offrono facilità d'uso, storage conveniente ed elevate prestazioni di query.
- Utilizzano reti ad alta larghezza di banda basate sul sistema AWS Nitro per ridurre ulteriormente il tempo necessario per scaricare e recuperare i dati da Amazon S3.

Valuta l'opportunità di scegliere i tipi di nodo RA3 nei casi seguenti:

- Hai bisogno di flessibilità per scalare e pagare il calcolo separatamente dallo storage.
- Esegui query su una frazione dei dati totali.
- Il volume di dati cresce rapidamente o prevedi cresca rapidamente.
- Desideri la flessibilità per dimensionare il cluster solo in base alle esigenze di prestazioni.

Per utilizzare i tipi di nodi RA3, la tua regione deve supportare RA3. AWS Per ulteriori informazioni, consulta [Disponibilità del tipo di nodo RA3 nelle regioni AWS](#).

### Important

È possibile utilizzare i tipi di nodo ra3.xlplus solo con la versione del cluster 1.0.21262 o successiva. È possibile visualizzare la versione di un cluster esistente con la console Amazon Redshift. Per ulteriori informazioni, consultare [Determinazione della versione di manutenzione del cluster](#).

Assicurarsi di utilizzare la nuova console Amazon Redshift quando lavori con i tipi di nodo RA3.

Inoltre, per utilizzare i tipi di nodo RA3 con le operazioni Amazon Redshift che utilizzano la traccia di manutenzione, il valore di tale traccia deve essere impostato su una versione del

cluster che supporti RA3. Per ulteriori informazioni sulle tracce di manutenzione, consultare [Selezione delle tracce di manutenzione del cluster](#).

Considerare quanto segue quando si utilizzano tipi di nodi RA3 a nodo singolo.

- I produttori e i consumatori di datasharing sono supportati.
- Per modificare i tipi di nodi, è supportato solo il ridimensionamento classico. La modifica del tipo di nodo con il ridimensionamento elastico o il ripristino dello snapshot non è supportata. Sono supportati gli scenari seguenti:
  - Ridimensionamento classico di un dc2.xlarge a 1 nodo a un ra3.xlplus a 1 nodo e viceversa.
  - Ridimensionamento classico di un dc2.xlarge a 1 nodo su un ra3.xlplus a nodo multiplo e viceversa.
  - Ridimensionamento classico di un dc2.xlarge a più nodi ra3.xlplus a 1 nodo e viceversa.

Utilizzo dello spazio di archiviazione gestito di Amazon Redshift

Con l'archiviazione gestita di Amazon Redshift, è possibile archiviare ed elaborare tutti i dati in Amazon Redshift ottenendo una maggiore flessibilità per scalare separatamente la capacità di calcolo e quella di archiviazione. I dati continuano a essere inseriti con il comando COPY o INSERT. Per ottimizzare le prestazioni e gestire il posizionamento dei dati automatico nei vari livelli di storage, Amazon Redshift si avvale di ottimizzazioni quali temperatura di blocco dei dati, età di blocco dei dati e modelli di carichi di lavoro. Quando necessario, Amazon Redshift dimensiona automaticamente l'archiviazione in Amazon S3 senza richiedere alcuna azione manuale.

Per ulteriori informazioni sui costi di archiviazione, consultare [Prezzi di Amazon Redshift](#).

Gestione dei tipi di nodo RA3

Per sfruttare la separazione del calcolo dallo storage, puoi creare o aggiornare il cluster con il tipo di nodo RA3. Per utilizzare i tipi di nodo RA3, è necessario creare i cluster in un virtual private cloud (EC2-VPC).

Per modificare il numero di nodi del cluster Amazon Redshift con un tipo di nodo RA3, effettuare una delle operazioni seguenti:

- Aggiungere o rimuovere nodi con l'operazione di ridimensionamento elastico. In alcune situazioni, la rimozione di nodi da un cluster RA3 non è consentita con il ridimensionamento elastico. Ad

esempio, quando un aggiornamento del numero di nodi 2:1 imposta il numero di sezioni per nodo su 32. Per ulteriori informazioni, consultare [Ridimensionamento di cluster](#). Se il ridimensionamento elastico non è disponibile, utilizzare il ridimensionamento classico.

- Aggiungere o rimuovere nodi con l'operazione di ridimensionamento classico. Scegliere questa opzione quando si sta ridimensionando una configurazione che non è disponibile tramite il ridimensionamento elastico. Il ridimensionamento elastico è più veloce del ridimensionamento classico. Per ulteriori informazioni, consulta [Ridimensionamento di cluster](#).

## Disponibilità del tipo di nodo RA3 nelle regioni AWS

I tipi di nodi RA3 sono disponibili solo nelle seguenti regioni: AWS

- Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Regione Stati Uniti orientali (Ohio) (us-east-2)
- Regione Stati Uniti occidentali (California settentrionale) (us-west-1)
- Regione Stati Uniti occidentali (Oregon) (us-west-2)
- Regione Africa (Città del Capo) (af-south-1)
- Regione Asia Pacifico (Hong Kong) (ap-east-1)
- Regione Asia Pacifico (Hyderabad) (ap-south-2)
- Regione Asia Pacifico (Jakarta) (ap-southeast-3)
- Regione Asia Pacifico (Melbourne) (ap-southeast-4)
- Regione Asia Pacifico (Mumbai) (ap-south-1)
- Regione Asia Pacifico (Osaka) (ap-northeast-3)
- Regione Asia Pacifico (Seoul) (ap-northeast-2)
- Regione Asia Pacifico (Singapore) (ap-southeast-1)
- Regione Asia Pacifico (Sydney) (ap-southeast-2)
- Regione Asia Pacifico (Tokyo) (ap-northeast-1)
- Regione Canada (Centrale) (ca-central-1)
- Regione Canada occidentale (Calgary) (ca-west-1)
- Regione Cina (Pechino) (cn-north-1)
- Regione Cina (Ningxia) (cn-northwest-1)
- Regione Europa (Francoforte) (eu-central-1)
- Regione Europa (Zurigo) (eu-central-2)

- Regione Europa (Irlanda) (eu-west-1)
- Regione Europa (Londra) (eu-west-2)
- Regione Europa (Milano) (eu-south-1)
- Regione Europa (Spagna) (eu-south-2)
- Regione Europa (Parigi) (eu-west-3)
- Regione Europa (Stoccolma) (eu-north-1)
- Regione di Israele (Tel Aviv) (il-central-1)
- Regione Medio Oriente (Bahrein) (me-south-1)
- Regione Medio Oriente (EAU) (me-central-1)
- Regione Sud America (San Paolo) (sa-east-1)
- AWS GovCloud (Stati Uniti orientali) (us-gov-east-1)
- AWS GovCloud (Stati Uniti occidentali) (us-gov-west-1)

### Aggiornamento ai tipi di nodo RA3

Per aggiornare il tipo di nodo esistente a RA3, sono disponibili le seguenti opzioni per modificare il tipo di nodo:

- Ripristino da uno snapshot: Amazon Redshift utilizza lo snapshot più recente del cluster e lo ripristina per creare un nuovo cluster RA3. Al termine della creazione del cluster (in genere entro pochi minuti), i nodi RA3 sono pronti per eseguire il carico di lavoro di produzione completo. Poiché il calcolo è separato dallo storage, i dati hot vengono trasferiti nella cache locale a velocità elevate grazie all'ampia larghezza di banda di rete. Se esegui il ripristino dall'ultima istantanea DC2, RA3 conserva le informazioni relative agli hot block del carico di lavoro DC2 e popola la cache locale con i blocchi più caldi. Per ulteriori informazioni, consulta [Ripristino di un cluster da uno snapshot](#).

Per mantenere lo stesso endpoint per le applicazioni e gli utenti, è possibile rinominare il nuovo cluster RA3 con lo stesso nome del cluster DC2 originale. Per rinominare il cluster, modificare il cluster nella console Amazon Redshift o con l'operazione API `ModifyCluster`. Per ulteriori informazioni, consultare [Ridenominazione dei cluster](#) o [Operazione API `ModifyCluster`](#) nella Guida di riferimento dell'API di Amazon Redshift.

- Ridimensionamento elastico: ridimensiona il cluster utilizzando il ridimensionamento elastico. Quando si utilizza il ridimensionamento elastico per modificare il tipo di nodo, Amazon Redshift crea automaticamente uno snapshot, crea un nuovo cluster, elimina il cluster precedente e rinomina il nuovo cluster. L'operazione di ridimensionamento elastico può essere eseguita

on demand o pianificata per l'esecuzione in un secondo momento. È possibile aggiornare rapidamente i cluster di tipo nodo DC2 esistenti a RA3 con il ridimensionamento elastico. Per ulteriori informazioni, consulta [Elastic resize \(Ridimensionamento elastico\)](#).

Nella tabella seguente vengono illustrati i suggerimenti durante l'aggiornamento a tipi di nodo RA3. (Queste raccomandazioni si applicano anche ai nodi riservati.)

I consigli in questa tabella riguardano i tipi e le dimensioni iniziali dei nodi del cluster, ma dipendono dai requisiti di elaborazione del carico di lavoro. Per valutare meglio i requisiti, prendi in considerazione la possibilità di eseguire un proof of concept (POC) che utilizzi [Test Drive](#) per eseguire potenziali configurazioni. Effettua il provisioning di un cluster per il tuo data warehouse POC anziché Redshift Serverless. Per ulteriori informazioni sulla conduzione di un proof of concept, consulta [Conduct a proof of concept \(POC\) per Amazon Redshift nella Amazon Redshift Database Developer Guide](#).

Tipo di nodo esistente	Numero di nodi esistenti	Nuovo tipo di nodo consigliato	Operazione di aggiornamento
dc2.8xlarge	2-15	ra3.4xlarge	Creare 2 nodi di ra3.4xlarge per ogni nodo di dc2.8xlarge <sup>1</sup> .
dc2.8xlarge	16-128	ra3.16xlarge	Creare 1 nodo di ra3.16xlarge per ogni 2 nodi di dc2.8xlarge <sup>1</sup> .
dc2.large	1-4	nessuno	Mantenere il cluster dc2.large esistente.
dc2.large	5-15	ra3.xlplus	Creare 3 nodi di ra3.4xlarge per ogni 8 nodi di dc2.large <sup>1</sup> .

Tipo di nodo esistente	Numero di nodi esistenti	Nuovo tipo di nodo consigliato	Operazione di aggiornamento
dc2.large	16-32	ra3.4xlarge	Creare 1 nodo di ra3.4xlarge per ogni 8 nodi di dc2.large <sup>1,2</sup> .

<sup>1</sup> Nodi aggiuntivi potrebbero essere necessari a seconda dei requisiti del carico di lavoro. Aggiungere o rimuovere nodi in base ai requisiti di calcolo delle prestazioni delle query richieste.

<sup>2</sup> I cluster con il tipo di nodo dc2.large sono limitati a 32 nodi.

Il numero minimo di nodi per alcuni tipi di nodo RA3 è due. Tenere presente questo aspetto quando si crea un cluster RA3.

## Tipi di nodi DC2

Queste sezioni descrivono in dettaglio le attività disponibili per i tipi di nodi DC2.

## Operazioni del cluster

Dopo la creazione del cluster, è possibile eseguire diverse operazioni. Le operazioni includono ridimensionamento, sospensione, ripristino, ridenominazione ed eliminazione.

### Argomenti

- [Ridimensionamento di cluster](#)
- [Sospensione e ripristino dei cluster](#)
- [Ridenominazione dei cluster](#)
- [Chiusura ed eliminazione di cluster](#)
- [Trasferimento del cluster](#)
- [Snapshot e backup di Amazon Redshift](#)

## Ridimensionamento di cluster

Con l'evolversi delle esigenze prestazionali e di capacità del data warehouse, puoi ridimensionare il cluster per usufruire al meglio delle opzioni di calcolo e archiviazione fornite da Amazon Redshift.

Un'operazione di ridimensionamento è disponibile in due tipi:

- **Ridimensionamento elastico:** puoi aggiungere o rimuovere nodi dal cluster. È inoltre possibile modificare il tipo di nodo, ad esempio da nodi DC2 a nodi RA3. Un ridimensionamento elastico viene in genere completato rapidamente, impiegando in media dieci minuti. Per questo motivo, la consigliamo come prima opzione. Quando esegui un ridimensionamento elastico, vengono ridistribuite le sezioni dei dati, ovvero le partizioni in cui sono allocati memoria e spazio su disco in ogni nodo. Il ridimensionamento elastico è appropriato quando:
  - Aggiungi o riduci nodi in un cluster esistente, ma non modifichi il tipo di nodo: questo è comunemente chiamato ridimensionamento locale. Quando si esegue questo tipo di ridimensionamento, alcune query in esecuzione vengono completate correttamente, ma altre possono essere eliminate come parte dell'operazione.
  - Cambi il tipo di nodo per un cluster: quando modifichi il tipo di nodo, viene creato uno snapshot e i dati vengono ridistribuiti dal cluster di origine a un cluster costituito dal nuovo tipo di nodo. Al termine, le query in esecuzione vengono eliminate. Come il ridimensionamento locale, si completa rapidamente.
- **Ridimensionamento classico:** puoi modificare il tipo, il numero di nodi oppure entrambi, come nel ridimensionamento elastico. Il ridimensionamento classico richiede più tempo per essere completato, ma può essere utile nei casi in cui la modifica del conteggio dei nodi o del tipo di nodo verso cui migrare non rientra nei limiti per il ridimensionamento elastico. Ciò può essere applicato, ad esempio, quando la modifica del numero di nodi è molto grande.

## Argomenti

- [Elastic resize \(Ridimensionamento elastico\)](#)
- [Classic resize \(Ridimensionamento classico\)](#)

## Elastic resize (Ridimensionamento elastico)

Un'operazione di ridimensionamento elastico, quando si aggiungono o rimuovono nodi dello stesso tipo, prevede le seguenti fasi:

1. Il ridimensionamento elastico acquisisce lo snapshot di un cluster. Questo snapshot include sempre [tabelle senza backup](#) per i nodi in cui è applicabile. (Alcuni tipi di nodi, come RA3, non hanno tabelle senza backup). Se il cluster non dispone di uno snapshot recente perché sono stati disabilitati gli snapshot automatici, l'operazione di backup richiederà più tempo. Per ridurre al minimo i tempi prima che inizi l'operazione di ridimensionamento, consigliamo di abilitare

- gli snapshot automatici o creare uno snapshot manuale. Quando avvii un ridimensionamento elastico ed è in corso un'operazione di snapshot, il ridimensionamento potrebbe non riuscire se l'operazione di snapshot non viene completata entro pochi minuti. Per ulteriori informazioni, consulta [Snapshot e backup di Amazon Redshift](#).
2. L'operazione esegue la migrazione dei metadati del cluster. Questo cluster non è disponibile per alcuni minuti. La maggior parte delle query viene temporaneamente sospesa e le connessioni vengono mantenute aperte. Tuttavia, è possibile che alcune query vengano eliminate. Questa fase è breve.
  3. Le connessioni delle sessioni vengono reintegrate e le query ripristinate.
  4. Il ridimensionamento elastico ridistribuisce i dati alle sezioni dei nodi in background. Il cluster è disponibile per le operazioni di lettura e scrittura, ma l'esecuzione di alcune query potrebbe richiedere più tempo.
  5. Al termine dell'operazione, Amazon Redshift invia una notifica di evento.

Il ridimensionamento elastico per modificare il tipo di nodo funziona in modo simile all'aggiunta o alla rimozione di nodi dello stesso tipo. Innanzitutto, viene creato uno snapshot. A un nuovo cluster di destinazione vengono forniti i dati più recenti dello snapshot; tali dati vengono trasferiti nel nuovo cluster in background. Durante questo periodo, i dati sono di sola lettura. Quando il processo di ridimensionamento è prossimo alla conclusione, Amazon Redshift aggiorna l'endpoint in modo da fare riferimento al nuovo cluster e tutte le connessioni al cluster di origine vengono eliminate.

È improbabile che un ridimensionamento elastico fallisca. Tuttavia, in caso di errore, il rollback avviene automaticamente nella maggior parte dei casi senza bisogno di alcun intervento manuale.

Se si dispone di nodi riservati, ad esempio nodi riservati DC2, è possibile eseguire l'aggiornamento ai nodi riservati RA3 quando si esegue un ridimensionamento. Puoi farlo quando esegui un ridimensionamento elastico o se utilizzi la console per eseguire il ripristino da uno snapshot. Tutto il processo può essere eseguito nella console. Per ulteriori informazioni sulla creazione di nodi RA3, consultare [Aggiornamento ai tipi di nodo RA3](#).

Il ridimensionamento elastico non ordina le tabelle né recupera spazio sul disco, pertanto non deve essere considerato come sostituzione di un'operazione di vacuum. Per ulteriori informazioni, consultare [Vacuum delle tabelle](#).

Il ridimensionamento elastico presenta le seguenti limitazioni:

- Cluster di condivisione dati e ridimensionamento elastico: quando si aggiungono o si sottraggono nodi in un cluster producer di condivisione dati, non è possibile connettersi a tale cluster dai

consumer mentre Amazon Redshift esegue la migrazione dei metadati del cluster. Analogamente, se si esegue un ridimensionamento elastico e si sceglie un nuovo tipo di nodo, la condivisione dati non è disponibile mentre le connessioni vengono interrotte e trasferite al nuovo cluster di destinazione. In entrambi i tipi di ridimensionamento elastico, il producer non è disponibile per diversi minuti.

- Trasferimento dei dati da uno snapshot condiviso: per eseguire un ridimensionamento elastico in un cluster che trasferisce dati da uno snapshot condiviso, deve essere disponibile almeno un backup per il cluster. È possibile visualizzare i backup nell'elenco snapshot della console Amazon Redshift, mediante il comando `describe-cluster-snapshots` della CLI oppure mediante l'operazione API `DescribeClusterSnapshots`.
- Limitazione della piattaforma: il ridimensionamento elastico è disponibile solo per i cluster che utilizzano la piattaforma EC2-VPC. Per ulteriori informazioni, consulta [Utilizzo di EC2-VPC durante la creazione del cluster](#).
- Considerazioni sull'archiviazione: assicurati che la nuova configurazione del nodo disponga di spazio di archiviazione sufficiente per i dati esistenti. Potrebbe essere necessario aggiungere altri nodi o modificare la configurazione.
- Dimensioni del cluster di origine e di destinazione: il numero e il tipo di nodi consentiti dal ridimensionamento elastico sono determinati dal numero di nodi nel cluster di origine e dal tipo di nodi scelto per il cluster ridimensionato. Per determinare le possibili configurazioni disponibili, è possibile utilizzare la console. Oppure puoi usare il `describe-node-configuration-options` AWS CLI comando con l'opzione `action-type resize-cluster`. Per ulteriori informazioni sul ridimensionamento tramite la console Amazon Redshift, consultare [Ridimensionamento di un cluster](#).

Il comando della CLI seguente descrive le opzioni di configurazione disponibili. In questo esempio, il cluster denominato `mycluster` è un cluster `dc2.large` a 8 nodi.

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --region eu-west-1 --action-type resize-cluster
```

Questo comando restituisce un elenco di opzioni con tipi di nodi consigliati, numero di nodi e utilizzo del disco per ogni opzione. Le configurazioni restituite possono variare in base al cluster di input specifico. È possibile scegliere una di queste configurazioni quando si specificano le opzioni del comando `resize-cluster` della CLI.

- Limite massimo sui nodi aggiuntivi: il ridimensionamento elastico ha dei limiti sui nodi che puoi aggiungere a un cluster. Ad esempio, un cluster `dc2` supporta il ridimensionamento elastico fino a

raddoppiare il numero di nodi. Ad esempio, puoi aggiungere un nodo a un cluster dc2.8xlarge a 4 nodi per renderlo un cluster a 5 nodi o aggiungere altri nodi fino a raggiungerne 8.

### Note

I limiti di crescita e riduzione si basano sul tipo di nodo originale e sul numero di nodi del cluster originale o dell'ultimo ridimensionamento classico. Se il ridimensionamento elastico supera il limite di crescita o riduzione, utilizza un ridimensionamento classico.

Con alcuni tipi di nodi ra3, è possibile aumentare il numero di nodi fino a quattro volte il numero esistente. In particolare, si supponga che il cluster sia costituito da nodi ra3.4xlarge o ra3.16xlarge. È quindi possibile utilizzare il ridimensionamento elastico per aumentare il numero di nodi in un cluster a 8 nodi a 32. Oppure è possibile scegliere un valore al di sotto del limite. La possibilità di aumentare il cluster di 4 volte dipende dalle dimensioni del cluster di origine. Se il cluster ha nodi ra3.xlplus, il limite è il doppio.

Tutti i tipi di nodi ra3 supportano una diminuzione del numero di nodi fino a un quarto del numero esistente. Ad esempio, è possibile ridurre la dimensione di un cluster con nodi ra3.4xlarge da 12 nodi a 3 o a un numero superiore al minimo.

Nella tabella seguente sono elencati i limiti di crescita e riduzione per ogni tipo di nodo che supporta il ridimensionamento elastico.

Tipo di nodo originale	Limite di crescita	Limite di riduzione
ra3.16xlarge	4x (da 4 a 16 nodi, ad esempio)	A un quarto del numero (da 16 a 4 nodi, ad esempio)
ra3.4xlarge	4x	A un quarto del numero
ra3.xlplus	2x (da 4 a 8 nodi, ad esempio)	A un quarto del numero
dc2.8xlarge	2x	A metà del numero (da 16 a 8 nodi, ad esempio)
dc2.large	2x	A metà del numero

**Note**

Scelta dei tipi di nodi precedenti quando si ridimensiona un cluster RA3: se si tenta di ridimensionare un cluster con nodi RA3 a un altro tipo di nodo, ad esempio DC2, nella console viene visualizzato un messaggio di avviso di convalida e l'operazione di ridimensionamento non verrà completata. Ciò si verifica perché il ridimensionamento in base ai tipi di nodi legacy non è supportato. Questo serve a impedire a un cliente di ridimensionare un tipo di nodo obsoleto oppure obsoleto a breve. Questo vale sia per il ridimensionamento elastico che per il ridimensionamento classico.

## Classic resize (Ridimensionamento classico)

Il ridimensionamento classico gestisce i casi in cui la modifica della dimensione del cluster o del tipo di nodo non è supportata dal ridimensionamento elastico. Quando esegui un ridimensionamento classico, Amazon Redshift crea un cluster di destinazione ed esegue la migrazione dei dati e dei metadati dal cluster di origine.

Il ridimensionamento classico a RA3 può fornire una migliore disponibilità

Il ridimensionamento classico è stato migliorato quando il tipo di nodo di destinazione è RA3. Ciò è stato possibile grazie all'utilizzo di un'operazione di backup e ripristino tra il cluster di origine e quello di destinazione. Quando il ridimensionamento inizia, il cluster di origine si riavvia e non è disponibile per alcuni minuti. Dopodiché, il cluster diventa disponibile per le operazioni di lettura e scrittura mentre il ridimensionamento continua in background.

### Controllo del cluster

Per assicurarti di ottenere prestazioni e risultati ottimali quando esegui un ridimensionamento classico su un cluster RA3, completa questo elenco di controllo. Se non segui l'elenco di controllo, potresti non ottenere alcuni dei vantaggi del ridimensionamento classico con i nodi RA3, come la possibilità di eseguire operazioni di lettura e scrittura.

1. La dimensione dei dati deve essere inferiore a due petabyte (un petabyte equivale a 1.000 terabyte). Per convalidare la dimensione dei dati, crea uno snapshot e controlla le dimensioni. Puoi anche eseguire la seguente query per verificare le dimensioni:

```
SELECT
```

```
sum(case when lower(diststyle) like ('%key%') then size else 0 end) distkey_blocks,  
sum(size) as total_blocks,  
((distkey_blocks/(total_blocks*1.00))*100 as Blocks_need_redist  
FROM svv_table_info;
```

La tabella `svv_table_info` è visibile solo per gli utenti con privilegi avanzati.

2. Prima di iniziare un ridimensionamento classico, assicurati di avere uno snapshot manuale precedente di 10 ore al massimo. In caso contrario, acquisisci uno snapshot.
3. Lo snapshot utilizzato per eseguire il ridimensionamento classico non può essere utilizzato per il ripristino di una tabella o per altri scopi.
4. Il cluster deve trovarsi in un VPC.

Operazioni di ordinamento e distribuzione derivanti dal ridimensionamento classico a RA3

Durante il ridimensionamento classico a RA3, le tabelle con distribuzione delle chiavi migrate con la distribuzione uniforme vengono riconvertite nel loro stile di distribuzione originale. La durata dipende dalla dimensione dei dati e dal carico di lavoro del cluster. Durante la migrazione dei dati viene data maggiore priorità all'esecuzione dei carichi di lavoro delle query. Per ulteriori informazioni, consulta [Piani di distribuzione](#). Le operazioni di lettura e scrittura nel database funzionano durante questo processo di migrazione, tuttavia potrebbe essere necessario più tempo per il completamento delle query. Il dimensionamento simultaneo può migliorare le prestazioni durante il processo, aggiungendo risorse per i carichi di lavoro delle query. Puoi vedere l'avanzamento della migrazione dei dati visualizzando i risultati nelle viste [SYS\\_RESTORE\\_STATE](#) e [SYS\\_RESTORE\\_LOG](#). Seguono ulteriori informazioni sul monitoraggio.

Dopo il completo ridimensionamento del cluster, si verifica il seguente comportamento di ordinamento:

- Se il ridimensionamento comporta che il cluster abbia più sezioni, le tabelle di distribuzione KEY sono parzialmente non ordinate, ma le tabelle EVEN rimangono ordinate. Inoltre, le informazioni sulla quantità di dati ordinati potrebbero non essere aggiornate subito dopo il ridimensionamento. Dopo il recupero della chiave, il vacuum automatico ordina la tabella nel tempo.
- Se il ridimensionamento comporta che una riduzione del numero di sezioni del cluster, le tabelle di distribuzione KEY e EVEN sono parzialmente non ordinate. Il vacuum automatico ordina la tabella nel tempo.

Per ulteriori informazioni sul vacuum automatico della tabella, consulta [Vacuum delle tabelle](#). Per ulteriori informazioni sulle sezioni dei nodi di calcolo, consulta [Architettura del sistema di data warehouse](#).

Fasi del ridimensionamento classico quando il cluster di destinazione è RA3

Il ridimensionamento classico consiste nelle seguenti fasi, quando il tipo di cluster di destinazione è RA3 e sono soddisfatti i prerequisiti descritti nella sezione precedente.

1. La migrazione inizia dal cluster di origine verso il cluster di destinazione. Dopo aver effettuato il provisioning del nuovo cluster di destinazione, Amazon Redshift invia un evento di notifica che indica l'inizio del ridimensionamento, quindi riavvia il cluster esistente, interrompendo tutte le connessioni. Se il cluster esistente è un cluster producer di condivisione dati, anche le connessioni ai cluster consumer vengono chiuse. Il riavvio richiede alcuni minuti.

Tieni presente che qualsiasi relazione del database, come una tabella o una vista materializzata, creata con `BACKUP NO` non viene mantenuta durante il ridimensionamento classico. Per ulteriori informazioni, consulta [CREATE MATERIALIZED VIEW](#).

2. Dopo il riavvio, il database è disponibile per le operazioni di lettura e scrittura. Riprende anche la condivisione dei dati, il che richiede qualche minuto in più.
3. I dati vengono migrati al cluster di destinazione. Quando il tipo di nodo di destinazione è RA3, le operazioni di lettura e scrittura sono disponibili durante la migrazione dei dati.
4. Quando il processo di ridimensionamento è prossimo alla conclusione, Amazon Redshift aggiorna l'endpoint sul cluster di destinazione e tutte le connessioni al cluster di origine vengono eliminate. Il cluster di destinazione diventa il producer della condivisione dei dati.
5. Il ridimensionamento viene completato. Amazon Redshift invia una notifica dell'evento.

È possibile visualizzare lo stato di avanzamento del processo di dimensionamento nella console Amazon Redshift. L'intervallo di tempo necessario per ridimensionare un cluster dipende dalla quantità di dati.

#### Note

Scelta dei tipi di nodi precedenti quando si ridimensiona un cluster RA3: se si tenta di ridimensionare da un cluster con nodi RA3 a un altro tipo di nodo, ad esempio DC2, nella console viene visualizzato un messaggio di avviso di convalida e l'operazione di ridimensionamento non verrà completata. Ciò si verifica perché il ridimensionamento in base

ai tipi di nodi legacy non è supportato. Questo serve a impedire a un cliente di ridimensionare un tipo di nodo obsoleto oppure obsoleto a breve. Questo vale sia per il ridimensionamento elastico che per il ridimensionamento classico.

## Monitoraggio di un ridimensionamento classico quando il cluster di destinazione è RA3

Per monitorare il ridimensionamento classico in esecuzione di un cluster con provisioning, inclusa la distribuzione delle chiavi, usa [SYS\\_RESTORE\\_STATE](#). Mostra la percentuale di completamento della tabella in fase di conversione. Devi essere un utente con privilegi avanzati per poter accedere ai dati.

Elimina le tabelle che non ti servono quando esegui un ridimensionamento classico. In questo modo, le tabelle esistenti possono essere distribuite più rapidamente.

## Fasi del ridimensionamento classico quando il cluster di destinazione non è RA3

Il ridimensionamento classico prevede quanto segue, quando il tipo di nodo di destinazione è diverso da RA3, ad esempio DC2.

1. La migrazione inizia dal cluster di origine verso il cluster di destinazione. Dopo aver effettuato il provisioning del nuovo cluster di destinazione, Amazon Redshift invia un evento di notifica che indica l'inizio del ridimensionamento, quindi riavvia il cluster esistente, interrompendo tutte le connessioni. Se il cluster esistente è un cluster producer di condivisione dati, anche le connessioni ai cluster consumer vengono chiuse. Il riavvio richiede alcuni minuti.

Tieni presente che qualsiasi relazione del database, come una tabella o una vista materializzata, creata con `BACKUP NO` non viene mantenuta durante il ridimensionamento classico. Per ulteriori informazioni, consulta [CREATE MATERIALIZED VIEW](#).

2. Dopo il riavvio, il database è disponibile in sola lettura. Riprende la condivisione dei dati, il che richiede qualche minuto in più.
3. I dati vengono migrati al cluster di destinazione. Il database rimane in sola lettura.
4. Quando il processo di ridimensionamento è prossimo alla conclusione, Amazon Redshift aggiorna l'endpoint sul cluster di destinazione e tutte le connessioni al cluster di origine vengono eliminate. Il cluster di destinazione diventa il producer della condivisione dei dati.
5. Il ridimensionamento viene completato. Amazon Redshift invia una notifica dell'evento.

È possibile visualizzare lo stato di avanzamento del processo di dimensionamento nella console Amazon Redshift. L'intervallo di tempo necessario per ridimensionare un cluster dipende dalla quantità di dati.

### Note

Possono essere necessari giorni o anche settimane per ridimensionare un cluster con una grande quantità di dati quando il cluster di destinazione non è RA3 o non soddisfa i requisiti di un cluster di destinazione RA3 descritti nella sezione precedente.

Tieni inoltre presente che la capacità di archiviazione utilizzata per il cluster può aumentare dopo un ridimensionamento classico. Si tratta di un normale comportamento del sistema quando il cluster contiene porzioni di dati aggiuntive risultanti dal ridimensionamento classico. Questo uso di capacità aggiuntiva può verificarsi anche quando il numero di nodi nel cluster rimane invariato.

## Ridimensionamento elastico e ridimensionamento classico

Nella tabella seguente viene confrontato il comportamento tra i due tipi di ridimensionamento.

### Ridimensionamento elastico e ridimensionamento classico

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Comme				
Conservazione dei dati di sistema	Il ridimensionamento elastico conserva i dati dei log di sistema.	Il ridimensionamento classico non conserva tabelle e dati di sistema.	Se hai abilitato la registrazione di controllo nel tuo cluster di				

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Comme				
			origine, puoi continuare ad accedere ai log in Amazon S3 o CloudWatch in Amazon S3, dopo un ridimensionamento. Puoi conservare o eliminare questi log, in base a quanto specifico to nelle policy				

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Commenti
			dei dati.
Modifica dei tipi di nodo	<p>Ridimensionamento elastico, quando il tipo di nodo non cambia: ridimensionamento sul posto e la maggior parte delle query vengono conservate.</p> <p>Ridimensionamento elastico, con un nuovo tipo di nodo selezionato: viene creato un nuovo cluster. Le query vengono eliminate al termine del processo di ridimensionamento.</p>	<p>Ridimensionamento classico: viene creato un nuovo cluster. Le query vengono eliminate al termine del processo di ridimensionamento.</p>	

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Comme				
Conservazione di sessioni e query	Il ridimensionamento elastico conserva sessioni e query quando il tipo di nodo è lo stesso nel cluster di origine e di destinazione. Se si sceglie un nuovo tipo di nodo, le query vengono eliminate.	Il ridimensionamento classico non conserva sessioni e query. Le query vengono eliminate.	Quando le query vengono eliminate, ci si può aspettare un certo peggioramento delle prestazioni. È meglio eseguire un'operazione di ridimensionamento durante un periodo di utilizzo leggero.				

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Comme
Annullamento di un'operazione di ridimensionamento	Non è possibile annullare un ridimensionamento elastico.	È possibile annullare l'operazione di ridimensionamento classico prima che sia completata, scegliendo Annulla ridimensionamento nei dettagli dei cluster nella console Amazon Redshift.	La durata dell'annullamento dell'operazione di ridimensionamento dipende dalla fase in cui si trova il ridimensionamento al momento in cui viene annullato. Il cluster non sarà disponibile fino al completam

Comportamento	Elastic resize (Ridimensionamento elastico)	Classic resize (Ridimensionamento classico)	Comme				
			<p>ento dell'operazione di annullamento. Se il ridimensionamento si trova nella fase finale, non potrai annullare l'operazione.</p> <p>Il ridimensionamento classico in un cluster RA3 non può essere annullato.</p>				

## Pianificazione di un ridimensionamento

Puoi pianificare le operazioni di ridimensionamento per il cluster in modo da aumentarlo per anticipare un utilizzo elevato o ridurlo per diminuire i costi. La pianificazione funziona sia per il ridimensionamento elastico che per il ridimensionamento classico. Puoi pianificare una query sulla console Amazon Redshift. Per ulteriori informazioni, consulta [Ridimensionamento di un cluster](#) in Gestione dei cluster tramite la console. Puoi anche utilizzare AWS CLI le nostre operazioni API di Amazon Redshift per pianificare un ridimensionamento. Per ulteriori informazioni, consulta [create-scheduled-action](#) nel AWS CLI Command Reference o [CreateScheduledAction](#) nel Amazon Redshift API Reference.

## Snapshot, ripristino e ridimensionamento

Il [ridimensionamento elastico](#) è il metodo più rapido per ridimensionare un cluster Amazon Redshift. Se il ridimensionamento elastico non è facoltativo per te e hai bisogno di un accesso in scrittura quasi costante al cluster, puoi utilizzare le operazioni di snapshot e ripristino con ridimensionamento classico descritte nella seguente sezione. Questo approccio richiede che tutti i dati scritti sul cluster di origine dopo l'acquisizione dello snapshot siano copiati manualmente nel cluster target dopo lo switch. A seconda della durata della copia, potrebbe essere necessario ripetere l'operazione varie volte fino a che non avrai gli stessi dati in entrambi i cluster. Quindi, puoi effettuare lo switch al cluster di destinazione. Questo processo può avere un impatto negativo sulle query esistenti fino a che il set di dati completo non è disponibile nel cluster di destinazione, ma riduce al minimo la durata per la quale non puoi scrivere sul database.

L'approccio mediante snapshot, ripristino e ridimensionamento classico utilizza il seguente processo:

1. Acquisire una snapshot del cluster esistente. Il cluster esistente è il cluster di origine.
2. Prendere nota dell'ora in cui è stato acquisito lo snapshot. In questo modo sarà possibile individuare in un secondo momento il punto in cui eseguire nuovamente i processi di estrazione, transazione e caricamento (ETL) per caricare i dati post-snapshot nel database di destinazione.
3. Ripristinare lo snapshot in un nuovo cluster. Questo nuovo cluster è il cluster target. Verificare la presenza dei dati di esempio nel cluster target.
4. Ridimensionare il cluster target. Scegliere il nuovo tipo di nodo, il numero di nodi e altre impostazioni per il cluster di destinazione.
5. Esaminare i caricamenti dai processi ETL avvenuti dopo l'acquisizione dello snapshot del cluster di origine. Accertarsi di ricaricare gli stessi dati nello stesso ordine nel cluster di destinazione. Nel caso di caricamenti in esecuzione, ripetere questo processo varie volte fino a che i dati non saranno gli stessi in entrambi i cluster.

6. Interrompere tutte le query in esecuzione nel cluster di origine. A questo proposito, è possibile riavviare il cluster oppure accedere come utente con privilegi avanzati e utilizzare i comandi [PG\\_CANCEL\\_BACKEND](#) e [PG\\_TERMINATE\\_BACKEND](#). Il riavvio del cluster è il modo più semplice di assicurarsi che il cluster non è disponibile.
7. Rinominare il cluster di origine. Ad esempio, cambiare il nome da `examplecluster` a `examplecluster-source`.
8. Rinominare il cluster con il nome del cluster di origine prima che venisse cambiato, ad esempio, rinominare il cluster di destinazione da precedente a `examplecluster`. Da questo momento, tutte le applicazioni che utilizzano l'endpoint contenente `examplecluster` si connettono al cluster di destinazione.
9. Eliminare il cluster di origine dopo lo switch al cluster target e verificare che tutti i processi funzionino come previsto.

In alternativa, puoi rinominare i cluster di origine e destinazione prima di ricaricare i dati nel cluster di destinazione. Questo approccio funziona se non hai la necessità di aggiornare immediatamente i sistemi e i report dipendenti con quelli del cluster di destinazione. In questo caso, la fase 6 è l'ultima del processo descritto precedentemente.

Il processo di assegnazione di un nuovo nome è necessario solo se vuoi che le applicazioni continuino a utilizzare lo stesso endpoint per connettersi al cluster. Se non c'è questa necessità, puoi invece aggiornare le applicazioni che si connettono al cluster per utilizzare l'endpoint del cluster di destinazione senza assegnare un nuovo nome al cluster.

Riutilizzare un nome di cluster presenta due vantaggi. Il primo è che non è necessario aggiornare le stringhe di connessione delle applicazioni in quanto l'endpoint non cambia, anche se ciò avviene per il cluster sottostante. In secondo luogo, gli elementi correlati come gli CloudWatch allarmi Amazon e le notifiche di Amazon Simple Notification Service (Amazon SNS) sono legati al nome del cluster. Ciò significa che puoi continuare a utilizzare gli stessi allarmi e le stesse notifiche che hai configurato per il cluster. L'esigenza di un utilizzo continuo è motivo di preoccupazione soprattutto negli ambienti di produzione, dove è necessario disporre della flessibilità di ridimensionare il cluster senza dover riconfigurare gli elementi correlati come gli allarmi e le notifiche.

## Sospensione e ripristino dei cluster

Se si dispone di un cluster che deve essere disponibile solo in orari specifici, è possibile sospendere il cluster e riprenderlo in seguito. Durante la sospensione del cluster, la fatturazione su richiesta viene

sospesa. Solo l'archiviazione del cluster comporta addebiti. Per informazioni sui prezzi, consultare la [pagina dei prezzi di Amazon Redshift](#).

Quando si sospende un cluster, Amazon Redshift crea uno snapshot, inizia a terminare le query e mette il cluster in uno stato di sospensione. Se elimini un cluster in sospensione senza richiedere uno snapshot finale, non puoi ripristinare il cluster. Non puoi annullare o ripristinare un'operazione di sospensione o riprendere dopo l'avvio.

Puoi mettere in pausa e riprendere un cluster sulla console Amazon Redshift, con o con AWS CLI le operazioni API di Amazon Redshift.

Puoi pianificare delle operazioni per sospendere e riprendere un cluster. Quando si utilizza la nuova console Amazon Redshift per creare una pianificazione ricorrente per sospendere e riprendere il cluster, vengono create due operazioni pianificate per l'intervallo di date scelto. I nomi delle operazioni pianificate sono suffissi con `-pause` e `-resume`. La lunghezza totale del nome deve corrispondere alle dimensioni massime di un nome dell'operazione pianificata.

Non puoi sospendere i seguenti tipi di cluster:

- Cluster EC2-Classical.
- Cluster che non sono attivi, ad esempio un cluster in fase di modifica.
- Cluster del modulo di sicurezza hardware (HSM).
- Cluster con gli snapshot automatizzati disattivati.

Quando decidi di sospendere un cluster, considera quanto segue:

- Le connessioni o le query al cluster non sono disponibili.
- Non è possibile visualizzare le informazioni di monitoraggio delle query di un cluster in sospensione sulla console Amazon Redshift.
- Non è possibile modificare un cluster in sospensione. Le operazioni pianificate nel cluster non vengono eseguite. Tali operazioni includono la creazione di snapshot, il ridimensionamento del cluster e le operazioni di manutenzione del cluster.
- I parametri hardware non vengono creati. Aggiorna gli CloudWatch allarmi se gli allarmi sono impostati su parametri mancanti.
- Non puoi copiare gli snapshot automatici più recenti di un cluster in sospensione su snapshot manuali.

- Mentre un cluster è in sospensione, non può essere ripreso fino al completamento dell'operazione di sospensione.
- Quando sospendi un cluster, la fatturazione viene sospesa. Tuttavia, l'operazione di sospensione viene completata in genere entro 15 minuti, a seconda delle dimensioni del cluster.
- I log di controllo vengono archiviati e non ripristinati al riavvio.
- Dopo la sospensione di un cluster, tracce e registri potrebbero non essere disponibili per la risoluzione dei problemi verificatisi prima della sospensione.
- Le tabelle senza backup sul cluster non vengono ripristinate al momento della ripresa. Per ulteriori informazioni sulle tabelle senza backup, consulta [Esclusione di tabelle dagli snapshot](#).
- Se gestisci le tue credenziali di amministratore utilizzando AWS Secrets Manager e metti in pausa il cluster, il segreto del cluster non verrà eliminato e continuerai a ricevere la fattura per il segreto. Per ulteriori informazioni sulla gestione della password di amministratore di Redshift con AWS Secrets Manager, consulta [Gestione delle password di amministrazione di Amazon Redshift tramite AWS Secrets Manager](#)

Quando riprendi un cluster, considera quanto segue:

- La versione del cluster ripristinato viene aggiornata alla versione di manutenzione in base alla finestra di manutenzione del cluster.
- Se elimini la sottorete associata a un cluster in sospensione, potresti avere una rete incompatibile. In questo caso, ripristina il cluster dall'ultimo snapshot.
- Se elimini un indirizzo IP elastico mentre il cluster è in sospensione, viene richiesto un nuovo indirizzo IP elastico.
- Se Amazon Redshift non può ripristinare il cluster con la precedente interfaccia di rete elastica, Amazon Redshift tenta di assegnarne una nuova.
- Quando ripristini un cluster, gli indirizzi IP del nodo potrebbero cambiare. Potrebbe essere necessario aggiornare le impostazioni VPC per supportare questi nuovi indirizzi IP per funzionalità come COPY da Secure Shell (SSH) o COPY da Amazon EMR.
- Se tenti di ripristinare un cluster che non è in sospensione, l'operazione di ripristino restituisce un errore. Se l'operazione di ripristino fa parte di un'operazione pianificata, modifica o elimina l'operazione pianificata per evitare errori futuri.
- A seconda delle dimensioni del cluster, è possibile che siano necessari alcuni minuti per riprendere un cluster prima che le query possano essere elaborate. Inoltre, le prestazioni delle query

possono essere influenzate per un certo periodo di tempo mentre il cluster viene ripopolato dopo il completamento del ripristino.

## Ridenominazione dei cluster

Puoi rinominare un cluster se desideri che il cluster usi un nome diverso. Poiché l'endpoint del cluster include il nome del cluster (definito anche identificatore cluster), al termine dell'operazione di ridenominazione l'endpoint viene modificato e utilizza il nuovo nome. Ad esempio, se è presente un cluster denominato `examplecluster` e decidi di rinominarlo in `newcluster`, l'endpoint viene modificato e utilizza l'identificatore `newcluster`. Tutte le applicazioni che si connettono al cluster devono essere aggiornate in base al nuovo endpoint.

Puoi rinominare un cluster se desideri modificare il cluster a cui si connettono le applicazioni senza dover modificare l'endpoint in tali applicazioni. In questo caso, devi prima rinominare il cluster originale e quindi modificare il cluster così ottenuto in modo che utilizzi il nome del cluster originale prima della ridenominazione. Questa operazione è necessaria perché l'identificatore del cluster deve essere univoco all'interno dell'account e della regione. Pertanto, il cluster originale e il secondo cluster non possono avere lo stesso nome. Potresti adottare questo approccio se, in caso di ripristino di un cluster da uno snapshot, non desideri modificare le proprietà di connessione delle applicazioni dipendenti.

### Note

Se elimini il cluster originale, eliminerai anche qualsiasi snapshot indesiderato del cluster.

Quando rinomini un cluster, lo stato del cluster cambia in `renaming` fino al completamento del processo. Il vecchio nome DNS che veniva utilizzato dal cluster viene eliminato immediatamente, anche se potrebbe rimanere memorizzato nella cache per alcuni minuti. Il nuovo nome DNS per il cluster ridenominato diventa effettivo dopo circa 10 minuti. Il cluster ridenominato non è disponibile fino a quando il nuovo nome non diventa effettivo. Il cluster verrà riavviato e qualsiasi connessione esistente al cluster verrà rilasciata. Al completamento di questa operazione, l'endpoint utilizzerà il nuovo nome. Per questo motivo, ti consigliamo di arrestare l'esecuzione delle query prima del processo di ridenominazione e quindi di riavviarle al termine dell'operazione.

Gli snapshot del cluster vengono conservati e tutti gli snapshot associati a un cluster rimangono associati a tale cluster dopo la ridenominazione. Ad esempio, supponiamo che disponi di un cluster utilizzato dal database di produzione e che il cluster disponga di numerosi snapshot. Se rinomini il

cluster e quindi lo sostituisci nell'ambiente di produzione con una snapshot, al cluster ridenominato restano comunque associati gli snapshot esistenti.

Gli CloudWatch allarmi di Amazon e le notifiche degli eventi di Amazon Simple Notification Service (Amazon SNS) sono associate al nome del cluster. Se rinomini il cluster, devi aggiornarli di conseguenza. Puoi aggiornare gli CloudWatch allarmi nella CloudWatch console e aggiornare le notifiche degli eventi di Amazon SNS nella console Amazon Redshift nel riquadro Eventi. I dati relativi a caricamento e query per il cluster continueranno a essere visualizzati sia prima che dopo la ridenominazione. Tuttavia, i dati relativi alle prestazioni vengono azzerati al termine del processo di ridenominazione.

Per ulteriori informazioni, consultare [Modifica di un cluster](#).

## Chiusura ed eliminazione di cluster

Puoi arrestare il cluster se desideri arrestarne l'esecuzione ed evitare eventuali addebiti. Quando arresti il cluster, se lo desideri puoi creare uno snapshot finale. Se viene creato uno snapshot finale, Amazon Redshift creerà uno snapshot manuale del cluster prima di arrestarlo. In seguito potrai ripristinare tale snapshot se desideri riprendere l'esecuzione del cluster e l'esecuzione di query sui dati.

Se il cluster e i relativi dati non sono più necessari, puoi arrestare il cluster senza creare uno snapshot finale. In questo caso, il cluster e i dati vengono eliminati in modo definitivo. Per ulteriori informazioni sulla chiusura e sull'eliminazione dei cluster, consultare [Eliminazione di un cluster](#).

Indipendentemente dal fatto che il cluster sia stato arrestato con uno snapshot finale manuale o meno, tutti gli snapshot automatici associati al cluster verranno eliminati dopo l'arresto del cluster. Vengono tuttavia conservati tutti gli snapshot manuali associati al cluster. Tutti gli snapshot manuali conservati, incluso lo snapshot finale opzionale, vengono addebitati alla tariffa di archiviazione di Amazon Simple Storage Service in assenza di altri cluster in esecuzione quando si arresta il cluster oppure se si supera l'archiviazione libera disponibile fornito per i cluster Amazon Redshift in esecuzione. Per ulteriori informazioni sui prezzi relativi all'archiviazione degli snapshot, consultare la [pagina dei prezzi di Amazon Redshift](#).

L'eliminazione di un cluster elimina anche tutti i segreti associati. AWS Secrets Manager

## Trasferimento del cluster

Tramite il trasferimento in Amazon Redshift si consente ad Amazon Redshift di spostare un cluster in un'altra zona di disponibilità (AZ) senza perdita di dati o modifiche alle applicazioni. Con la

rilocazione, è possibile continuare le operazioni in caso di interruzione del servizio nel cluster con un impatto minimo.

Quando il trasferimento dei cluster è abilitato, Amazon Redshift potrebbe scegliere di trasferire i cluster in alcune situazioni. In particolare, ciò si verifica quando i problemi nella zona di disponibilità corrente impediscono il funzionamento ottimale del cluster o per migliorare la disponibilità del servizio. È inoltre possibile richiamare la funzione di rilocazione nei casi in cui i vincoli delle risorse in una determinata zona di disponibilità interromperanno le operazioni del cluster. Un esempio è la possibilità di riprendere o ridimensionare un cluster. Amazon Redshift offre la funzione di rilocazione senza alcun costo aggiuntivo.

Quando un cluster Amazon Redshift viene rilocato in una nuova zona di disponibilità, il nuovo cluster ha lo stesso endpoint del cluster originale. Le applicazioni possono riconnettersi all'endpoint e continuare le operazioni senza modifiche o perdita di dati. Tuttavia, la rilocazione potrebbe non essere sempre possibile a causa di potenziali vincoli sulle risorse in una determinata zona di disponibilità.

La rilocazione del cluster Amazon Redshift è supportata solo per i tipi di istanza RA3, ad esempio ra3.16xlarge, ra3.4xlarge e ra3.xplus. I tipi di istanza RA3 utilizzano Redshift Managed Storage (RMS) come livello di archiviazione durevole. L'ultima copia dei dati di un cluster è sempre disponibile in altre zone di disponibilità di una AWS regione. In altre parole, è possibile trasferire un cluster Amazon Redshift in un'altra zona di disponibilità senza alcuna perdita di dati.

Quando si abilita il trasferimento dei cluster, Amazon Redshift esegue la migrazione del cluster in modo che sia dietro un proxy. Questa operazione consente di implementare l'accesso indipendente dalla posizione alle risorse di calcolo di un cluster. La migrazione fa sì che il cluster venga riavviato. Quando un cluster viene rilocato in un'altra zona di disponibilità, si verifica un'interruzione mentre il nuovo cluster viene riportato in linea nella nuova zona di disponibilità. Tuttavia, non è necessario apportare modifiche alle applicazioni perché l'endpoint del cluster rimane invariato anche dopo la rilocazione del cluster nella nuova zona di disponibilità.

Il trasferimento dei cluster è disabilitato per impostazione predefinita su tutti i cluster RA3. Amazon Redshift assegna come porta predefinita la porta 5439 durante la creazione di un cluster con provisioning. È possibile passare a un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215. Non utilizzare una porta non compresa negli intervalli in quanto viene generato un errore. Per modificare la porta predefinita per un cluster fornito, utilizza la console AWS CLI Amazon Redshift o l'API Amazon Redshift. Per modificare la porta predefinita per un gruppo di lavoro serverless, usa AWS CLI o l'API Serverless di Amazon Redshift.

Se si abilita il trasferimento e si utilizza l'indirizzo IP del nodo principale per accedere al cluster, assicurarsi di modificare tale accesso. Utilizzare invece l'indirizzo IP associato all'endpoint Virtual Private Cloud (VPC) del cluster. Per trovare questo indirizzo IP del cluster, individuare e utilizzare l'endpoint VPC nella sezione Rete e sicurezza dedicata alla pagina dei dettagli del cluster. Per maggiori dettagli sull'endpoint VPC, accedere alla console Amazon VPC.

È inoltre possibile utilizzare il comando AWS Command Line Interface (AWS CLI) `describe-vc-Endpoints` per ottenere l'interfaccia elastica di rete associata all'endpoint. È possibile utilizzare il comando `describe-network-interfaces` per ottenere l'indirizzo IP associato. Per ulteriori informazioni sui comandi di Amazon Redshift, consulta AWS CLI [Comandi disponibili nel AWS CLI Command Reference](#).

### Note

Ricordiamo che il trasferimento del cluster non è un prerequisito per la configurazione di funzionalità di rete aggiuntive di Redshift. Ad esempio, puoi completarlo con la [copia di snapshot tra regioni](#), per fornire maggiore resilienza all'ambiente, ma non è un requisito. Inoltre, non è necessario attivarlo per abilitare le seguenti funzionalità:

- Connessione da un VPC multiaccount o interregionale a Redshift: puoi connetterti da un cloud privato AWS virtuale (VPC) a un altro che contiene un database Redshift. In tal modo semplifichi la gestione, ad esempio, dell'accesso dei client da account o VPC diversi, senza dover fornire l'accesso VPC locale alle identità che si connettono al database. Per ulteriori informazioni, consulta [Connessione ad Amazon Redshift serverless da un endpoint VPC Redshift di un altro account o un'altra regione](#).
- Configurazione di un nome di dominio personalizzato: puoi creare un nome di dominio personalizzato, denominato anche URL personalizzato, per il cluster Amazon Redshift o il gruppo di lavoro Amazon Redshift serverless, per rendere il nome dell'endpoint più semplice e facile da ricordare. Per ulteriori informazioni, consulta [Utilizzo di un nome di dominio personalizzato per le connessioni client](#).

## Limitazioni

Durante l'utilizzo della funzione di rilocalizzazione di Amazon Redshift, è necessario tenere in considerazione seguenti le limitazioni:

- La rilocazione del cluster potrebbe non essere possibile in tutti gli scenari a causa di potenziali limitazioni delle risorse in una determinata zona di disponibilità. In questo caso, Amazon Redshift non modifica il cluster originale.
- Il trasferimento non è supportato sulle famiglie di prodotti di istanze DC2.
- Non è possibile effettuare un trasferimento tra regioni. AWS
- Per impostazione predefinita, il trasferimento di Amazon Redshift avviene sul numero di porta 5439. È anche possibile utilizzare un'altra porta compresa nell'intervallo 5431-5455 o 8191-8215.

## Attivazione del trasferimento dei cluster

Puoi attivare e gestire il trasferimento dei cluster dalla console AWS CLI Amazon Redshift e dall'API Amazon Redshift.

Per attivare il trasferimento dei cluster, definisci un gruppo di sottoreti che includa più zone di disponibilità. Se Amazon Redshift identifica più di una zona di disponibilità accessibile, Amazon Redshift ne sceglierà automaticamente una dall'elenco delle zone di disponibilità accessibili per rilocare il cluster.

Al termine della rilocazione, sarà possibile utilizzare lo stesso endpoint per accedere al cluster. Amazon Redshift elimina le risorse di calcolo del cluster originale e le restituisce al pool di risorse.

## Gestione della rilocazione mediante la console

È possibile gestire le impostazioni per la rilocazione del cluster utilizzando la console Amazon Redshift.

### Attivazione del trasferimento durante la creazione di un nuovo cluster

Utilizza la seguente procedura per attivare il trasferimento durante la creazione di un nuovo cluster.

#### Come attivare il trasferimento per un nuovo cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Per creare un cluster, scegliere Crea cluster. Per ulteriori informazioni su come creare un cluster, consulta [Amazon Redshift provisioned clusters nella Amazon Redshift Getting Started Guide](#).
4. In Backup, per Cluster relocation (Riposizionamento del cluster) scegli Enabled (Abilitato). Per impostazione predefinita, il trasferimento è disattivato.

## 5. Scegli Create cluster (Crea cluster).

### Modifica della rilocazione per un cluster esistente

Per modificare l'impostazione di rilocazione di un cluster esistente, utilizzare la procedura seguente.

Come modificare l'impostazione di rilocazione per un cluster esistente

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster). Sono elencati i cluster per il tuo account nella AWS regione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Selezionare il nome del cluster che si desidera modificare dall'elenco. Viene visualizzata la pagina dei dettagli del cluster.
4. Selezionare la scheda Manutenzione, quindi nella sezione Dettagli del backup scegliere Modificare.
5. In Backup, scegli Enabled (Abilitato). Per impostazione predefinita, il trasferimento è disattivato.
6. Scegliere Modify cluster (Modifica cluster).

### Rilocazione di un cluster

Per rilocare manualmente un cluster in un'altra zona di disponibilità, utilizzare la procedura seguente. Ciò è particolarmente utile quando si desidera verificare la configurazione di rete nelle zone di disponibilità secondarie o quando si incorre in vincoli di risorse nella zona di disponibilità corrente.

Come rilocare un cluster in un'altra zona di disponibilità

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster). Sono elencati i cluster per il tuo account nella AWS regione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Selezionare il nome del cluster da cui si desidera rimuovere i tag. Viene visualizzata la pagina dei dettagli del cluster.
4. In Operazioni, scegliere Riavvia. Viene visualizzata la pagina Crea cluster.

5. (Facoltativo) Selezionare una zona di disponibilità. Se non si sceglie una zona di disponibilità, Amazon Redshift ne sceglierà automaticamente una per conto dell'utente.

Amazon Redshift avvia la rilocazione e visualizza il cluster come In fase di rilocazione. Al termine della rilocazione, lo stato del cluster diventa Disponibile.

## Gestione della rilocazione tramite la CLI di Amazon Redshift

È possibile gestire le impostazioni per la rilocazione del cluster utilizzando l'interfaccia a riga di comando di AWS (CLI).

Con la AWS CLI, il seguente comando di esempio crea un cluster Amazon Redshift **mycluster** denominato con la rilocazione attivata.

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --
master-username enter a username --master-user-password enter a password --node-type
ra3.4xlarge --port 5439 --availability-zone-relocation
```

Se il cluster corrente utilizza una porta diversa, è necessario modificarlo in modo che utilizzi l'intervallo di porte 5431-5455 o 8191-8215 prima di modificarlo per attivare il trasferimento. Il valore predefinito è 5439. Il comando di esempio seguente modifica la porta nel caso in cui il cluster non ne utilizzi una compresa nell'intervallo fornito.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

Il seguente comando di esempio include il `availability-zone-relocation` parametro sul cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone-
relocation
```

Il seguente comando di esempio disattiva il `availability-zone-relocation` parametro sul cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --no-availability-zone-
relocation
```

Il comando di esempio seguente richiama la rilocazione nel cluster Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone us-east-1b
```

## Snapshot e backup di Amazon Redshift

### Argomenti

- [Panoramica degli snapshot](#)
- [Snapshot automatici](#)
- [Pianificazioni di snapshot automatici](#)
- [Formato di una pianificazione di snapshot](#)
- [Snapshot manuali](#)
- [Gestione dello storage di snapshot](#)
- [Esclusione di tabelle dagli snapshot](#)
- [Copia di snapshot in un'altra regione AWS](#)
- [Ripristino di un cluster da uno snapshot](#)
- [Ripristino di una tabella da uno snapshot](#)
- [Condivisione di snapshot](#)
- [Gestione di snapshot tramite la console](#)
- [Gestione delle istantanee utilizzando l' AWS CLI API Amazon Redshift](#)
- [Utilizzo di AWS Backup](#)

### Panoramica degli snapshot

Le istantanee sono point-in-time backup di un cluster. Esistono due tipi di snapshot: automatici e manuali. Amazon Redshift memorizza questi snapshot internamente in Amazon S3 utilizzando una connessione SSL (Secure Sockets Layer) crittografata.

Amazon Redshift acquisisce automaticamente snapshot incrementali che tengono traccia delle modifiche al cluster dal momento dell'esecuzione dello snapshot automatico precedente. Gli snapshot automatizzati conservano tutti i dati necessari per ripristinare un cluster da uno snapshot. Puoi creare una pianificazione degli snapshot per controllare quando vengono eseguiti gli snapshot automatici oppure acquisire uno snapshot manuale in qualsiasi momento.

Quando si esegue il ripristino da uno snapshot, Amazon Redshift crea un nuovo cluster e lo rende disponibile prima che tutti i dati vengano caricati, in modo che sia possibile iniziare immediatamente a eseguire query sul nuovo cluster. Il cluster trasmette i dati on demand dallo snapshot in risposta alle query attive, quindi carica i dati rimanenti in background.

Quando avvii un cluster, puoi impostare il periodo di conservazione degli snapshot automatici e manuali; È possibile modificare il periodo di conservazione di default degli snapshot automatici e manuali modificando il cluster. Puoi modificare il periodo di conservazione di uno snapshot manuale al momento della sua creazione oppure modificando lo snapshot stesso.

[È possibile monitorare l'avanzamento delle istantanee visualizzando i dettagli dell'istantanea nell'AWS Management Console azione describe-cluster-snapshots nella CLI o nell'azione dell'API Snapshots. DescribeCluster](#) Per uno snapshot in corso, vengono visualizzate informazioni come la dimensione dello snapshot incrementale, la velocità di trasferimento, il tempo trascorso e il tempo rimanente stimato.

Per garantire che i backup siano sempre disponibili per il cluster, Amazon Redshift archivia gli snapshot in un bucket Amazon S3 gestito internamente da Amazon Redshift. Per gestire gli addebiti di archiviazione, valutare il numero di giorni per cui è necessario conservare gli snapshot automatici e configurare il periodo di conservazione di conseguenza. Eliminare gli snapshot manuali non più necessari. Per ulteriori informazioni sui costi di archiviazione di backup, consultare la pagina dei [prezzi di Amazon Redshift](#).

## Utilizzo di istantanee e backup in Amazon Redshift Serverless

Amazon Redshift Serverless, come un cluster con provisioning, consente di eseguire un backup come point-in-time rappresentazione degli oggetti e dei dati nel namespace. Esistono due tipi di backup in Amazon Redshift Serverless: istantanee create manualmente e punti di ripristino creati automaticamente da Amazon Redshift Serverless. Puoi trovare ulteriori informazioni sull'utilizzo degli snapshot per Amazon Redshift Serverless nella pagina [Lavorare con istantanee](#) e punti di ripristino.

Puoi anche ripristinare un'istantanea da un cluster fornito in un namespace senza server. Per ulteriori informazioni, vedere [Ripristino di uno spazio dei nomi serverless da un'istantanea](#).

## Snapshot automatici

Quando gli snapshot automatici sono abilitati per un cluster, Amazon Redshift esegue periodicamente l'acquisizione degli snapshot per quel cluster. Per impostazione predefinita, Amazon Redshift acquisisce uno snapshot ogni otto ore o ogni 5 GB di modifiche dei dati per nodo, a seconda di quale evento si verifica prima. Se i dati sono più grandi di 5 GB \* come numero di nodi, il periodo

di tempo minimo tra la creazione automatica di snapshot è di 15 minuti. In alternativa, puoi creare una pianificazione degli snapshot per controllare quando vengono eseguiti gli snapshot automatici. Se utilizzi pianificazioni personalizzate, il tempo minimo tra gli snapshot automatici è di un'ora. Gli snapshot automatici sono abilitati per impostazione predefinita al momento della creazione di un cluster.

Gli snapshot automatici vengono eliminati alla fine del periodo di conservazione. Il periodo di conservazione predefinito è di un giorno, ma è possibile modificarlo usando la console Amazon Redshift oppure a livello di programmazione usando la CLI o l'API di Amazon Redshift.

Per disabilitare gli snapshot automatici, imposta il periodo di conservazione su zero. Se disabiliti gli snapshot automatici, Amazon Redshift smette di acquisire snapshot ed elimina eventuali snapshot automatici esistenti per il cluster. Non è possibile disattivare gli snapshot automatici per i tipi di nodo RA3. È possibile impostare un periodo di conservazione automatizzato del tipo di nodo RA3 compreso tra 1 e 35 giorni.

Solo Amazon Redshift può eliminare uno snapshot automatico; non è possibile eliminarlo manualmente. Amazon Redshift elimina gli snapshot automatici alla fine del periodo di conservazione, quando vengono disabilitati gli snapshot automatici per un cluster o quando si elimina il cluster. Amazon Redshift conserva l'ultimo snapshot automatizzato fino a quando non vengono disabilitati gli snapshot automatizzati o si elimina il cluster.

Se desideri conservare uno snapshot automatico per un periodo più lungo, puoi crearne una copia come snapshot manuale. Lo snapshot automatico viene conservato fino alla fine del periodo di conservazione, mentre lo snapshot manuale corrispondente viene conservato fino a quando non viene eliminato manualmente o fino alla fine del periodo di conservazione.

## Pianificazioni di snapshot automatici

Per controllare con precisione quando vengono acquisiti gli snapshot, puoi creare una pianificazione di snapshot e collegarla a uno o più cluster. Quando modifichi una pianificazione di snapshot, la pianificazione viene modificata per tutti i cluster associati. Se a un cluster non è associata una pianificazione di snapshot, il cluster utilizza la pianificazione di snapshot automatici predefinita.

Una pianificazione di snapshot è un set di regole di pianificazione. È possibile definire una regola di pianificazione semplice in base a un intervallo specificato, ad esempio ogni 8 ore o ogni 12 ore. Puoi anche aggiungere le regole per acquisire gli snapshot in determinati giorni della settimana, in momenti specifici o durante periodi specifici. Le regole possono anche essere definite usando espressioni cron di tipo Unix.

## Formato di una pianificazione di snapshot

Nella console Amazon Redshift è possibile creare una pianificazione di snapshot. Quindi, colleghi la pianificazione a un cluster per attivare la creazione di uno snapshot di sistema. Puoi collegare una pianificazione a più cluster e creare più definizioni cron in una pianificazione per attivare uno snapshot.

Puoi definire una pianificazione per gli snapshot utilizzando una sintassi cron. La definizione di queste pianificazioni usa una sintassi [cron](#) modificata di tipo Unix. L'ora specificata è espressa in [Tempo coordinato universale \(UTC\)](#). Puoi creare pianificazioni con una frequenza massima di un'ora e una precisione minima di un minuto.

Le espressioni cron modificate da Amazon Redshift hanno 3 campi obbligatori che sono separati da uno spazio.

### Sintassi

```
cron(Minutes Hours Day-of-month Month Day-of-week Year)
```

Campi	Valori	Caratteri jolly
Minuti	0-59	, - * /
Ore	0-23	, - * /
Day-of-month (Giorno del mese)	1-31	, - * ? / L W
Mese	1-12 o JAN-DEC	, - * /
Day-of-week (Giorno della settimana)	1-7 o SUN-SAT	, - * ? L #
Anno	1970–2199	, - * /

### Caratteri jolly

- Il carattere jolly , (virgola) include valori aggiuntivi. Nel campo Day-of-week, MON, WED, FRI includono lunedì, mercoledì e venerdì. I valori totali sono limitati a 24 per campo.

- Il carattere jolly - (trattino) specifica gli intervalli. Nel campo Hour<sub>r</sub>, 1-15 include le ore dall'1 alle 15 del giorno specificato.
- Il carattere jolly \* (asterisco) include tutti i valori nel campo. Nel campo Hour<sub>s</sub>, \* include ogni ora.
- Il carattere jolly / (barra) specifica gli incrementi. Nel campo Hour<sub>s</sub> puoi immettere **1/10** per specificare ogni decima ora, a partire dalla prima ora del giorno (ad esempio, 01:00, 11:00 e 21:00).
- Il carattere jolly ? (punto interrogativo) specifica un valore. Nel **Day-of-month** campo puoi inserire 7 e, se non ti interessa in che giorno della settimana è il settimo, puoi inserire? nel ay-of-week campo D.
- Il carattere jolly L nel campo Day-of-month o Day-of-week specifica l'ultimo giorno del mese o della settimana.
- Il carattere jolly W nel campo Day-of-month specifica un giorno feriale. Nel campo Day-of-month, 3W specifica il giorno più vicino al terzo giorno feriale del mese.
- Il carattere jolly # nel ay-of-week campo D specifica una determinata istanza del giorno della settimana specificato nell'arco di un mese. Ad esempio, 3#2 sarebbe il secondo martedì del mese: il 3 fa riferimento a martedì perché è il terzo giorno di ogni settimana e il 2 fa riferimento al secondo giorno di questo tipo in un mese.

#### Note

Se si utilizza un carattere '#', è possibile definire solo un'espressione nel day-of-week campo. Ad esempio, "3#1,6#3" non è valido perché viene interpretato come due espressioni.

## Limiti

- Non puoi specificare i campi Day-of-month e Day-of-week nella stessa espressione cron. Se specifichi un valore in uno dei campi, devi usare un carattere ? nell'altro campo.
- Le pianificazioni degli snapshot non supportano le seguenti frequenze:
  - Snapshot pianificati più frequentemente di uno all'ora.
  - Snapshot pianificati meno frequentemente di uno al giorno (24 ore).

Se sono presenti pianificazioni sovrapposte che determinano la pianificazione di snapshot nell'arco di un'ora, viene generato un errore di convalida.

Quando crei una pianificazione puoi utilizzare le seguenti stringhe cron di esempio.

Minuti	Ore	Giorno della settimana	Significato
0	14-20/1	TUE	Ogni ora tra le 14:00 e le 20:00 di martedì.
0	21	MON-FRI	Tutte le sere alle 21, dal lunedì al venerdì.
30	0/6	SAT-SUN	Ogni 6 ore di incremento il sabato e la domenica a partire da 30 minuti dopo la mezzanotte (00:30) di quel giorno. Ciò restituisce uno snapshot alle [00:30, 06:30, 12:30 e 18:30] ogni giorno.
30	12/4	*	Ogni 4 ore di incremento a partire dalle 12:30 ogni giorno. Pertanto, il risultato restituito è [12:30, 16:30, 20:30].

Ad esempio per eseguire una pianificazione ogni 2 ore di incremento a partire dalle 15:15 ogni giorno. Pertanto, il risultato restituito è [15:15, 17:15, 19:15, 21:15, 23:15], specifica:

```
cron(15 15/2 *)
```

Puoi creare più definizioni della pianificazione cron all'interno di una pianificazione. Ad esempio, il AWS CLI comando seguente contiene due pianificazioni cron in un'unica pianificazione.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

## Snapshot manuali

Puoi acquisire uno snapshot manuale in qualsiasi momento. Per impostazione predefinita, gli snapshot manuali vengono conservati per un periodo indefinito anche dopo l'eliminazione del cluster. Puoi specificare il periodo di conservazione al momento della creazione di uno snapshot manuale oppure cambiare tale periodo modificando lo snapshot stesso. Per ulteriori informazioni su come modificare il periodo di conservazione del registro, consultare [Modifica del periodo di conservazione di uno snapshot manuale](#).

Se uno snapshot viene eliminato, non puoi avviare nuove operazioni che fanno riferimento a tale snapshot. Se, tuttavia, è in corso un'operazione di ripristino, tale operazione verrà eseguita fino al completamento.

Amazon Redshift ha una quota che limita il numero totale di istantanee manuali che puoi creare; questa quota è per AWS account per regione. AWS Le quote di default sono elencate nella pagina [Quote e limiti in Amazon Redshift](#).

## Gestione dello storage di snapshot

Poiché gli snapshot comportano costi di archiviazione, è importante eliminarli quando non sono più necessari. Amazon Redshift elimina gli snapshot automatici e manuali alla fine dei rispettivi periodi di conservazione. Puoi anche eliminare le istantanee manuali utilizzando AWS Management Console o con il comando CLI [batch-delete-cluster-snapshots](#).

Puoi modificare il periodo di conservazione di uno snapshot manuale cambiando le relative impostazioni.

È possibile ottenere informazioni sulla quantità di archiviazione consumata dagli snapshot utilizzando la console Amazon Redshift o il comando [describe-storage](#) della CLI.

## Esclusione di tabelle dagli snapshot

Per impostazione predefinita, negli snapshot vengono incluse tutte le tabelle permanenti definite dall'utente. Se il backup di una tabella, ad esempio una tabella di gestione temporanea, non è

necessario, puoi ridurre significativamente il tempo necessario per la creazione di snapshot e il ripristino dagli snapshot. Puoi inoltre ridurre lo spazio di storage in Amazon S3 usando una tabella senza backup. Per creare una tabella senza backup, includi il parametro `BACKUP NO` quando crei la tabella. Per ulteriori informazioni, consultare [CREATE TABLE](#) e [CREATE TABLE AS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Copia di snapshot in un'altra regione AWS

Puoi configurare Amazon Redshift per copiare automaticamente le istantanee (automatizzate o manuali) di un cluster in un'altra regione. AWS Quando uno snapshot viene creato nella AWS regione principale del cluster, viene copiato in una regione secondaria. AWS Le due AWS regioni sono note rispettivamente come regione di origine e AWS regione di destinazione AWS . Se si archivia una copia delle istantanee in un'altra AWS regione, è possibile ripristinare il cluster dai dati recenti se qualcosa influisce sulla AWS regione principale. È possibile configurare il cluster per copiare le istantanee in una sola AWS regione di destinazione alla volta. Per l'elenco delle regioni di Amazon Redshift, consulta [Regioni ed endpoint](#) nei Riferimenti generali di Amazon Web Services.

Quando abiliti Amazon Redshift a copiare automaticamente gli snapshot in un'altra AWS regione, specifichi la regione di destinazione AWS in cui copiare gli snapshot. Per le istantanee automatizzate, puoi anche specificare il periodo di conservazione per conservarle nella regione di destinazione. AWS Dopo aver copiato un'istananea automatica AWS nella regione di destinazione e aver raggiunto il periodo di conservazione in quella regione, viene eliminata dalla regione di destinazione. AWS Ciò consente di mantenere l'uso di snapshot basso. Per conservare le istantanee automatiche per un periodo più o meno lungo nella AWS regione di destinazione, modifica questo periodo di conservazione.

Il periodo di conservazione impostato per le istantanee automatiche copiate AWS nella regione di destinazione è diverso dal periodo di conservazione per le istantanee automatiche nella regione di origine. AWS Il periodo di conservazione predefinito per gli snapshot copiati è di sette giorni. Tale periodo di sette giorni si applica solo agli snapshot automatici. In entrambe le regioni AWS di origine e di destinazione, gli snapshot manuali vengono eliminati manualmente o alla fine del periodo di conservazione.

Puoi disabilitare la copia degli snapshot automatici per un cluster in qualsiasi momento. Quando si disabilita questa funzionalità, le istantanee non vengono più copiate dalla regione di origine alla AWS regione di destinazione. AWS Tutte le istantanee automatiche copiate AWS nella regione di destinazione vengono eliminate quando raggiungono il limite del periodo di conservazione, a meno che non si creino copie istantanee manuali delle stesse. Queste istantanee manuali e tutte le

istantanee manuali copiate dalla regione di destinazione vengono conservate AWS nella regione di destinazione fino a quando non vengono eliminate manualmente. AWS

Per modificare la AWS regione di destinazione in cui copi le istantanee, disattiva innanzitutto la funzione di copia automatica. Quindi sarà possibile abilitarla nuovamente specificando la nuova regione AWS di destinazione.

Dopo che un'istananea è stata copiata AWS nella regione di destinazione, diventa attiva e disponibile per il ripristino.

Per copiare istantanee per cluster AWS KMS crittografati in un'altra AWS regione, crea una concessione ad Amazon Redshift per l'utilizzo di una chiave gestita dal cliente nella regione di destinazione. AWS Scegli quindi tale concessione quando abiliti la copia delle istantanee nella regione di origine. AWS Per ulteriori informazioni sulla configurazione delle autorizzazioni di copia degli snapshot, consultare [Copia di istantanee crittografate in un'altra regione AWS KMSAWS](#).

## Ripristino di un cluster da uno snapshot

Uno snapshot contiene i dati di tutti i database in esecuzione nel cluster, oltre che informazioni sul cluster, inclusi il numero di nodi, il tipo di nodi e il nome utente amministratore. Se il cluster viene ripristinato da uno snapshot, Amazon Redshift utilizza le informazioni sul cluster per creare un nuovo cluster. Quindi, ripristina tutti i database da dati di snapshot.

Per il nuovo cluster creato dallo snapshot originale, puoi scegliere la configurazione, ad esempio il tipo di nodo e il numero di nodi. Il cluster viene ripristinato nella stessa regione AWS e in una zona di disponibilità casuale scelta dal sistema, a meno che nella richiesta non venga specificata una zona di disponibilità diversa. Quando si ripristina un cluster da uno snapshot, è possibile scegliere una traccia di manutenzione compatibile per il nuovo cluster.

### Note

Quando ripristini uno snapshot in un cluster con una configurazione diversa, lo snapshot deve essere stato eseguito su un cluster con versione 1.0.10013 o successiva.

Quando è in corso un ripristino, gli eventi vengono in genere emessi nel seguente ordine:

1. RESTORE\_STARTED – REDSHIFT-EVENT-2008 inviato quando inizia il processo di ripristino.
2. RESTORE\_SUCCEEDED – REDSHIFT-EVENT-3003 inviato quando è stato creato il nuovo cluster.

Il cluster è disponibile per le query.

3. DATA\_TRANSFER\_COMPLETED – REDSHIFT-EVENT-3537 inviato una volta completato il trasferimento di dati.

#### Note

I cluster RA3 emettono solo eventi RESTORE\_STARTED e RESTORE\_SUCCEEDED. Non è necessario eseguire alcun trasferimento di dati esplicito dopo che un RESTORE ha esito positivo perché i tipi di nodo RA3 archiviano i dati nell'archiviazione gestita di Amazon Redshift. Con i nodi RA3, i dati vengono trasferiti continuamente tra i nodi RA3 e lo spazio di archiviazione gestito da Amazon Redshift come parte della normale elaborazione delle query. I nodi RA3 memorizzano automaticamente i dati hot in locale e mantengono i blocchi richiesti meno frequentemente nello spazio di archiviazione gestito da Amazon Redshift.

È possibile monitorare l'avanzamento di un ripristino richiamando l'operazione [DescribeClusters](#) API o visualizzando i dettagli del cluster in AWS Management Console. Per un ripristino in corso, vengono visualizzate informazioni come la dimensione dei dati dello snapshot, la velocità di trasferimento, il tempo trascorso e il tempo rimanente stimato. Per una descrizione di queste metriche, consulta [RestoreStatus](#).

Non è possibile usare uno snapshot per ripristinare lo stato precedente di un cluster attivo.

#### Note

Quando ripristini uno snapshot in un nuovo cluster, vengono usati il gruppo di sicurezza e il gruppo di parametri predefiniti, a meno che non vengano specificati valori diversi.

Potrebbe essere necessario ripristinare uno snapshot in un cluster con una configurazione diversa per i motivi riportati di seguito:

- Quando un cluster è costituito da tipi di nodi più piccoli e si desidera consolidarlo in un tipo di nodo più grande con un numero inferiore di nodi.
- Quando il carico di lavoro è stato monitorato ed è stata determinata la necessità di passare a un tipo di nodo con più CPU e storage.

- Quando si desidera misurare le prestazioni di carichi di lavoro di test con tipi di nodi diversi.

Il ripristino presenta le seguenti limitazioni:

- La nuova configurazione del nodo deve prevedere storage sufficiente per i dati esistenti. Anche durante l'aggiunta dei nodi, la nuova configurazione potrebbe non disporre di storage sufficiente a causa del modo in cui i dati vengono ridistribuiti.
- L'operazione di ripristino verifica se lo snapshot è stato creato in una versione del cluster compatibile con la versione del cluster del nuovo cluster. Se il nuovo cluster ha un livello di versione troppo anticipato, l'operazione di ripristino non riesce e riporta ulteriori informazioni in un messaggio di errore.
- Le possibili configurazioni (numero di nodi e tipo di nodo) che è possibile ripristinare sono determinate dal numero di nodi nel cluster originale e dal tipo di nodo di destinazione del nuovo cluster. Per determinare le possibili configurazioni disponibili, puoi utilizzare la console Amazon Redshift o `describe-node-configuration-options` AWS CLI il comando con `action-type restore-cluster` Per ulteriori informazioni sul ripristino tramite la console Amazon Redshift, consultare [Ripristino di un cluster da uno snapshot](#).

La procedura seguente accetta un cluster con molti nodi e lo consolida in un tipo di nodo più grande con un numero inferiore di nodi utilizzando AWS CLI. Per questo esempio, iniziamo con un cluster di origine costituito da 24 nodi . In questo caso, supponiamo di avere già creato uno snapshot di questo cluster e di volerlo ripristinare in un tipo di nodo più grande.

1. Per ottenere informazioni sul cluster a 24 nodi, esegui questo comando:

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier  
mycluster-123456789012
```

2. Esegui il seguente comando per ottenere informazioni sullo snapshot.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier  
mycluster-snapshot
```

3. Esegui il seguente comando per descrivere le opzioni disponibili per questo snapshot.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-  
snapshot --region eu-west-1 --action-type restore-cluster
```

Questo comando restituisce un elenco di opzioni con tipi di nodi consigliati, numero di nodi e utilizzo del disco per ogni opzione. Per questo esempio, il comando precedente elenca le seguenti possibili configurazioni nodo. Scegliamo di eseguire il ripristino in un cluster a tre nodi.

```
{
  "NodeConfigurationOptionList": [
    {
      "EstimatedDiskUtilizationPercent": 65.26134808858235,
      "NodeType": "dc2.large",
      "NumberOfNodes": 24
    },
    {
      "EstimatedDiskUtilizationPercent": 32.630674044291176,
      "NodeType": "dc2.large",
      "NumberOfNodes": 48
    },
    {
      "EstimatedDiskUtilizationPercent": 65.26134808858235,
      "NodeType": "dc2.8xlarge",
      "NumberOfNodes": 3
    },
    {
      "EstimatedDiskUtilizationPercent": 48.94601106643677,
      "NodeType": "dc2.8xlarge",
      "NumberOfNodes": 4
    },
    {
      "EstimatedDiskUtilizationPercent": 39.156808853149414,
      "NodeType": "dc2.8xlarge",
      "NumberOfNodes": 5
    },
    {
      "EstimatedDiskUtilizationPercent": 32.630674044291176,
      "NodeType": "dc2.8xlarge",
      "NumberOfNodes": 6
    }
  ]
}
```

4. Esegui il comando seguente per ripristinare lo snapshot nella configurazione cluster scelta. Dopo che questo cluster è stato ripristinato, abbiamo lo stesso contenuto del cluster di origine, ma i dati sono stati consolidati in tre nodi `dc2.8xlarge`.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type
dc2.8xlarge --number-of-nodes 3
```

Se disponi di nodi riservati, ad esempio nodi riservati DC2, puoi eseguire l'aggiornamento a nodi riservati RA3. Puoi farlo quando esegui il ripristino da una snapshot o esegui un ridimensionamento elastico. La console può guidarti attraverso questo processo. Per ulteriori informazioni sulla creazione di nodi RA3, consulta [Aggiornamento ai tipi di nodo RA3](#).

## Ripristino di una tabella da uno snapshot

È possibile ripristinare una singola tabella da uno snapshot anziché ripristinare l'intero cluster. Quando ripristini una singola tabella da uno snapshot, devi specificare lo snapshot, il database, lo schema e il nome di tabella di origine e il database, lo schema e un nuovo nome di tabella di destinazione per la tabella ripristinata.

Il nuovo nome di tabella non può corrispondere al nome di una tabella esistente. Per sostituire una tabella esistente con una tabella ripristinata da uno snapshot, rinomina o elimina la tabella esistente prima di ripristinare la tabella dallo snapshot.

La tabella di destinazione viene creata usando le definizioni di colonna, gli attributi di tabella e gli attributi di colonna della tabella di origine, a esclusione delle chiavi esterne. Per impedire conflitti dovuti alle dipendenze, la tabella di destinazione non eredita le chiavi estere dalla tabella di origine. Eventuali dipendenze, come viste o autorizzazioni concesse nella tabella di origine, non vengono applicate alla tabella di destinazione.

Se il proprietario della tabella di origine esiste, l'utente del database diventa il proprietario della tabella ripristinata, a condizione che abbia le autorizzazioni sufficienti per diventare il proprietario di una relazione nel database e nello schema specificati. In caso contrario, la tabella ripristinata è di proprietà dell'utente master creato all'avvio del cluster.

La tabella ripristinata torna allo stato in cui si trovava al momento dell'esecuzione del backup. Ciò include le regole di visibilità delle transazioni definite dall'applicazione in Amazon Redshift dell'[isolamento serializzabile](#), che prevede che i dati siano immediatamente visibili per le transazioni in corso avviate dopo il backup.

Il ripristino di una tabella da uno snapshot prevede le limitazioni seguenti:

- È possibile ripristinare una tabella solo nel cluster in esecuzione attivo e corrente e da uno snapshot acquisito da tale cluster.
- È possibile ripristinare una sola tabella per volta.
- Non è possibile ripristinare una tabella da uno snapshot di un cluster acquisito prima del ridimensionamento del cluster. Un'eccezione è che è possibile ripristinare una tabella dopo un ridimensionamento elastico se il tipo di nodo non è cambiato.
- Eventuali dipendenze, come viste o autorizzazioni concesse nella tabella di origine, non vengono applicate alla tabella di destinazione.
- Se la sicurezza a livello di riga è attivata per il ripristino di una tabella, Amazon Redshift ripristina la tabella con la sicurezza a livello di riga attivata.

Per ripristinare una tabella da uno snapshot

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster che si intende utilizzare per ripristinare una tabella.
3. Alla voce Actions (Operazioni), scegli Restore table (Ripristina tabella) per visualizzare la pagina Restore table (Ripristina tabella).
4. Inserisci le informazioni su quale snapshot, tabella di origine e tabella di destinazione da utilizzare, quindi scegli Restore table (Ripristina tabella).

Example Esempio: ripristino di una tabella da uno snapshot utilizzando il AWS CLI

L'esempio seguente utilizza il `restore-table-from-cluster-snapshot` AWS CLI comando per ripristinare la `my-source-table` tabella dallo `sample-database` schema di `my-snapshot-id`. È possibile utilizzare il AWS CLI comando `describe-table-restore-status` per verificare lo stato dell'operazione di ripristino. L'esempio ripristina lo snapshot nel cluster `mycluster-example` con un nuovo nome di tabella corrispondente a `my-new-table`.

```
aws redshift restore-table-from-cluster-snapshot --cluster-identifier mycluster-  
example --new-table-name my-new-table --snapshot-identifier my-snapshot-id
```

```
database
```

```
--source-database-name sample-
```

```
--source-table-name my-source-table
```

## Condivisione di snapshot

È possibile condividere un'istantanea manuale esistente con altri account AWS cliente autorizzando l'accesso all'istantanea. Puoi autorizzarne fino a 20 per ogni istantanea e 100 per ogni () chiave. AWS Key Management Service AWS KMS Cioè, se disponi di 10 istantanee crittografate con una singola chiave KMS, puoi autorizzare 10 AWS account a ripristinare ciascuna istantanea o altre combinazioni che sommano fino a 100 account e non superino i 20 account per ogni istantanea. Una persona connessa come utente in uno degli account autorizzati può quindi descrivere lo snapshot o ripristinarlo per creare un nuovo cluster Amazon Redshift nel proprio account. Ad esempio, se utilizzi account AWS cliente separati per la produzione e il test, un utente può accedere utilizzando l'account di produzione e condividere un'istantanea con gli utenti dell'account di test. Una persona connessa come utente dell'account di test può quindi ripristinare lo snapshot per creare un nuovo cluster di proprietà dell'account di test a scopo di test o diagnostica.

Un'istantanea manuale è permanentemente di proprietà dell'account AWS cliente con cui è stata creata. Solo gli utenti che fanno parte dell'account proprietario dello snapshot possono autorizzare altri account ad accedere allo snapshot oppure revocare le autorizzazioni. Gli utenti negli account autorizzati possono solo descrivere o ripristinare gli snapshot condivisi con loro, ma non possono copiare o eliminare tali snapshot. Un'autorizzazione rimane valida fino a quando il proprietario dello snapshot non la revoca. Se un'autorizzazione viene revocata, l'utente autorizzato in precedenza perde la visibilità dello snapshot e non può avviare nuove operazioni che fanno riferimento allo snapshot. Se l'account sta ripristinando lo snapshot quando l'accesso viene revocato, il ripristino viene completato. Non è possibile eliminare uno snapshot con autorizzazioni attive. È prima necessario revocare tutte le autorizzazioni.

AWS gli account dei clienti sono sempre autorizzati ad accedere alle istantanee di proprietà dell'account. I tentativi di autorizzare o revocare l'accesso per l'account del proprietario causano la generazione di un errore. Non è possibile ripristinare o descrivere un'istantanea di proprietà di un account cliente inattivo AWS .

Dopo aver autorizzato l'accesso a un account AWS cliente, nessun utente di quell'account può eseguire alcuna azione sullo snapshot a meno che non assuma un ruolo nell'elaborazione di politiche che gli consentano di farlo.

- Gli utenti nell'account del proprietario dello snapshot possono autorizzare e revocare l'accesso a uno snapshot solo se dispongono di un ruolo con una policy IAM che permetta loro di eseguire queste operazioni con una specifica delle risorse che include lo snapshot. Ad esempio, la seguente politica consente a un utente o a un ruolo nell' AWS account di 012345678912 autorizzare altri account ad accedere a un'istantanea denominata: my-snapshot20130829

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:AuthorizeSnapshotAccess",
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-snapshot20130829"
      ]
    }
  ]
}
```

- Gli utenti di un AWS account con cui è stata condivisa un'istantanea non possono eseguire azioni su quella istantanea a meno che non dispongano delle autorizzazioni che consentono tali azioni. A tale scopo, puoi assegnare la policy a un ruolo e quindi assumerlo.
- Per elencare o descrivere uno snapshot, è necessaria una policy IAM che permette l'operazione DescribeClusterSnapshots. Il codice seguente mostra un esempio:

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

```
}
```

- Per ripristinare uno snapshot, un utente deve disporre di un ruolo con una policy IAM che permetta l'operazione `RestoreFromClusterSnapshot` e che includa un elemento di risorsa che comprende sia il cluster che sta cercando di creare che lo snapshot. Se, ad esempio, un utente in un account `012345678912` ha condiviso lo snapshot `my-snapshot20130829` con l'account `219876543210`, per creare un cluster ripristinando lo snapshot, un utente nell'account `219876543210` deve assumere un ruolo con una policy come la seguente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:012345678912:snapshot:*/my-
snapshot20130829",
        "arn:aws:redshift:us-east-1:219876543210:cluster:from-another-account"
      ]
    }
  ]
}
```

- Dopo la revoca dell'accesso a un'istanza da un AWS account, nessun utente di quell'account può accedere all'istanza. Ciò accade anche se gli account hanno a disposizione policy IAM che permettono operazioni sulla risorsa snapshot precedentemente condivisa.

## Gestione di snapshot tramite la console

Amazon Redshift acquisisce periodicamente snapshot incrementali automatici dei dati e li salva in Amazon S3. Puoi inoltre acquisire snapshot manuali dei dati ogni volta che lo desideri. In questa sezione viene descritto come gestire gli snapshot dalla console Amazon Redshift. Per ulteriori informazioni sugli snapshot, consulta [Snapshot e backup di Amazon Redshift](#).

Tutte gli snapshot acquisiti nella console Amazon Redshift hanno come punto di partenza l'elenco di snapshot. Puoi filtrare l'elenco in base a un intervallo di tempo, un tipo di snapshot e il cluster associato allo snapshot. Inoltre, puoi ordinare l'elenco per data, dimensioni e tipo di snapshot. A

seconda del tipo di snapshot selezionato, saranno disponibili opzioni diverse per lavorare con lo snapshot stesso.

## Argomenti

- [Creazione di una pianificazione di snapshot](#)
- [Creazione di uno snapshot manuale](#)
- [Modifica del periodo di conservazione di uno snapshot manuale](#)
- [Eliminazione degli snapshot manuali](#)
- [Copia di uno snapshot automatico](#)
- [Ripristino di un cluster da uno snapshot](#)
- [Ripristino di uno spazio dei nomi serverless da uno snapshot](#)
- [Condivisione di uno snapshot di un cluster](#)
- [Configurazione della copia di snapshot tra regioni per un cluster non crittografato](#)
- [Configura una copia delle istantanee tra regioni per un cluster crittografato AWS KMS](#)
- [Modifica del periodo di conservazione per la copia di snapshot tra regioni](#)

## Creazione di una pianificazione di snapshot

Per controllare con precisione quando vengono acquisiti gli snapshot, puoi creare una pianificazione di snapshot e collegarla a uno o più cluster. Puoi collegare una pianificazione creando o modificando un cluster. Per ulteriori informazioni, consulta [Pianificazioni di snapshot automatici](#).

Per creare una pianificazione di snapshot

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere la scheda Snapshot schedules (Pianificazioni snapshot). Sono visualizzate le pianificazioni snapshot.
3. Scegli Add schedule (Aggiungi pianificazione) per visualizzare la pagina in cui è possibile aggiungere la pianificazione.
4. Inserisci le proprietà della definizione della pianificazione, quindi scegli Add schedule (Aggiungi pianificazione).
5. Nella pagina che compare, puoi collegare dei cluster alla nuova pianificazione snapshot, quindi scegli OK.

## Creazione di uno snapshot manuale

Puoi creare uno snapshot manuale di un cluster dall'elenco di snapshot come illustrato di seguito. In alternativa, puoi acquisire uno snapshot di un cluster nel riquadro di configurazione del cluster. Per ulteriori informazioni, consulta [Acquisizione di uno snapshot di un cluster](#).

### Creazione di uno snapshot manuale

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere Create snapshot (Crea snapshot). Viene visualizzata la pagina snapshot per creare uno snapshot manuale.
3. Inserisci le proprietà della definizione dello snapshot, quindi scegli Create snapshot (Crea snapshot). La disponibilità dello snapshot potrebbe richiedere del tempo.

### Modifica del periodo di conservazione di uno snapshot manuale

Puoi modificare il periodo di conservazione di uno snapshot manuale cambiando le relative impostazioni.

### Per modificare il periodo di conservazione di uno snapshot manuale

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere lo snapshot manuale da modificare.
3. Alla voce Actions (Operazioni), scegli Manual snapshot settings (Impostazioni snapshot manuale) per visualizzare le proprietà dello snapshot manuale.
4. Inserisci le proprietà della definizione dello snapshot aggiornate, quindi scegli Save (Salva).

### Eliminazione degli snapshot manuali

Puoi eliminare gli snapshot manuali selezionandone uno o diversi nel relativo elenco.

## Per eliminare uno snapshot manuale

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere lo snapshot da eliminare.
3. Alla voce Actions (Operazioni), scegli Delete Snapshot (Elimina snapshot) per eliminare lo snapshot.
4. Conferma la cancellazione degli snapshot elencati, quindi scegli Delete (Elimina).

## Copia di uno snapshot automatico

Gli snapshot automatici vengono eliminati automaticamente allo scadere del periodo di conservazione, quando disabiliti gli snapshot automatici oppure quando elimini un cluster. Se desideri conservare uno snapshot automatico, puoi copiarlo in uno snapshot manuale.

## Per copiare uno snapshot automatico

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere lo snapshot da copiare.
3. Alla voce Actions (Operazioni), scegli Copy automated snapshot (Copia snapshot automatici) per copiare lo snapshot.
4. Aggiorna le proprietà del nuovo snapshot, quindi scegli Copy (Copia).

## Ripristino di un cluster da uno snapshot

Quando si ripristina un cluster da uno snapshot, Amazon Redshift crea un nuovo cluster contenente tutti i dati dello snapshot nel nuovo cluster.

## Per ripristinare un cluster da uno snapshot

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere lo snapshot da ripristinare.

3. Scegli Restore from snapshot (Ripristina dallo snapshot) per visualizzare i valori di Cluster configuration (Configurazione del cluster) e Cluster details (Dettagli del cluster) del nuovo cluster da creare utilizzando le informazioni dello snapshot.
4. Aggiorna le proprietà del nuovo cluster, quindi scegli Restore cluster from snapshot (Ripristina cluster da uno snapshot).

Se AWS Secrets Manager non gestiva la password di amministratore del cluster, puoi fare in modo che gestisca il cluster ripristinato selezionando Gestisci le credenziali di amministratore AWS Secrets Manager nella sezione Configurazione del cluster e specificando una chiave KSM. In caso contrario, il cluster viene ripristinato con le credenziali dell'amministratore disponibili al momento dello snapshot. È possibile aggiornare le credenziali di amministratore del cluster nella pagina dei dettagli del cluster dopo il ripristino.

Se AWS Secrets Manager gestiva la password di amministratore del cluster al momento dello screenshot, devi continuare a utilizzarla AWS Secrets Manager per gestire la password di amministratore. Puoi scegliere di non utilizzare un segreto dopo aver ripristinato il cluster aggiornando le credenziali di amministratore del cluster nella pagina dei dettagli del cluster.

Se disponi di nodi riservati, ad esempio nodi riservati DC2, puoi eseguire l'aggiornamento ai nodi riservati RA3. Puoi farlo quando esegui il ripristino da una snapshot o esegui un ridimensionamento elastico. La console può guidarti attraverso questo processo. Per ulteriori informazioni sulla creazione di nodi RA3, consultare [Aggiornamento ai tipi di nodo RA3](#).

### Ripristino di uno spazio dei nomi serverless da uno snapshot

Il ripristino di uno spazio dei nomi serverless da uno snapshot sostituisce tutti i database dello spazio dei nomi con i database nello snapshot. Per ulteriori informazioni sugli snapshot serverless, consulta [Utilizzo di snapshot e punti di ripristino](#). Amazon Redshift converte automaticamente le tabelle con chiavi interlacciate in chiavi composte quando ripristini uno snapshot del cluster fornito in uno spazio dei nomi Amazon Redshift Serverless. Per ulteriori informazioni sulle chiavi di ordinamento, consulta [Utilizzo delle chiavi di ordinamento](#).

### Ripristino di uno snapshot dal cluster con provisioning nello spazio dei nomi serverless.

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Clusters (Cluster), Snapshots (Snapshot), quindi scegli lo snapshot da utilizzare.

3. Scegli Restore from snapshot (Ripristina da snapshot), Restore to serverless namespace (Ripristina su spazio dei nomi serverless).
4. Scegli lo spazio dei nomi su cui desideri eseguire il ripristino.
5. Conferma di voler eseguire il ripristino dallo snapshot. Scegli restore (ripristina). Questa operazione sostituisce tutti i database dello spazio dei nomi serverless con i dati del cluster con provisioning.

### Condivisione di uno snapshot di un cluster

Puoi autorizzare altri utenti ad accedere a uno snapshot manuale di tua proprietà e successivamente puoi revocare l'accesso, quando non è più necessario.

Per condividere uno snapshot con un altro account

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), Snapshots (Snapshot), quindi scegliere lo snapshot manuale da condividere.
3. Alla voce Actions (Operazioni), scegli Manual snapshot settings (Impostazioni snapshot manuale) per visualizzare le proprietà dello snapshot manuale.
4. Inserisci il o gli account con cui effettuare la condivisione nella sezione Manage access (Gestisci accesso), quindi scegli Save (Salva).

### Considerazioni sulla sicurezza per la condivisione di snapshot crittografati

Quando si fornisce l'accesso a un'istantanea crittografata, Redshift richiede che AWS la chiave gestita dal cliente KMS utilizzata per creare l'istantanea sia condivisa con l'account o gli account che eseguono il ripristino. Se la chiave non è condivisa, il tentativo di ripristino dello snapshot genera un errore di accesso negato. L'account di ricezione non necessita di autorizzazioni aggiuntive per ripristinare uno snapshot condiviso. Quando si autorizza l'accesso allo snapshot e si condivide la chiave, l'identità che autorizza l'accesso deve disporre delle autorizzazioni `kms:DescribeKey` sulla chiave usata per crittografare lo snapshot. Tale autorizzazione è descritta in maggiore dettaglio in [autorizzazioni AWS KMS](#). Per ulteriori informazioni, consulta la [DescribeKey](#) documentazione di riferimento dell'API Amazon Redshift.

La policy sulle chiavi gestite dal cliente può essere aggiornata a livello di codice o nella console. AWS Key Management Service

## Consentire l'accesso alla chiave AWS KMS per un'istantanea crittografata

Per condividere la chiave gestita dal cliente AWS KMS per un'istantanea crittografata, aggiorna la politica delle chiavi eseguendo le seguenti operazioni:

1. Aggiorna la politica della chiave KMS con l'Amazon Resource Name (ARN) AWS dell'account con cui stai condividendo, `Principal` come indicato nella politica delle chiavi KMS.
2. Consentire l'operazione `kms:Decrypt`.

Nel seguente esempio di policy di chiavi, l'utente `111122223333` è il proprietario della chiave KMS mentre l'utente `444455556666` è l'account con cui viene condivisa la chiave. Questa politica chiave consente all'AWS account di accedere alla chiave KMS di esempio includendo l'ARN per l'identità dell'account AWS root per `444455556666` l'utente `Principal` come criterio e `kms:Decrypt` autorizzando l'azione.

```
{
  "Id": "key-policy-1",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow use of the key",
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::111122223333:user/KeyUser",
          "arn:aws:iam::444455556666:root"
        ]
      },
      "Action": [
        "kms:Decrypt"
      ],
      "Resource": "*"
    }
  ]
}
```

Dopo aver concesso l'accesso alla chiave KMS gestita dal cliente, l'account che ripristina lo snapshot crittografato deve creare un ruolo AWS Identity and Access Management (IAM) o un utente, se non ne ha già uno. Inoltre, tale AWS account deve anche allegare una policy IAM a quel ruolo o utente

IAM che consenta loro di ripristinare uno snapshot del database crittografato, utilizzando la chiave KMS.

Per ulteriori informazioni su come concedere l'accesso a una AWS KMS chiave, consulta [Consentire agli utenti di altri account di utilizzare una chiave KMS](#), nella AWS Key Management Service guida per sviluppatori.

Per una panoramica delle politiche chiave, consulta [Come usa Amazon Redshift](#). AWS KMS

Configurazione della copia di snapshot tra regioni per un cluster non crittografato

Puoi configurare Amazon Redshift per copiare le istantanee di un cluster in un'altra regione. AWS Per configurare la copia degli snapshot tra regioni, devi abilitare questa funzione di copia per ogni cluster e configurare dove copiare gli snapshot e per quanto tempo conservare gli snapshot copiati, automatici o manuali, nella regione di destinazione. AWS Quando la copia tra regioni è abilitata per un cluster, tutte le nuove istantanee manuali e automatiche vengono copiate nella regione specificata. AWS Ai nomi degli snapshot copiati viene anteposto il prefisso **copy** :

Per configurare uno snapshot tra regioni

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster) , quindi scegliere il cluster per il quale spostare gli snapshot.
3. Per Operazioni, scegliere Configura snapshot tra regioni.

Viene visualizzata la finestra di dialogo Configura tra regioni.

4. Per Copia snapshot, scegliere Sì.
5. In AWS Regione di destinazione, scegli la AWS regione in cui copiare le istantanee.
6. In Periodo di conservazione automatica delle istantanee (giorni), scegli il numero di giorni per i quali desideri che le istantanee automatiche vengano conservate nella AWS regione di destinazione prima che vengano eliminate.
7. In Periodo di conservazione manuale delle istantanee, scegli il valore che rappresenta il numero di giorni per i quali desideri che le istantanee manuali vengano conservate nella regione di destinazione AWS prima che vengano eliminate. Se si sceglie Valore personalizzato, il periodo di conservazione deve essere compreso tra 1 e 3653 giorni.
8. Selezionare Salva.

## Configura una copia delle istantanee tra regioni per un cluster crittografato AWS KMS

Quando avvii un cluster Amazon Redshift, puoi scegliere di crittografarlo con una chiave radice da (). AWS Key Management Service AWS KMS AWS KMS le chiavi sono specifiche di una AWS regione. Se si desidera abilitare la copia di istantanee tra regioni per un cluster AWS KMS crittografato, è necessario configurare una concessione di copia delle istantanee per una chiave radice nella regione di destinazione. AWS In tal modo si consente ad Amazon Redshift di eseguire le operazioni di crittografia nella regione AWS di destinazione.

La procedura seguente descrive il processo di abilitazione della copia degli snapshot tra regioni per un cluster crittografato. AWS KMS Per ulteriori informazioni sulla crittografia in Amazon Redshift e sulle autorizzazioni di copia degli snapshot, consultare [Copia di istantanee crittografate in un'altra regione AWS KMSAWS](#).

Per configurare un'istananea interregionale per un cluster crittografato AWS KMS

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster) , quindi scegliere il cluster per il quale spostare gli snapshot.
3. Per Operazioni, scegliere Configura snapshot tra regioni.

Viene visualizzata la finestra di dialogo Configura tra regioni.

4. Per Copia snapshot, scegliere Sì.
5. In AWS Regione di destinazione, scegli la AWS regione in cui copiare le istantanee.
6. In Periodo di conservazione automatica delle istantanee (giorni), scegli il numero di giorni per i quali desideri che le istantanee automatiche vengano conservate nella AWS regione di destinazione prima che vengano eliminate.
7. In Periodo di conservazione manuale delle istantanee, scegli il valore che rappresenta il numero di giorni per i quali desideri che le istantanee manuali vengano conservate nella regione di destinazione AWS prima che vengano eliminate. Se si sceglie Valore personalizzato, il periodo di conservazione deve essere compreso tra 1 e 3653 giorni.
8. Selezionare Salva.

## Modifica del periodo di conservazione per la copia di snapshot tra regioni

Dopo aver configurato la copia di snapshot tra regioni, puoi modificare le impostazioni. Puoi modificare facilmente il periodo di conservazione selezionando un nuovo numero di giorni e salvando le modifiche.

### Warning

Non è possibile modificare la AWS regione di destinazione dopo aver configurato la copia dello snapshot tra aree geografiche.

Se desideri copiare le istantanee in una AWS regione diversa, disabilita innanzitutto la copia delle istantanee tra regioni. Quindi riattivala con una nuova AWS regione di destinazione e un nuovo periodo di conservazione. Tutti gli snapshot automatici copiati vengono eliminati dopo la disabilitazione della copia di snapshot tra regioni. Per questo motivo è necessario determinare se ce ne sono alcuni da conservare e copiarli in snapshot manuali prima di disabilitare la copia di snapshot tra regioni.

Per modificare uno snapshot tra regioni

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster per il quale modificare gli snapshot.
3. In Actions (Operazioni), scegliere Configure cross-region snapshot (Configura snapshot tra regioni) per visualizzare le proprietà dello snapshot.
4. Inserisci le proprietà della definizione dello snapshot aggiornate, quindi scegli Save (Salva).

## Gestione delle istantanee utilizzando l' AWS CLI API Amazon Redshift

Per gestire gli snapshot, è possibile usare le operazioni della CLI di Amazon Redshift elencate di seguito.

- [authorize-snapshot-access](#)
- [copy-cluster-snapshot](#)
- [create-cluster-snapshot](#)
- [delete-cluster-snapshot](#)

- [describe-cluster-snapshots](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)
- [modify-snapshot-copy-retention-period](#)
- [restore-from-cluster-snapshot](#)
- [revoke-snapshot-access](#)

Per gestire gli snapshot, è possibile usare le operazioni API di Amazon Redshift elencate di seguito.

- [AuthorizeSnapshotAccesso](#)
- [CopyClusterIstantanea](#)
- [CreateClusterIstantanea](#)
- [DeleteClusterIstantanea](#)
- [DescribeClusterIstantanee](#)
- [DisableSnapshotCopia](#)
- [EnableSnapshotCopia](#)
- [ModifySnapshotCopyRetentionPeriodo](#)
- [RestoreFromClusterSnapshot](#)
- [RevokeSnapshotAccesso](#)

Per ulteriori informazioni sugli snapshot di Amazon Redshift, consultare [Snapshot e backup di Amazon Redshift](#).

## Utilizzo di AWS Backup

AWS Backup è un servizio totalmente gestito che aiuta a centralizzare e automatizzare la protezione dei dati in tutti i servizi AWS nel cloud e on-premise.

AWS Backup per Amazon Redshift consente di configurare le policy di protezione dei dati e monitorare l'attività di diverse risorse Amazon Redshift in un'unica posizione. Permette inoltre di creare e archiviare snapshot su cluster con provisioning Amazon Redshift. In questo modo è possibile automatizzare e consolidare le attività di backup che prima dovevano essere eseguite separatamente, il tutto senza processi manuali.

Un backup, o punto di ripristino, rappresenta il contenuto di una risorsa, ad esempio un cluster Amazon Redshift, in un determinato momento. In generale un backup fa riferimento a diversi backup nei servizi AWS, come gli snapshot di Amazon Redshift. AWS Backup salva i backup in vault di backup, che è possibile organizzare in base alle esigenze aziendali. I termini punto di ripristino e backup vengono utilizzati in modo intercambiabile. Per ulteriori informazioni su AWS Backup, consulta [Utilizzo dei backup](#).

Amazon Redshift è integrato in modo nativo con AWS Backup. Ciò consente di definire i piani di backup e assegnare le risorse Amazon Redshift ai piani di backup. AWS Backup automatizza la creazione di snapshot manuali di Amazon Redshift e archivia in modo sicuro gli snapshot in un vault di backup crittografato designato nel piano di backup. Per informazioni sui vault, consulta [Utilizzo di vault di backup](#). Nel piano di backup, è possibile definire la frequenza dei backup, la finestra di backup, il ciclo di vita o il vault di backup. Per ulteriori informazioni sui piani di backup, consulta [Gestione dei backup tramite piani di backup](#).

## Argomenti

- [Considerazioni sull'utilizzo di AWS Backup con Amazon Redshift](#)
- [Gestione di AWS Backup con Amazon Redshift](#)

## Considerazioni sull'utilizzo di AWS Backup con Amazon Redshift

Le sezioni seguenti descrivono le considerazioni e le limitazioni per l'utilizzo di AWS Backup con Amazon Redshift.

## Considerazioni sull'utilizzo di AWS Backup con Amazon Redshift

Di seguito sono riportate alcune considerazioni sull'utilizzo di AWS Backup con Amazon Redshift:

- AWS Backup per Amazon Redshift è disponibile se AWS Backup e Amazon Redshift sono disponibili nelle stesse Regioni AWS. Per informazioni su dove AWS Backup è disponibile, consulta [Disponibilità delle funzionalità per Regioni AWS](#).
- Per iniziare a utilizzare AWS Backup, verifica di aver soddisfatto tutti i prerequisiti. Per ulteriori informazioni, consulta [Prerequisiti](#).
- Aderisci in modo esplicito al servizio AWS Backup. Le scelte di adesione si applicano all'account specifico e alla Regione AWS. Potrebbe essere necessario eseguire l'adesione in più regioni utilizzando lo stesso account. Per ulteriori informazioni, consulta [Nozioni di base 1: adesione al servizio](#).

- Dalla console Amazon Redshift è possibile creare snapshot manuali e automatici. Al momento AWS Backup supporta solo snapshot manuali.
- Quando utilizzi AWS Backup per gestire le impostazioni degli snapshot, non puoi continuare a gestire le impostazioni manuali degli snapshot utilizzando Amazon Redshift. Puoi però continuare a gestire le impostazioni utilizzando un piano AWS Backup. Per maggiori informazioni, consulta [Gestione dei backup tramite piani di backup](#).
- Per risparmiare sui costi di archiviazione quando si dispone di bucket Amazon S3 abilitati per il controllo delle versioni di cui eseguire il backup, è consigliabile impostare una regola di scadenza del ciclo di vita. Per informazioni sull'impostazione di una regola per il ciclo di vita, consulta [Esempio 6: specifica di una regola del ciclo di vita per un bucket che supporta la funzione di controllo delle versioni](#). Se non imposti un periodo di scadenza del ciclo di vita, i costi di archiviazione di Amazon Redshift potrebbero aumentare, perché AWS Backup mantiene tutte le versioni dei tuoi dati di Amazon Redshift.

## Restrizioni

Di seguito sono riportate le limitazioni per l'utilizzo di AWS Backup in Amazon Redshift:

- Non puoi utilizzare AWS Backup per gestire gli snapshot automatici di Amazon Redshift. Per gestire gli snapshot automatici utilizza i tag. Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta [Assegnazione di tag alle risorse in Amazon Redshift](#).
- AWS Backup non supporta Amazon Redshift serverless.

## Gestione di AWS Backup con Amazon Redshift

Per proteggere le risorse sui cluster Amazon Redshift con provisioning, puoi utilizzare la console AWS Backup o l'API AWS Backup o AWS Command Line Interface (AWS CLI) in modo programmatico. Quando è necessario ripristinare una risorsa, è possibile utilizzare la console AWS Backup o AWS CLI per trovare e ripristinare le risorse di cui si ha bisogno. Per ulteriori informazioni, consulta [AWS Command Line Interface](#).

Quando utilizzi AWS Backup per Amazon Redshift puoi:

- Creare backup periodici che avviano automaticamente gli snapshot di Amazon Redshift. I backup periodici sono utili per soddisfare le esigenze di conservazione dei dati a lungo termine. Per ulteriori informazioni, consulta [Backup di Amazon Redshift](#).

- Automatizzare la pianificazione e la conservazione dei backup configurando centralmente piani di backup.
- Ripristinare un cluster nel backup salvato che hai scelto. Sei tu a stabilire la frequenza con cui eseguire il backup delle risorse. Per ulteriori informazioni, consulta [Ripristino di un cluster Amazon Redshift](#).

## Configurazione dell'implementazione multi-AZ

Amazon Redshift supporta le implementazioni multi-AZ (con più zone di disponibilità) per cluster RA3 con provisioning. Utilizzando le implementazioni multi-AZ, il tuo data warehouse Amazon Redshift può continuare a funzionare in scenari di errore in cui si verifica un evento imprevisto in una zona di disponibilità. Un'implementazione multi-AZ distribuisce le risorse di calcolo in due zone di disponibilità a cui è possibile accedere tramite un singolo endpoint. In caso di errore dell'intera zona di disponibilità, le risorse di calcolo rimanenti nella seconda zona di disponibilità saranno disponibili per continuare l'elaborazione dei carichi di lavoro. Amazon Redshift addebita le stesse tariffe orarie di calcolo di RA3 quando si esegue un data warehouse multi-AZ. I costi di archiviazione rimangono gli stessi in quanto sono condivisi tra tutte le zone di disponibilità e nella Regione AWS.

Attualmente, Amazon Redshift supporta zero Recovery Point Objective (RPO) che consente ai dati di essere aggiornati e up-to-date in caso di guasto. Con l'implementazione multi-AZ, Amazon Redshift migliora ulteriormente le funzionalità di ripristino esistenti e riduce l'obiettivo del tempo di ripristino (RTO). Ciò è possibile perché un'implementazione multi-AZ favorisce un ripristino più rapido in caso di errore o emergenza, portando così l'Accordo sul livello di servizio (SLA) di Amazon Redshift al 99,99% rispetto al 99,9% con un data warehouse single-AZ.

## Configurazione di un'implementazione multi-AZ

Per configurare un'implementazione multi-AZ seleziona l'opzione Multi-AZ e specifica il numero di nodi di calcolo di cui eseguire il provisioning in ciascuna zona di disponibilità. Amazon Redshift implementa automaticamente risorse di elaborazione uguali in due zone di disponibilità e tutte le risorse di calcolo sono sempre disponibili per l'elaborazione delle operazioni di lettura e scrittura durante il normale funzionamento. In tal modo un'implementazione multi-AZ può agire come un unico data warehouse con un singolo endpoint, eliminando la necessità di modificare le applicazioni in caso di emergenza. Sebbene un'implementazione multi-AZ elabori una singola query utilizzando le risorse di calcolo che risiedono in una sola zona di disponibilità, può distribuire automaticamente l'elaborazione di più query simultanee su entrambe le zone di disponibilità per aumentare la velocità di trasmissione effettiva complessiva per i carichi di lavoro a elevata simultaneità.

È anche possibile convertire un data warehouse single-AZ esistente in un data warehouse multi-AZ o viceversa. Tutto rimane invariato, a eccezione del fatto che nella seconda zona di disponibilità vengono fornite risorse di calcolo aggiuntive. Durante la migrazione a multi-AZ da un cluster single-AZ esistente, potrebbe essere necessario raddoppiare il numero di nodi del cluster per facilitare il mantenimento delle prestazioni delle singole query. La maggior parte dei carichi di lavoro registra un aumento generale della velocità di trasmissione effettiva di elaborazione delle query con un data warehouse multi-AZ, in quanto la quantità di risorse di elaborazione disponibili è raddoppiata.

In caso di guasto in una zona di disponibilità, Amazon Redshift continua a operare utilizzando automaticamente le risorse nella zona di disponibilità rimanente. Tuttavia, le connessioni dell'utente potrebbero andare perse e dover essere ristabilite. Inoltre, le query in esecuzione nella zona di disponibilità in cui si è verificato l'errore possono non riuscire e devono essere ritentate. Tuttavia, puoi riconnetterti al cluster e ripianificare le query immediatamente in modo da permettere ad Amazon Redshift di elaborarle nella restante zona di disponibilità. Le query eseguite durante o dopo il verificarsi di un guasto potrebbero subire ritardi di esecuzione durante il ripristino del data warehouse multi-AZ.

#### Note

Per ottenere prestazioni migliori e maggiore disponibilità, ti consigliamo di utilizzare l'opzione `SNAPSHOT ISOLATION` con i cluster multi-AZ. Per ulteriori informazioni, consulta la pagina [CREATE DATABASE](#).

## Limitazioni

Un data warehouse multi-AZ ha le stesse capacità funzionali di un data warehouse single-AZ, a eccezione delle seguenti limitazioni che si applicano al data warehouse multi-AZ:

- Non è possibile creare un data warehouse multi-AZ non crittografato. Assicurati di aggiungere la crittografia quando crei un nuovo data warehouse multi-AZ, converti un data warehouse single-AZ in un data warehouse multi-AZ o converti un data warehouse single-AZ in un data warehouse multi-AZ.
- Non è possibile creare un'implementazione multi-AZ a nodo singolo per nessuno dei tipi di istanze RA3. Seleziona 2 o più nodi per zona di disponibilità durante la creazione di un'implementazione multi-AZ.
- Amazon Redshift non supporta la configurazione di una sottorete per meno di tre zone di disponibilità. In altre parole, il gruppo di sottoreti configurato richiede più di tre sottoreti.

- Non è possibile utilizzare un'implementazione multi-AZ in un'altra zona di disponibilità. Quando si utilizza un'implementazione multi-AZ, il trasferimento viene determinato e condotto automaticamente da Amazon Redshift.
- Non è possibile sospendere o riprendere un'implementazione multi-AZ.
- Non è possibile eseguire l'implementazione multi-AZ al di fuori degli intervalli di porte supportati da 5431 a 5455 e da 8191 a 8215.
- Non è possibile utilizzare le viste STL, SVCS, SVL, SVV, STV con le implementazioni multi-AZ perché supportano solo le viste di monitoraggio del sistema (viste SYS\_\*). Modifica le query di monitoraggio per utilizzare le viste di monitoraggio del sistema (viste SYS\_\*).
- Non è possibile collegare un indirizzo IP elastico a un cluster esistente con Multi-AZ abilitato.
- Non è possibile convertire un cluster con un indirizzo IP elastico collegato da Single-AZ a Multi-AZ.
- L'implementazione di Amazon Redshift Multi-AZ è disponibile nelle seguenti versioni: Regioni AWS
  - Stati Uniti orientali (Ohio) (us-east-2)
  - Stati Uniti orientali (Virginia settentrionale) (us-east-1)
  - Stati Uniti occidentali (Oregon) (us-west-2)
  - Africa (Città del Capo) (af-south-1)
  - Asia Pacifico (Hong Kong) ap-east-1
  - Asia Pacifico (Hyderabad) (ap-south-2)
  - Asia Pacifico (Giacarta) (ap-southeast-3)
  - Asia Pacifico (Melbourne) (ap-southeast-4)
  - Asia Pacifico (Mumbai) (ap-south-1)
  - Asia Pacifico (Osaka-Locale) (ap-northeast-3)
  - Asia Pacifico (Seoul) (ap-northeast-2)
  - Asia Pacifico (Singapore) (ap-southeast-1)
  - Asia Pacifico (Sydney) (ap-southeast-2)
  - Asia Pacifico (Tokyo) (ap-northeast-1)
  - Canada (Centrale) (ca-central-1)
  - Europa (Francoforte) (eu-central-1)
  - Europa (Irlanda) (eu-west-1)
  - Europa (Milano) (eu-south-1)
  - Europa (Parigi) (eu-west-3)

- Europa (Spagna) (eu-south-2)
- Europa (Stoccolma) (eu-north-1)
- Europa (Zurigo) (eu-central-2)
- Israele (Tel Aviv) (il-central-1)
- Medio Oriente (Bahrein) (me-south-1)
- Medio Oriente (EAU) (me-central-1)

## Argomenti

- [Gestione di un'implementazione multi-AZ](#)
- [Errore dell'implementazione multi-AZ](#)
- [Monitoraggio delle query per Multi-AZ](#)

## Gestione di un'implementazione multi-AZ

La funzionalità multi-AZ di Amazon Redshift supporta due zone di disponibilità alla volta. Amazon Redshift seleziona automaticamente le zone di disponibilità in base alla configurazione del gruppo di sottoreti selezionata. Puoi convertire un data warehouse esistente con una singola zona di disponibilità in un data warehouse multi-AZ o eseguire il ripristino da uno snapshot e configurarlo in un data warehouse multi-AZ.

Utilizzando la console Amazon Redshift puoi creare facilmente nuove implementazioni multi-AZ. Per creare una nuova implementazione multi-AZ utilizzando la console Amazon Redshift, seleziona l'opzione multi-AZ durante la creazione del data warehouse. Specifica il numero di nodi di calcolo richiesti in una singola zona di disponibilità per permettere ad Amazon Redshift di distribuirli in ciascuna delle due zone di disponibilità. Tutti i nodi sono usati per eseguire l'elaborazione del carico di lavoro in lettura e scrittura durante il normale funzionamento. Puoi anche usare il AWS CLI `create-cluster` comando per creare un nuovo data warehouse Multi-AZ utilizzando il parametro. `multi-az`

Puoi convertire un data warehouse Single-AZ esistente in un data warehouse Multi-AZ, puoi utilizzare la console Amazon Redshift o il comando che utilizza AWS CLI `modify-cluster` il parametro. `multi-az` In alternativa, puoi eseguire il ripristino da uno snapshot per configurare un data warehouse Single-AZ in un data warehouse Multi-AZ utilizzando la console Amazon Redshift o il comando che utilizza il AWS CLI `restore-from-cluster-snapshot` parametro. `multi-az`

L'implementazione multi-AZ supporta solo i tipi di nodi RA3 che utilizzano Amazon Redshift Managed Storage (RMS). Amazon Redshift archivia i dati in RMS, che utilizza Amazon S3 ed è accessibile in tutte le zone di disponibilità in un unico sistema Regione AWS, senza dover replicare i dati a livello di Amazon Redshift.

## Configurazione di implementazioni multi-AZ durante la creazione di un nuovo cluster

Puoi configurare un'implementazione multi-AZ durante la creazione di un nuovo cluster utilizzando la console Amazon Redshift o l' AWS Command Line Interface.

### Utilizzo della console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo dei cluster con provisioning) e seleziona Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegli il pulsante Crea cluster per aprire la pagina di creazione del cluster.
4. Inserisci le proprietà del cluster. Per informazioni generali sulla creazione di cluster, consulta [Creazione di un cluster](#).
5. Seleziona uno dei tipi di nodo RA3 dall'elenco a discesa Node type (Tipo di nodo). L'opzione Configurazione AZ diventa disponibile solo quando selezioni un tipo di nodo RA3.
6. In Configurazione AZ scegli Multi-AZ.
7. In Numero di nodi per AZ inserisci almeno due nodi per il cluster.
8. Hai la possibilità di caricare i dati di esempio o utilizzare dati forniti da te:
  - In Dati campione, scegliere Carica dati di esempio per caricare il set di dati di esempio nel cluster Amazon Redshift. Amazon Redshift carica il set di dati Tackit di esempio nel database dev e nello schema pubblico predefiniti. Amazon Redshift carica automaticamente il set di dati di esempio nel cluster Amazon Redshift. È possibile iniziare a utilizzare l'editor di query v2 per eseguire query sui dati.
  - Per utilizzare i dati da te forniti nel cluster Amazon Redshift, attieniti alla procedura riportata in [Utilizzo dei propri dati in Amazon Redshift](#).
9. Scorri verso il basso fino a Additional configurations (Configurazioni aggiuntive), espandi Network and security (Rete e sicurezza) e assicurati di accettare il Cluster subnet group

- (Gruppo di sottoreti del cluster) predefinito o di sceglierne un altro. Se scegli un altro gruppo di sottoreti del cluster, assicurati che siano presenti 3 zone di disponibilità nel gruppo di sottoreti selezionato.
10. In **Additional configurations (Configurazioni aggiuntive)**, espandi **Database configurations (Configurazioni del database)**.
  11. Per utilizzare una AWS KMS chiave personalizzata anziché la AWS Key Management Service chiave predefinita, fai clic su **Personalizza le impostazioni di crittografia** in **Crittografia del database**.
  12. In **Scegli una chiave KMS**, puoi scegliere una AWS Key Management Service chiave o inserire un ARN. In alternativa, puoi fare clic su **Crea una AWS Key Management Service chiave** nella AWS Key Management Service console. Per ulteriori informazioni sulla creazione di chiavi KMS, consultare [Creazione di chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .
  13. Fai clic su **Create cluster (Crea cluster)**. Quando la creazione del cluster ha esito positivo, puoi visualizzare i dettagli nella pagina dei dettagli del cluster. Puoi usare il tuo client SQL per caricare i dati ed eseguire query su di essi.

## Usando il AWS Command Line Interface

Per configurare Multi-AZ durante la creazione di un cluster utilizzando AWS Command Line Interface

- Da qui AWS CLI utilizzare il `create-cluster` comando e il `multi-az` parametro come segue.

```
aws redshift create-cluster
  --port 5439
  --master-username master
  --master-user-password #####
  --node-type ra3.4xlarge
  --number-of-nodes 2
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz
  --multi-az
  --maintenance-track-name CURRENT
  --encrypted
```

## Conversione di un data warehouse single-AZ in un data warehouse multi-AZ

Convertendo un data warehouse single-AZ in un data warehouse multi-AZ, il data warehouse diventa altamente disponibile con una garanzia dell'Accordo sul livello di servizio (SLA) del 99,99%. Le prestazioni di una singola query rimangono invariate anche con un data warehouse multi-AZ. Per carichi di lavoro a elevata simultaneità noterai un aumento generale della velocità di trasmissione effettiva perché Amazon Redshift può eseguire le richieste utilizzando risorse di calcolo in due zone di disponibilità.

### Note

Amazon Redshift non ti consente di suddividere le risorse di calcolo esistenti durante la conversione da single-AZ a multi-AZ o viceversa. Questa operazione non è supportata per mantenere costanti le prestazioni delle singole query.

### Utilizzo della console

Per convertire un cluster single-AZ in un data warehouse multi-AZ utilizzando la console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo dei cluster con provisioning) e seleziona Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegli il cluster che desideri convertire in un'implementazione multi-AZ. Viene visualizzata la pagina dei dettagli del cluster.
4. In Operazioni scegli Attiva Multi-AZ. Viene visualizzato il riepilogo delle modifiche. Fai clic su Attiva Multi-AZ.
5. In caso di errore, esegui una delle operazioni indicate di seguito, quindi fai clic su Attiva Multi-AZ.
  - Crittografia del cluster: scegli Proprietà per modificare le impostazioni di crittografia nella sezione Configurazione del database della scheda Proprietà della pagina dei dettagli del cluster.
  - Gruppo di sottoreti: scegli Gruppo di sottoreti per modificare le impostazioni del gruppo di sottoreti del cluster facendo clic sul collegamento del gruppo di sottoreti. Se scegli un altro

gruppo di sottoreti del cluster, assicurati che siano presenti 3 zone di disponibilità nel gruppo di sottoreti selezionato.

- Impostazioni della porta: scegli Proprietà per modificare l'impostazione della porta nella sezione Configurazione del database della scheda Proprietà della pagina dei dettagli del cluster.

6. Puoi usare il tuo client SQL per caricare i dati ed eseguire query su di essi.

### Usando il AWS Command Line Interface

- Da AWS CLI, utilizzare il `modify-cluster` comando e il `multi-az` parametro come segue.

```
aws redshift modify-cluster
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
  --multi-az
```

## Conversione di un data warehouse multi-AZ in un data warehouse single-AZ

Convertendo un data warehouse multi-AZ in un data warehouse single-AZ, il data warehouse non otterrà la garanzia dell'Accordo sul livello di servizio (SLA) del 99,99% offerta da Multi-AZ. Le prestazioni di una singola query rimangono invariate, ma la velocità di trasmissione effettiva complessiva ne risente perché le risorse di elaborazione nella seconda zona di disponibilità non sono disponibili. Hai la possibilità di abilitare il dimensionamento simultaneo per dimensionare automaticamente la velocità di trasmissione effettiva e ottenere prestazioni costanti anche con Single-AZ.

### Note

Amazon Redshift non ti consente di suddividere le risorse di calcolo esistenti durante la conversione da single-AZ a multi-AZ o viceversa. Questa operazione non è supportata per mantenere costanti le prestazioni delle singole query.

## Utilizzo della console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo dei cluster con provisioning) e seleziona Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegli il cluster che desideri convertire in un'implementazione multi-AZ. Viene visualizzata la pagina dei dettagli del cluster.
4. In Operazioni scegli Disattiva Multi-AZ. Viene visualizzato il riepilogo delle modifiche. Fai clic su Disattiva Multi-AZ.

## Usando il AWS Command Line Interface

- Da AWS CLI, utilizzare il `modify-cluster` comando e il `no-multi-az` parametro come segue.

```
aws redshift modify-cluster
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
  --no-multi-az
```

Una volta convertito in Single-AZ, il data warehouse perde la garanzia dell'Accordo sul livello di servizio (SLA) del 99,99%. Anche la velocità di trasmissione effettiva complessiva ne risente. Quando le modifiche vengono salvate, puoi visualizzare le informazioni nella pagina dei dettagli del cluster.

## Ridimensionamento di un data warehouse multi-AZ

È possibile ridimensionare un data warehouse multi-AZ e specificare un numero di nodi o un tipo di nodo diverso da quello della configurazione corrente del data warehouse.

## Utilizzo della console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo dei cluster con provisioning) e seleziona Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegli il cluster per cui desideri ridimensionare il data warehouse multi-AZ. Viene visualizzata la pagina dei dettagli del cluster.
4. In Actions (Operazioni), scegli Resize (Ridimensiona). Appare la pagina Resize cluster (Ridimensiona cluster).
5. Segui le istruzioni visualizzate nella pagina. È possibile ridimensionare il cluster ora, una volta in un momento specifico oppure aumentare e diminuire le dimensioni del cluster in base a una pianificazione.
6. In Nuove configurazioni seleziona uno dei tipi di nodo RA3 dall'elenco a discesa Tipo di nodo.
7. Fai clic su Ridimensiona cluster.

## Usando il AWS Command Line Interface

Per ridimensionare un data warehouse Multi-AZ utilizzando il AWS Command Line Interface

- Da AWS CLI, utilizzare il `resize-cluster` comando per modificare il numero di nodi per una singola zona di disponibilità come segue.

```
aws redshift resize-cluster \  
  --cluster-identifier test-maz-11 \  
  --cluster-type multi-node \  
  --node-type ra3.4xlarge \  
  --number-of-nodes 6
```

## Configurazione di Multi-AZ per un data warehouse ripristinato da uno snapshot

Puoi creare un cluster multi-AZ anche ripristinandolo da uno snapshot.

### Utilizzo della console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegli Clusters (Cluster), Snapshots (Snapshot), quindi scegli lo snapshot da utilizzare.

3. Scegli Restore snapshot (Ripristina snapshot), Restore to a provisioned cluster (Ripristina su un cluster con provisioning).
4. Inserisci le proprietà per il cluster. Per informazioni generali sulla creazione di cluster, consulta [Creazione di un cluster](#).
5. Seleziona uno dei tipi di nodo RA3 dall'elenco a discesa Node type (Tipo di nodo). L'opzione Configurazione AZ diventa disponibile solo quando selezioni un tipo di nodo RA3.
6. In Configurazione AZ scegli Multi-AZ.
7. In Numero di nodi per AZ inserisci almeno due nodi per il cluster.
8. Hai la possibilità di caricare i dati di esempio o utilizzare dati forniti da te:
  - In Dati campione, scegliere Carica dati di esempio per caricare il set di dati di esempio nel cluster Amazon Redshift. Amazon Redshift carica il set di dati Tockit di esempio nel database dev e nello schema pubblico predefiniti. Amazon Redshift carica automaticamente il set di dati di esempio nel cluster Amazon Redshift. È possibile iniziare a utilizzare l'editor di query v2 per eseguire query sui dati.
  - Per trasferire i tuoi dati nel tuo cluster Amazon Redshift, segui la procedura descritta in [Caricare dati da Amazon S3 ad Amazon Redshift](#).
9. Scorri verso il basso fino a Additional configurations (Configurazioni aggiuntive), espandi Network and security (Rete e sicurezza) e assicurati di accettare il Cluster subnet group (Gruppo di sottoreti del cluster) predefinito o di sceglierne un altro. Se scegli un altro gruppo di sottoreti del cluster, assicurati che siano presenti 3 zone di disponibilità nel gruppo di sottoreti selezionato.
10. In Additional configurations (Configurazioni aggiuntive), espandi Database configurations (Configurazioni del database).
11. In Crittografia del database, per utilizzare una chiave KMS personalizzata diversa dalla AWS Key Management Service chiave predefinita, fai clic su Personalizza le impostazioni di crittografia. Questa opzione è deselezionata per impostazione predefinita.
12. In Scegli una chiave KMS, puoi scegliere una AWS Key Management Service chiave o inserire un ARN. In alternativa, puoi fare clic su Crea una AWS Key Management Service chiave nella AWS Key Management Service console. Per ulteriori informazioni sulla creazione di chiavi KMS, consultare [Creazione di chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .
13. Fai clic su Restore cluster from snapshot (Ripristina cluster da snapshot). Quando il ripristino del cluster ha esito positivo, puoi visualizzare i dettagli nella pagina dei dettagli del cluster.

## Usando il AWS Command Line Interface

- Da AWS CLI, utilizzare il `restore-from-cluster-snapshot` comando come segue.

```
aws redshift restore-from-cluster-snapshot
--region eu-west-1
--multi-az
--snapshot-identifier test-snap1
--cluster-identifier test-saz-11
--endpoint-url https://redshift.eu-west-1.amazonaws.com/
```

## Errore dell'implementazione multi-AZ

Il data warehouse multi-AZ è una raccolta di risorse di calcolo distribuite contemporaneamente in due zone di disponibilità. Le risorse di calcolo distribuite nella zona di disponibilità primaria sono denominate risorse di calcolo primarie e quelle della zona di disponibilità secondaria sono denominate risorse di calcolo secondarie. Un data warehouse multi-AZ può essere ripristinato automaticamente senza l'intervento dell'utente nel caso di un evento improbabile, ad esempio un errore della zona di disponibilità o dell'infrastruttura. Il processo di ripristino prevede il failover dalla risorsa di calcolo primaria nella risorsa di calcolo secondaria e la designazione delle risorse di calcolo secondarie come primarie. Inoltre, vengono fornite nuove risorse di calcolo secondarie in una terza zona di disponibilità. Il processo di ripristino automatico viene misurato in termini di RTO e RPO.

- Obiettivo del tempo di ripristino (RTO): il tempo necessario a un sistema per tornare in uno stato funzionante dopo un'emergenza. In altre parole, l'RTO misura i tempi di inattività.
- Obiettivo del punto di ripristino (RPO): la quantità di dati che possono essere persi (misurata nel tempo). Per un data warehouse multi-AZ Amazon Redshift, l'obiettivo del punto di ripristino (RPO) è in genere pari a zero perché tutti i dati sono archiviati in Amazon Redshift Managed Storage (RMS), supportato da Amazon Simple Storage Service, che è un servizio altamente durevole e disponibile per impostazione predefinita.

### Note

Le prestazioni di una singola query non cambiano dopo che si è verificato un failover. La velocità di trasmissione effettiva complessiva del data warehouse viene ridotta per un breve periodo a causa dell'indisponibilità delle risorse di calcolo in una delle zone di disponibilità. Tuttavia, Amazon Redshift acquisisce automaticamente capacità in un'altra zona

di disponibilità per garantire il ripristino della medesima capacità di elaborazione del data warehouse.

Oltre che automaticamente, puoi attivare il processo di ripristino anche manualmente per il data warehouse utilizzando l'opzione Calcolo primario con failover. Puoi utilizzare questo approccio per testare in che modo Multi-AZ può aiutare la tua applicazione a garantire una maggiore disponibilità e una migliore continuità.

### Utilizzo della console

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Esegui una di queste operazioni:
  - Dal menu di navigazione, scegliere Clusters (Cluster). In Clusters (Cluster), scegli un cluster. Viene visualizzata la pagina dei dettagli del cluster.
  - Dal pannello di controllo del cluster, scegli un cluster.
3. In Operazioni scegli Calcolo primario con failover.
4. Quando richiesto, fai clic su Confirm (Conferma).

### Usando il AWS Command Line Interface

- Da AWS CLI, utilizzare il `failover-primary-compute` comando come segue.

```
aws redshift failover-primary-compute
  --profile maz-test
  --endpoint-url https://redshift.eu-west-1.amazonaws.com
  --region eu-west-1
  --cluster-identifier test-maz-11
```

Dopo la conferma dell'operazione sopra descritta, Amazon Redshift esegue gli stessi passaggi del ripristino automatico da un errore della zona di disponibilità o dell'infrastruttura. Il processo rende indisponibili i nodi di calcolo nella zona di disponibilità primaria e le risorse di calcolo nella zona di disponibilità secondaria vengono designate come risorse di calcolo primarie. Quando il ripristino del cluster viene completato, l'implementazione multi-AZ diventa disponibile. Il data warehouse multi-AZ

esegue inoltre al provisioning automatico di nuove risorse di calcolo secondarie in una terza zona di disponibilità non appena disponibile.

Durante questo processo, lo stato del cluster sulla console cambia costantemente, poiché il cluster viene ripristinato e riconfigurato automaticamente secondo la configurazione dell'implementazione multi-AZ. Il cluster può accettare nuove connessioni immediatamente. Le connessioni esistenti e le query in transito potrebbero essere eliminate. Puoi provare a rieseguirle immediatamente.

## Monitoraggio delle query per Multi-AZ

È possibile visualizzare le informazioni sulle query eseguite negli ultimi 7 giorni indipendentemente dal tipo, dalle dimensioni e dallo stato (sospeso o ripreso) del cluster.

### Visualizzazione di query e caricamenti per data warehouse multi-AZ

Le informazioni mostrate nella pagina relativa a query e caricamenti sono compilate con informazioni provenienti dalle tabelle di sistema Amazon Redshift (viste SYS\_\*). Queste informazioni ti consentono di visualizzare informazioni aggiuntive sulle tue query e sulle offerte per 7 giorni consecutivi. La diagnostica delle query diventa più rapida e consente di filtrare i dati per database, nome utente o tipo di istruzione SQL. Per visualizzare questi filtri e informazioni aggiuntivi su tutte le query eseguite, tieni presente i seguenti prerequisiti:

- È necessario connettersi a un database scegliendo Connect to database (Connettiti al database).
- L'utente del database deve disporre dei ruoli e delle autorizzazioni sys:operator o sys:monitor per eseguire il monitoraggio delle query. Per informazioni sui ruoli di sistema, consulta [Ruoli definiti dal sistema di Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Visualizzerai questi filtri aggiuntivi e le informazioni sulle query una volta effettuata la connessione a un database.

Come visualizzare i dati sulle prestazioni delle query provenienti da Queries and loads (Query e caricamenti)

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Queries and loads (Query e carichi) per visualizzare l'elenco delle query dell'account.

3. Potrebbe doverti connetterei a un database per utilizzare un filtro aggiuntivo. Se necessario, fai clic su **Connect to database** (Connettiti al database) e segui le istruzioni per connetterti a un database.

Per impostazione predefinita, l'elenco visualizza le query di tutti i cluster delle ultime 24 ore. Puoi modificare l'ambito della data visualizzata nella console.

Come visualizzare i dati sulle prestazioni delle query da Query monitoring (Monitoraggio della query)

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere **Clusters** (Cluster). In **Clusters** (Cluster), seleziona un cluster.
3. Seleziona **Query monitoring** (Monitoraggio della query).
4. A seconda della configurazione o della versione del cluster, potrebbe essere necessario connettersi a un database per visualizzare filtri aggiuntivi. Se necessario, fai clic su **Connect to database** (Connettiti al database) e segui le istruzioni per connetterti a un database.

## Monitoraggio di una query in un'implementazione multi-AZ

Un'implementazione multi-AZ utilizza risorse di calcolo distribuite in entrambe le zone di disponibilità e può continuare a funzionare nel caso in cui le risorse in una determinata zona di disponibilità non siano disponibili. Tutte le risorse di calcolo verranno utilizzate in ogni momento. Ciò consente il funzionamento completo su due zone di disponibilità in modo attivo-attivo sia per le operazioni di lettura che di scrittura.

È possibile eseguire query sulle viste `SYS_` nello schema `pg_catalog` per monitorare l'esecuzione delle query in un'implementazione multi-AZ. Le viste `SYS_` mostrano le attività o le statistiche dell'esecuzione delle query dai cluster principali e secondari. Per l'elenco delle viste di monitoraggio, consulta [Viste di monitoraggio](#).

Attieniti a questa procedura per monitorare l'esecuzione delle query per ogni zona di disponibilità all'interno dell'implementazione multi-AZ:

1. Accedi alla console Amazon Redshift e connettiti al database nella tua implementazione multi-AZ ed esegui le query tramite l'editor di query.
2. Esegui qualsiasi query di esempio sull'implementazione multi-AZ di Amazon Redshift.

3. Per un'implementazione multi-AZ, è possibile identificare una query e la zona di disponibilità in cui viene eseguita utilizzando la colonna `compute_type` nella tabella `SYS_QUERY_HISTORY`. `primary` indica le query eseguite sul cluster principale nell'implementazione multi-AZ e `secondary` indica le query eseguite sul cluster secondario nell'implementazione multi-AZ.

La seguente query utilizza la colonna `compute_type` per monitorare una query.

```
select (compute_type) as compute_type, left(query_text, 50) query_text from
sys_query_history order by start_time desc;
```

```
compute_type | query_text
```

```
-----+-----
```

```
secondary | select count(*) from t1;
```

## Terminazione di una query per i cluster

### Terminazione di una query per i cluster

La procedura è applicabile sia ai cluster multi-AZ che a quelli single-AZ.

Per terminare una query

Puoi utilizzare la pagina `Queries (Query)` anche per terminare una query in esecuzione.

L'utente del database deve disporre del ruolo `sys:operator` e delle autorizzazioni per terminare una query in esecuzione. Per informazioni sui ruoli di sistema, consulta [Ruoli definiti dal sistema di Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere `Queries and loads (Query e carichi)` per visualizzare l'elenco delle query dell'account.
3. Scegli la query in esecuzione che desideri terminare nell'elenco e quindi scegli `Terminate query (Termina query)`.

## Gestione dei cluster con la console

Per creare, modificare, ridimensionare, eliminare, riavviare e creare copie di backup dei cluster, utilizzare la sezione `Cluster` della console Amazon Redshift.

## Per visualizzare i cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster). Sono elencati i cluster per il tuo account nella AWS regione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster. Se non disponi di nessun cluster, scegli Create cluster (Crea cluster) per crearne uno.
3. Per visualizzare ulteriori dettagli di un cluster, scegli il nome del cluster nell'elenco.

## Argomenti

- [Creazione di un cluster](#)
- [Creazione di un cluster di anteprima](#)
- [Modifica di un cluster](#)
- [Eliminazione di un cluster](#)
- [Riavvio di un cluster](#)
- [Ridimensionamento di un cluster](#)
- [Per aggiornare una versione di rilascio del cluster](#)
- [Recupero di informazioni sulla configurazione del cluster](#)
- [Visualizzazione di una panoramica dello stato di un cluster](#)
- [Acquisizione di uno snapshot di un cluster](#)
- [Creazione o modifica dell'allarme dello spazio su disco](#)
- [Utilizzo dei dati di prestazioni del cluster](#)

## Creazione di un cluster

Prima di creare un cluster, leggi [Panoramica di Amazon Redshift](#) e [Cluster e nodi in Amazon Redshift](#).

### Come creare un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).

2. Dal menu di navigazione, scegliere Clusters (Cluster). Sono elencati i cluster per il tuo account nella AWS regione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Per creare un cluster, scegli Create cluster (Crea cluster).
4. Segui le istruzioni sulla pagina della console per inserire le proprietà della Cluster configuration (Configurazione del cluster).

Il passaggio seguente descrive una console Amazon Redshift in esecuzione su e Regione AWS che supporta i tipi di nodi RA3. Per un elenco dei tipi di nodi Regioni AWS che supportano RA3, consulta [Panoramica dei tipi di nodi RA3](#) nella Amazon Redshift Management Guide.

Se non si conosce la dimensione del cluster, scegliere Aiutami a scegliere. In questo modo viene avviato un calcolatore di dimensionamento in cui vengono poste domande sulle dimensioni e le caratteristiche delle query dei dati che si prevede di archiviare nel data warehouse. Se si conosce la dimensione richiesta del cluster, ovvero il tipo di nodo e il numero di nodi, scegliere Sceglierò. Quindi scegliere il tipo di nodo e il numero di nodi per dimensionare il cluster per il proof of concept.

#### Note

Se la tua organizzazione è idonea e il tuo cluster viene creato in un Regione AWS paese in cui Amazon Redshift Serverless non è disponibile, potresti essere in grado di creare un cluster nell'ambito del programma di prova gratuita di Amazon Redshift. Scegli Produzione o Versione di prova gratuita per rispondere alla domanda Per cosa si intende utilizzare questo cluster? Se scegli Versione di prova gratuita, crei una configurazione con il tipo di nodo dc2.large. Per ulteriori informazioni sulla scelta di una versione prova gratuita, consulta [Prova gratuita di Amazon Redshift](#). Per un elenco delle aree Regioni AWS in cui è disponibile Amazon Redshift Serverless, consulta gli endpoint elencati per l'API [Redshift](#) Serverless nel. Riferimenti generali di Amazon Web Services

5. Nella sezione Configurazione del database specifica i valori per Nome dell'utente amministratore. In Password dell'amministratore scegli una delle opzioni seguenti:
  - Genera una password: utilizza una password generata da Amazon Redshift.
  - Aggiungi manualmente una password dell'amministratore: utilizza una tua password.
  - Gestisci le credenziali di amministratore in AWS Secrets Manager: Amazon Redshift le AWS Secrets Manager utilizza per generare e gestire la password di amministratore. L'utilizzo

- AWS Secrets Manager per generare e gestire la password segreta comporta un costo. Per informazioni sui prezzi di AWS Secrets Manager , consulta [Prezzi di AWS Secrets Manager](#).
- (Facoltativo) Segui le istruzioni sulla pagina della console per inserire le proprietà delle Cluster permissions (Autorizzazioni del cluster). Fornisci le autorizzazioni del cluster se il cluster deve accedere ad altri AWS servizi per te, ad esempio per caricare dati da Amazon S3.
  - Per creare il cluster, scegli Create cluster (Crea cluster). Potrebbero essere necessari diversi minuti prima che il cluster sia pronto per l'utilizzo.

## Configurazioni aggiuntive

Durante la creazione di un cluster, è possibile specificare proprietà aggiuntive per personalizzarlo. Puoi trovare ulteriori dettagli su alcune di queste proprietà nell'elenco seguente.

### Tipo di indirizzo IP

Scegli il tipo di indirizzo IP per il cluster. Puoi scegliere di far comunicare le risorse solo tramite il protocollo di indirizzamento IPv4 oppure la modalità dual-stack, che consente alle risorse di comunicare sia su IPv4 che su IPv6. Questa funzionalità è disponibile solo nelle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). Per ulteriori informazioni sulle AWS regioni, consulta [Regioni e zone di disponibilità](#).

### Virtual Private Cloud (VPC) (Cloud privato virtuale (VPC))

Scegli un VPC con un gruppo di sottoreti del cluster. Dopo la creazione del cluster, il gruppo di sottoreti del cluster non può essere più modificato.

### Gruppi di parametri

Selezionare un gruppo di parametri cluster da associare al cluster. Se non si effettua una selezione, il cluster utilizza il gruppo di parametri predefinito.

### Encryption (Crittografia)

Specificare se crittografare tutti i dati all'interno del cluster e dei relativi snapshot. Se si lascia l'impostazione predefinita, None (Nessuna), la crittografia non viene abilitata. Per abilitare la crittografia, specificare se utilizzare AWS Key Management Service (AWS KMS) o un modulo sicurezza hardware (HSM, Hardware Security Module), quindi configurare le relative impostazioni. Per informazioni sulla crittografia in Amazon Redshift, consultare [Crittografia dei database di Amazon Redshift](#).

- KMS

Scegli Usa AWS Key Management Service (AWS KMS) se desideri abilitare la crittografia e utilizzarla AWS KMS per gestire la tua chiave di crittografia. Inoltre, scegli il tasto da utilizzare. Puoi scegliere una chiave di default, una chiave dall'account corrente o una chiave da un altro account.

 Note

Se desideri utilizzare una chiave di un altro AWS account, inserisci l'Amazon Resource Name (ARN) per la chiave da utilizzare. È necessario disporre dell'autorizzazione per utilizzare la chiave. Per ulteriori informazioni sull'accesso alle chiavi di accesso AWS KMS, consulta [Controlling access to your keys](#) nella AWS Key Management Service Developer Guide.

Per ulteriori informazioni sull'uso delle chiavi di AWS KMS crittografia in Amazon Redshift, consulta. [Crittografia dei database per Amazon Redshift tramite AWS KMS](#)

- HSM (HSM)

Scegliere HSM per abilitare la crittografia e utilizzare un modulo di sicurezza hardware (HSM, Hardware Security Module) per gestire la chiave di crittografia.

Se si sceglie HSM (HSM), selezionare i valori da HSM Connection (Connessione HSM) e HSM Client Certificate (Certificato client HSM). Questi valori sono necessari per Amazon Redshift e il modulo HSM per formare una connessione affidabile su cui passare la chiave cluster. Prima di avviare un cluster, è necessario che la connessione HSM e il certificato client siano configurati in Amazon Redshift. Per ulteriori informazioni sulla configurazione di connessioni HSM e certificati client, vedi [Crittografia per Amazon Redshift tramite moduli di sicurezza hardware \(HSM\)](#).

### Maintenance Track (Traccia di manutenzione)

Puoi scegliere se la versione del cluster utilizzata corrisponde alla traccia Current (Attuale), Trailing (Finale) o a volte Preview (Anteprima).

### Monitoraggio

Puoi scegliere se creare CloudWatch allarmi.

## Configure cross-region snapshot (Configurazione di snapshot tra regioni diverse)

Puoi scegliere se abilitare la configurazione di snapshot tra regioni.

## Automated Snapshot Retention Period (Periodo automatizzato di conservazione degli snapshot)

Puoi scegliere il numero di giorni in cui mantenere questi snapshot entro i 35 giorni. Se il tipo di nodo è DC2, puoi scegliere zero (0) giorni per non creare istantanee automatiche.

## Manual snapshot retention period (Periodo di conservazione di uno snapshot manuale)

Puoi scegliere il numero di giorni oppure Indefinitely in cui mantenere questi snapshot.

## Creazione di un cluster di anteprima

È possibile creare un cluster Amazon Redshift di anteprima per testare nuove funzionalità di Amazon Redshift. Non è possibile utilizzare queste funzionalità in produzione o spostare il cluster di anteprima in un cluster di produzione o in un cluster su un'altra traccia. Per i termini e le condizioni dell'anteprima, consulta la sezione relativa a beta e anteprime nei [termini del servizio AWS](#).

### Come creare un cluster di anteprima

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo dei cluster con provisioning) e seleziona Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Nella pagina dell'elenco dei cluster viene visualizzato un banner che introduce l'anteprima. Scegli il pulsante Create preview cluster (Crea cluster di anteprima) per aprire la pagina di creazione del cluster.
4. Inserisci le proprietà del cluster. Scegli la traccia di anteprima che contiene le funzionalità che desideri testare. Consigliamo di assegnare al cluster un nome che indichi che si trova in una traccia di anteprima. Scegli le opzioni per il cluster, tra cui quelle contrassegnate come - anteprima, per le funzionalità che desideri testare. Per informazioni generali sulla creazione di cluster, consulta [Creazione di un cluster](#) nella Guida alla gestione di Amazon Redshift.
5. Per creare un cluster di anteprima, scegli Crea cluster.

**Note**

La traccia `preview_2023` è la traccia di anteprima più recente disponibile. Questa traccia supporta la creazione di cluster solo con tipi di nodo RA3. Il tipo di nodo DC2 e qualsiasi tipo di nodo precedente non sono supportati.

6. Quando il cluster di anteprima è disponibile, utilizza il client SQL per caricare dati ed eseguire query su di essi.

Per informazioni sull'anteprima nei gruppi di lavoro Redshift serverless, consulta [Creazione di un gruppo di lavoro di anteprima](#).

## Modifica di un cluster

Di seguito sono riportate le opzioni le cui impostazioni vengono applicate immediatamente quando si modifica un cluster:

- Gruppi di sicurezza VPC
- Accessibile pubblicamente
- Password dell'utente amministratore
- Connessione HSM
- HSM Client Certificate (Certificato client HSM)
- Maintenance detail (Dettagli manutenzione)
- Snapshot preferences (Preferenze di snapshot)

Di seguito sono riportate le opzioni le cui modifiche diventano effettive solo dopo il riavvio del cluster:

- Cluster identifier (Identificatore del cluster)

Amazon Redshift riavvia automaticamente il cluster quando si modifica Identificatore del cluster.

- Routing VPC avanzato

Amazon Redshift riavvia automaticamente il cluster quando si modifica Routing VPC avanzato.

- Cluster parameter group (Gruppo di parametri del cluster)
- Tipo di indirizzo IP

Questa funzionalità è disponibile solo nelle regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). Per ulteriori informazioni sulle AWS regioni, consulta [Regioni e zone di disponibilità](#).

Se si riduce il periodo automatizzato di conservazione dello snapshot, gli snapshot automatizzati esistenti le cui impostazioni non rientrano nel nuovo periodo di conservazione vengono eliminati. Per ulteriori informazioni, consulta [Snapshot e backup di Amazon Redshift](#).

Per ulteriori informazioni sulle proprietà dei cluster, consulta [Configurazioni aggiuntive](#).

Per modificare un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster che desideri modificare.
4. Scegli Modifica. Viene visualizzata la pagina Modifica cluster.
5. Aggiorna le proprietà del cluster. Alcune delle proprietà che è possibile modificare sono:
  - Cluster identifier (Identificatore del cluster)
  - Conservazione degli snapshot
  - Rilocazione del cluster

Per modificare le impostazioni di Rete e sicurezza, Manutenzione e Configurazioni del database, la console fornisce collegamenti alla scheda dei dettagli del cluster appropriata.

6. Seleziona Salvataggio delle modifiche.

## Eliminazione di un cluster

È possibile eliminare un cluster che non è più necessario. Se si intende eseguire il provisioning di un nuovo cluster con gli stessi dati e la stessa configurazione di quello che si sta eliminando, è necessario uno snapshot manuale. L'uso di uno snapshot manuale permette di ripristinare uno snapshot in seguito e riprendere l'uso del cluster. Se si elimina il cluster senza creare uno snapshot manuale finale, i dati del cluster sono eliminati. In entrambi i casi gli snapshot automatizzati vengono eliminati dopo che è stato eliminato il cluster, mentre quelli manuali vengono mantenuti fino a quando

non si eliminano. Per gli snapshot manuali, è possibile che vengano addebitati i costi di archiviazione di Amazon Simple Storage Service a seconda della quantità di archiviazione disponibile per gli snapshot Amazon Redshift per i relativi cluster. Per ulteriori informazioni, consulta [Chiusura ed eliminazione di cluster](#).

L'eliminazione di un cluster elimina anche tutti i segreti associati. AWS Secrets Manager

Per eliminare un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster da eliminare.
4. In Actions (Azioni), scegliere Delete (Elimina). Appare la pagina Create cluster (Crea cluster).
5. Scegli Delete cluster (Elimina cluster).

#### Note

Quando elimini un cluster e scegli di creare uno snapshot finale, Amazon Redshift interromperà la richiesta di eliminazione se è in corso un'operazione di ripristino sul cluster. In tal caso, puoi eliminare il cluster senza uno snapshot finale oppure puoi eliminarlo con uno snapshot finale al termine del ripristino.

## Riavvio di un cluster

Quando si riavvia un cluster, il relativo stato è impostato su `rebooting` e viene creato un evento cluster una volta completato il riavvio. Eventuali modifiche cluster in sospeso vengono applicate al riavvio.

Per riavviare un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster da riavviare.

4. In Actions (Operazioni), scegliere Reboot cluster (Riavvia cluster). Appare la pagina Reboot cluster (Riavvia cluster).
5. Scegli Reboot cluster (Riavvia cluster).

## Ridimensionamento di un cluster

Quando si modificano le dimensioni di un cluster, si specifica un numero di nodi o un tipo di nodo diverso dalla configurazione corrente del cluster. Durante il processo di ridimensionamento del cluster, è possibile solo leggere le query, non è possibile eseguire query di scrittura o lettura/scrittura sul cluster.

Per ulteriori informazioni sul ridimensionamento dei cluster, inclusa la descrizione di approcci diversi del processo di ridimensionamento, vedi [Ridimensionamento di cluster](#).

Per ridimensionare un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster da ridimensionare.
4. In Actions (Operazioni), scegli Resize (Ridimensiona). Appare la pagina Resize cluster (Ridimensiona cluster).
5. Segui le istruzioni visualizzate nella pagina. È possibile ridimensionare il cluster ora, una volta in un momento specifico oppure aumentare e diminuire le dimensioni del cluster in base a una pianificazione.
6. A seconda delle scelte effettuate, scegliere Resize now (Ridimensiona ora) o Schedule resize (Pianifica ridimensionamento).

Se disponi di nodi riservati, puoi eseguire l'aggiornamento a nodi riservati RA3. Puoi farlo quando usi la console per eseguire il ripristino da una snapshot o esegui un ridimensionamento elastico. La console può guidarti attraverso questo processo. Per ulteriori informazioni sulla creazione di nodi RA3, consulta [Aggiornamento ai tipi di nodo RA3](#).

## Per aggiornare una versione di rilascio del cluster

È possibile aggiornare la versione di manutenzione di rilascio di un cluster che ha un valore per Release Status (Stato di rilascio) di New release available (Nuovo rilascio disponibile). Quando si aggiorna la versione di manutenzione è possibile scegliere se aggiornare immediatamente o aggiornare nella finestra di manutenzione successiva.

### Important

Se si aggiorna immediatamente, il cluster è offline finché non viene completato l'aggiornamento.

Per aggiornare una versione di rilascio del cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster da aggiornare.
4. Alla voce Actions (Operazioni), scegli Upgrade cluster version (Aggiorna versione del cluster). Appare la pagina Upgrade cluster version (Aggiorna versione del cluster).
5. Segui le istruzioni visualizzate nella pagina.
6. Scegli Upgrade cluster version (Aggiorna versione del cluster).

## Recupero di informazioni sulla configurazione del cluster

Per visualizzare le informazioni su un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Cluster performance (Prestazioni del cluster), Query monitoring (Monitoraggio della query), Databases (Database), Datashares (Unità di condivisione dati), Schedules (Pianificazioni), Maintenance (Manutenzione) e Properties (Proprietà).
3. Scegli le diverse schede per visualizzare ulteriori dettagli.

## Visualizzazione di una panoramica dello stato di un cluster

Per visualizzare lo stato di un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. La colonna Status (Stato) mostra lo stato del cluster.

## Acquisizione di uno snapshot di un cluster

Per creare uno snapshot di un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster).
3. Scegli il cluster per il quale creare lo snapshot.
4. In Actions (Operazioni), scegli Create snapshot (Crea snapshot). Viene visualizzata la pagina Create snapshot (Crea snapshot).
5. Segui le istruzioni visualizzate nella pagina.
6. Scegli Create snapshot (Crea snapshot).

## Creazione o modifica dell'allarme dello spazio su disco

Per creare un allarme sull'utilizzo dello spazio su disco di un cluster.

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Alarms (Allarmi).
3. Alla voce Actions (Operazioni), scegli Create alarm (Crea allarme). Viene visualizzata la pagina Create Alarm (Crea allarme).
4. Segui le istruzioni visualizzate nella pagina.
5. Seleziona Create Alarm (Crea allarme).

## Utilizzo dei dati di prestazioni del cluster

Nella console, è possibile operare sulle prestazioni del cluster nella scheda Cluster performance (Prestazioni del cluster) della pagina dei dettagli del cluster.

## Gestione dei cluster utilizzando l'API AWS CLI Amazon Redshift

Puoi utilizzare le seguenti AWS CLI operazioni per gestire i cluster in Amazon Redshift.

- [cancel-resize](#)
- [create-cluster](#)
- [delete-cluster](#)
- [describe-clusters](#)
- [describe-cluster-versions](#)
- [describe-node-configuration-options](#)
- [describe-orderable-cluster-options](#)
- [describe-resize](#)
- [modify-cluster](#)
- [pause-cluster](#)
- [reboot-cluster](#)
- [resize-cluster](#)
- [resume-cluster](#)

Per gestire i cluster è possibile usare le operazioni API Amazon Redshift riportate di seguito.

- [CancelResize](#)
- [CreateCluster](#)
- [DeleteCluster](#)
- [DescribeClusters](#)
- [DescribeClusterVersions](#)
- [DescribeNodeConfigurationOptions](#)
- [DescribeResize](#)

- [DescribeOrderableClusterOptions](#)
- [ModifyCluster](#)
- [PauseCluster](#)
- [RebootCluster](#)
- [ResizeCluster](#)
- [ResumeCluster](#)

## Gestione dei cluster in un VPC

### Argomenti

- [Panoramica](#)
- [Creazione di un cluster in un VPC](#)
- [Gestione dei gruppi di sicurezza VPC per un cluster](#)
- [Configurazione delle impostazioni di comunicazione dei gruppi di sicurezza per i cluster Amazon Redshift o per un gruppo di lavoro di Amazon Redshift serverless](#)
- [Come funziona Amazon Redshift con la condivisione di risorse tramite VPC AWS](#)
- [Gruppi di sottoreti dei cluster Amazon Redshift](#)

## Panoramica

Amazon Redshift supporta entrambe le piattaforme EC2-VPC ed EC2-Classical per avviare un cluster in un Virtual Private Cloud (VPC) basato sul servizio Amazon VPC. Per ulteriori informazioni, consultare [Utilizzo di EC2-VPC durante la creazione del cluster](#).

### Note

Amazon Redshift non supporta l'avvio dei cluster in VPC con tenancy dedicata. Per ulteriori informazioni, consultare [Istanze dedicate](#) nella Guida per l'utente di Amazon VPC.

Quando si effettua il provisioning di un cluster nel VPC, è necessario completare le operazioni seguenti:

- Fornisci le informazioni sul VPC.

Quando si richiede ad Amazon Redshift di creare un cluster nel VPC, è necessario fornire le informazioni sul VPC creando prima di tutto un gruppo di sottoreti del cluster. Tale informazione include l'ID del VPC e una lista di sottoreti nel tuo VPC. Quando viene avviato un cluster, viene fornito il gruppo di sottoreti del cluster, in modo che Amazon Redshift possa effettuare il provisioning del cluster in una delle sottoreti nel VPC. Per ulteriori informazioni sulla creazione di gruppi di sottoreti in Amazon Redshift, consultare [Gruppi di sottoreti dei cluster Amazon Redshift](#). Per ulteriori informazioni sulla configurazione del VPC, consulta [Nozioni di base di Amazon VPC](#) nella Guida alle operazioni di base di Amazon VPC.

- Facoltativamente, configura le opzioni accessibili pubblicamente.

Se configuri il cluster in modo che sia accessibile pubblicamente, Amazon Redshift utilizza un indirizzo IP elastico per l'indirizzo IP esterno. Un indirizzo IP elastico è un indirizzo IP statico. Esso permette di modificare la configurazione sottostante senza influire sull'indirizzo IP che i client usano per la connessione al cluster. Questo approccio può essere utile in casi come il ripristino dopo un errore. La creazione di un indirizzo IP elastico dipende dall'impostazione di trasferimento della zona di disponibilità. Sono disponibili due opzioni:

1. Se hai attivato il trasferimento della zona di disponibilità e desideri abilitare l'accesso pubblico, non devi specificare un indirizzo IP elastico. Viene assegnato un indirizzo IP elastico gestito da Amazon Redshift. È associato al tuo AWS account.
2. Se il trasferimento della zona di disponibilità è disattivato e desideri abilitare l'accesso pubblico, puoi scegliere di creare un indirizzo IP elastico per il VPC in Amazon EC2 prima di avviare il cluster Amazon Redshift. Se non crei un indirizzo IP, Amazon Redshift fornisce un indirizzo IP elastico configurato da utilizzare per il VPC. Questo indirizzo IP elastico è gestito da Amazon Redshift e non è associato al tuo AWS account.

Per ulteriori informazioni, consulta [Indirizzi IP elastici](#) nella Guida per l'utente di Amazon EC2.

In alcuni casi, potresti avere un cluster accessibile pubblicamente in un VPC e desiderarti connetterti a esso usando l'indirizzo IP privato dall'interno del VPC. In questo caso imposta i seguenti parametri VPC sul valore `true`:

- `DNS resolution`
- `DNS hostnames`

Supponi di avere un cluster accessibile pubblicamente in un VPC ma di non impostare tali parametri a `true` nel VPC. In questi casi, le connessioni effettuate dall'interno del VPC vengono risolte all'indirizzo IP elastico del cluster anziché all'indirizzo IP privato. È consigliabile impostare

questi parametri su `true` e usare l'indirizzo IP privato per un cluster accessibile pubblicamente quando la connessione avviene dall'interno del VPC. Per ulteriori informazioni, consultare [Utilizzo del DNS con VPC](#) nella Guida per l'utente di Amazon VPC.

#### Note

Se hai un cluster esistente accessibile pubblicamente in un VPC, le connessioni stabilite dall'interno del VPC continuano a usare l'indirizzo IP elastico per connettersi al cluster fino a quando non ridimensioni il cluster stesso. Ciò accade anche con il set di parametri precedente. I nuovi cluster seguono il nuovo comportamento che prevede l'utilizzo dell'indirizzo IP privato per la connessione al cluster accessibile pubblicamente dall'interno dello stesso VPC.

L'indirizzo IP elastico è un indirizzo IP esterno per l'accesso del cluster dall'esterno del VPC. Non è correlato agli indirizzi IP pubblici e privati dei nodi del cluster che sono visualizzati nella console Amazon Redshift in Dettagli di connessione. Gli indirizzi IP privati e pubblici dei nodi del cluster vengono visualizzati indipendentemente dal fatto che il cluster sia o meno accessibile pubblicamente. Sono usati solo in specifiche circostanze per configurare le regole di accesso sull'host remoto. Queste circostanze si verificano quando si caricano i dati da un'istanza Amazon EC2 o da un altro host remoto che utilizza una connessione Secure Shell (SSH). Per ulteriori informazioni, consultare [Fase 1: recupero della chiave pubblica del cluster e degli indirizzi IP dei nodi del cluster](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

È possibile associare un cluster a un indirizzo IP elastico al momento della creazione del cluster o del suo ripristino da uno snapshot. In alcuni casi, è possibile che si desideri associare il cluster a un indirizzo IP elastico o modificare un indirizzo IP elastico associato al cluster. Per collegare un indirizzo IP elastico dopo la creazione del cluster, aggiornare innanzitutto il cluster in modo che non sia accessibile pubblicamente, quindi renderlo accessibile pubblicamente e aggiungere un indirizzo IP elastico nella stessa operazione.

- Associa un gruppo di sicurezza VPC.

Quindi è necessario concedere l'accesso in ingresso usando un gruppo di sicurezza VPC. Questo gruppo di sicurezza VPC deve permettere l'accesso tramite la porta del database per il cluster, in modo che sia possibile stabilire la connessione usando gli strumenti client SQL. Puoi configurare questo comportamento in anticipo oppure aggiungere regole dopo l'avvio del cluster. Per ulteriori informazioni, consulta [Configurazione delle impostazioni di comunicazione dei gruppi di sicurezza](#)

[per i cluster Amazon Redshift](#), che fornisce indicazioni sulla configurazione delle regole in entrata e in uscita tra un client e un cluster con provisioning o un gruppo di lavoro Amazon Redshift serverless. Un'altra risorsa che ti aiuta a comprendere i gruppi di sicurezza è [Sicurezza nel VPC](#) nella Guida per l'utente di Amazon VPC. Non puoi usare i gruppi di sicurezza del cluster Amazon Redshift per concedere l'accesso in ingresso al cluster.

Per ulteriori informazioni sull'uso dei cluster in un VPC, consultare [Creazione di un cluster in un VPC](#).

## Ripristino di uno snapshot di un cluster nel VPC

Uno snapshot di un cluster nel VPC può essere ripristinato solo in un VPC e non all'esterno del VPC. Puoi eseguire il ripristino nello stesso VPC o in un altro VPC nel tuo account. Per ulteriori informazioni sugli snapshot, consulta [Snapshot e backup di Amazon Redshift](#).

## Creazione di un cluster in un VPC

Di seguito sono illustrate le fasi generali per la distribuzione di un cluster nel cloud privato virtuale (VPC, Virtual Private Cloud).

Per creare un cluster in un VPC

### 1. Configurare un VPC.

È possibile creare il cluster nel VPC predefinito per l'account, se presente, oppure in un VPC creato. Per ulteriori informazioni, consulta [Utilizzo di EC2-VPC durante la creazione del cluster](#). Per creare un VPC, consulta [Creazione di un VPC](#) nella Guida per l'utente di Amazon VPC. Prendere nota di identificatore, sottorete e zona di disponibilità della sottorete del VPC. Queste informazioni saranno necessarie per avviare il cluster.

#### Note

Deve essere presente almeno una sottorete definita nel VPC per poterla aggiungere al gruppo di sottoreti del cluster nella fase seguente. Per maggiori informazioni sull'aggiunta di una sottorete al VPC, consultare [Aggiunta di una sottorete al VPC](#) nella Guida per l'utente di Amazon VPC.

### 2. Creare un gruppo di sottoreti del cluster Amazon Redshift per specificare quale sottorete il cluster Amazon Redshift può usare nel VPC.

È possibile creare un gruppo di sottoreti del cluster usando la console Amazon Redshift o a livello di programmazione. Per ulteriori informazioni, consultare [Gruppi di sottoreti dei cluster Amazon Redshift](#).

3. Autorizzare l'accesso delle connessioni in ingresso in un gruppo di sicurezza VPC che verrà associato al cluster.

È possibile abilitare un client esterno al VPC (attestato sulla Internet pubblica) affinché possa collegarsi al cluster. Per farlo, è necessario associare il cluster a un gruppo di sicurezza VPC che permetta l'accesso in ingresso sulla porta usata all'avvio del cluster. Per esempi di regole dei gruppi di sicurezza, consultare [Regole dei gruppi di sicurezza](#) nella Guida per l'utente di Amazon VPC.

4. Segui i passaggi relativi ai [cluster forniti da Amazon Redshift nella Amazon Redshift Getting Started Guide](#) per creare un cluster. Durante la creazione del cluster, apportare le seguenti modifiche:
  - Per visualizzare la sezione Additional configurations (Configurazioni aggiuntive), disattiva la voce Use defaults (Utilizza le impostazioni predefinite).
  - Nella sezione Network and security (Rete e sicurezza), specificare il virtual private cloud (VPC), il gruppo di sottoreti del cluster e il gruppo di sicurezza del VPC configurati.

A questo punto, puoi iniziare a usare il cluster. Segui le fasi nella Guida alle operazioni di base per testare il cluster caricando dati di esempio e provando a eseguire query di esempio.

## Gestione dei gruppi di sicurezza VPC per un cluster

Quando si effettua il provisioning di un cluster Amazon Redshift, questo è bloccato per impostazione predefinita perché nessuno possa accedervi. Per concedere ad altri utenti l'accesso in ingresso a un cluster ad Amazon Redshift, è necessario associare il cluster a un gruppo di sicurezza. Se si utilizza la piattaforma EC2-VPC, è possibile usare un gruppo di sicurezza Amazon VPC esistente o definirne uno nuovo. Quindi puoi associarlo a un cluster come descritto qui di seguito. Se si utilizza la piattaforma EC2-Classic, è necessario definire un gruppo di sicurezza del cluster e associarlo a un cluster. Per ulteriori informazioni sull'uso dei gruppi di sicurezza del cluster nella piattaforma EC2-Classic, consultare [Gruppi di sicurezza dei cluster Amazon Redshift](#).

Un gruppo di sicurezza VPC è costituito da un set di regole che controllano l'accesso a un'istanza nel VPC, ad esempio un cluster. Le singole regole definiscono l'accesso in base a intervalli di indirizzi IP

oppure ad altri gruppi di sicurezza VPC. Quando associ un gruppo di sicurezza VPC a un cluster, le regole definite nel gruppo di sicurezza VPC controllano l'accesso al cluster.

A ogni cluster di cui si effettua il provisioning nella piattaforma EC2-Classical sono associati uno o più gruppi di sicurezza di Amazon VPC. Amazon VPC fornisce un gruppo di sicurezza VPC di default, creato automaticamente al momento della creazione del VPC. Ogni cluster avviato nel VPC viene associato automaticamente al gruppo di sicurezza VPC predefinito se non ne indichi uno diverso al momento della creazione del cluster. Puoi associare un gruppo di sicurezza VPC a un cluster al momento della creazione del cluster oppure successivamente, modificando il cluster.

La tabella seguente descrive le regole predefinite per il gruppo di sicurezza VPC predefinito.

Inbound			
Source	Protocol	Port Range	Comments
The security group ID (sg-xxxxxxx)	All	All	Allow inbound traffic from instances assigned to the same security group
Outbound			
Destination	Protocol	Port Range	Comments
0.0.0.0/0	All	All	Allow all outbound traffic

È possibile modificare le regole per il gruppo di sicurezza VPC predefinito per il cluster Amazon Redshift in base alle esigenze.

Se il gruppo di sicurezza VPC predefinito è sufficiente, non è necessario crearne altri. Tuttavia, puoi facoltativamente creare gruppi di sicurezza VPC aggiuntivi per gestire meglio l'accesso in ingresso al cluster. Ad esempio, si supponga di eseguire un servizio in un cluster Amazon Redshift e di fornire diversi livelli di servizio ai clienti. Se non desideri fornire lo stesso accesso a tutti i livelli di servizio, potresti creare gruppi di sicurezza VPC separati, uno per ogni livello di servizio. Puoi quindi associare questi gruppi di sicurezza VPC al cluster.

Puoi creare fino a 100 gruppi di sicurezza VPC per un VPC e associare un gruppo di sicurezza VPC a molti cluster. Tuttavia, puoi associare fino a un massimo di cinque gruppi di sicurezza VPC a uno specifico cluster.

Amazon Redshift applica immediatamente le modifiche a un gruppo di sicurezza del VPC. Di conseguenza, se hai associato il gruppo di sicurezza VPC a un cluster, le regole di accesso in ingresso del cluster nel gruppo di sicurezza VPC aggiornato vengono applicate immediatamente.

È possibile creare e modificare i gruppi di sicurezza VPC all'indirizzo <https://console.aws.amazon.com/vpc/>. Puoi anche gestire i gruppi di sicurezza VPC in modo programmatico utilizzando la CLI di AWS CLI Amazon EC2 e la AWS Tools for Windows PowerShell. Per ulteriori informazioni sull'uso dei gruppi di sicurezza del VPC, consultare [Gruppi di sicurezza per il VPC](#) nella Guida per l'utente di Amazon VPC.

## Configurazione delle impostazioni di comunicazione dei gruppi di sicurezza per i cluster Amazon Redshift o per un gruppo di lavoro di Amazon Redshift serverless

Questo argomento consente di configurare i gruppi di sicurezza per indirizzare e ricevere il traffico di rete in modo appropriato. I seguenti sono alcuni casi d'uso comuni:

- Attivi l'accessibilità pubblica per un cluster Amazon Redshift o per un gruppo di lavoro di Amazon Redshift serverless, ma non riceve traffico. È necessario configurare una regola in entrata per consentire al traffico di raggiungerlo da Internet.
- Il cluster non è accessibile al pubblico e utilizzi il gruppo di sicurezza del VPC predefinito preconfigurato per consentire il traffico in entrata. Tuttavia, è necessario utilizzare un gruppo di sicurezza diverso da quello predefinito e questo gruppo di sicurezza personalizzato non consente il traffico in entrata. È necessario configurarlo per consentire la comunicazione.

Le sezioni seguenti aiutano a scegliere la risposta corretta per ogni caso d'uso e mostrano come configurare il traffico di rete in base alle tue esigenze. Facoltativamente, puoi utilizzare i passaggi per configurare la comunicazione da altri gruppi di sicurezza privati.

### Note

Nella maggior parte dei casi, le impostazioni del traffico di rete non vengono configurate automaticamente in Amazon Redshift. Questo perché possono variare a livello granulare, a seconda che l'origine del traffico sia Internet o un gruppo di sicurezza privato e perché i requisiti di sicurezza variano.

## Accessibilità pubblica con configurazione predefinita o personalizzata del gruppo di sicurezza

Se stai creando o hai già un cluster, esegui la seguente procedura di configurazione per rendere il cluster accessibile pubblicamente. Ciò si applica sia quando si sceglie il gruppo di sicurezza predefinito sia un gruppo di sicurezza personalizzato:

1. Trovare le impostazioni di rete:

- Per un cluster Amazon Redshift con provisioning, scegli la scheda Proprietà, quindi in Impostazioni di rete e sicurezza, seleziona il VPC per il cluster.
  - Per un gruppo di lavoro Amazon Redshift serverless, scegli Configurazione del gruppo di lavoro. Scegli il gruppo di lavoro dall'elenco. Quindi in Accesso ai dati, nel pannello Rete e sicurezza scegli Modifica.
2. Configura il gateway Internet e la tabella di routing per il tuo VPC. Avvia la configurazione scegliendo il VPC in base al nome. Apre il pannello di controllo del VPC. Per connettersi a un cluster o a un gruppo di lavoro accessibile da Internet, è necessario collegare un gateway Internet alla tabella di routing. Puoi effettuare la configurazione scegliendo Tabelle di routing nel pannello di controllo del VPC. Verifica che la destinazione del gateway Internet sia impostata con l'origine 0.0.0.0/0 o un CIDR IP pubblico. La tabella di routing deve essere associata alla sottorete VPC in cui si trova il cluster. Per ulteriori informazioni sulla configurazione dell'accesso a Internet per un VPC, come descritto qui, consulta [Abilitazione dell'accesso a Internet](#) nella documentazione di Amazon VPC. Per ulteriori informazioni sulle tabelle di routing, consulta [Configurare le tabelle di routing](#).
  3. Dopo aver configurato il gateway Internet e la tabella di routing, torna alle impostazioni di rete per Redshift. Apri l'accesso in entrata scegliendo il gruppo di sicurezza e quindi scegliendo le Regole in entrata. Scegliere Edit inbound rules (Modifica regole in entrata).
  4. Scegli Protocollo e Porta per la regola in entrata, in base alle tue esigenze, per consentire il traffico dai client. Per un cluster RA3, seleziona una porta compresa negli intervalli 5431-5455 o 8191-8215. Al termine, salva ciascuna regola.
  5. Modifica l'impostazione Accessibile al pubblico per abilitarlo. Puoi effettuare questa operazione dal menu Operazioni del cluster o del gruppo di lavoro.

Quando attivi l'impostazione accessibile al pubblico, Redshift crea un indirizzo IP elastico. È un indirizzo IP statico associato al tuo account. AWS I client esterni al VPC possono utilizzarlo per connettersi.

Per ulteriori informazioni sulle configurazioni per i gruppi di sicurezza, consultare [Gruppi di sicurezza dei cluster Amazon Redshift](#).

Puoi testare le regole connettendoti a un client. Esegui le seguenti operazioni se ti connetti ad Amazon Redshift serverless. Dopo aver completato la configurazione di rete, connettiti al tuo strumento client, ad esempio [Amazon Redshift RSQL](#). Utilizzando il tuo dominio Amazon Redshift Serverless come host, inserisci quanto segue:

```
rsql -h workgroup-name.account-id.region.amazonaws.com -U admin -d dev -p 5439
```

## Accessibilità privata con configurazione predefinita o personalizzata del gruppo di sicurezza

Quando non comunichi tramite Internet con il cluster o gruppo di lavoro, si fa riferimento all'accesso privato. Se hai scelto il gruppo di sicurezza predefinito al momento della creazione, il gruppo di sicurezza include le seguenti regole di comunicazione predefinite:

- Una regola in entrata che consente il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza.
- Una regola in uscita che consente tutto il traffico in uscita. La destinazione di questa regola è 0.0.0.0/0. Nella notazione routing interdominio senza classi (CIDR), rappresenta tutti gli indirizzi IP possibili.

Puoi visualizzare le regole nella console selezionando il gruppo di sicurezza per il cluster o il gruppo di lavoro.

Se il cluster o il gruppo di lavoro e il client utilizzano entrambi il gruppo di sicurezza predefinito, non è necessaria alcuna configurazione aggiuntiva per consentire il traffico di rete. Tuttavia, se elimini o modifichi delle regole nel gruppo di sicurezza predefinito per Redshift o per il client, ciò non si applica più. In questo caso, è devi configurare le regole per consentire le comunicazioni in entrata e in uscita. Una configurazione comune dei gruppi di sicurezza è la seguente:

- Per un'istanza client di Amazon EC2:
  - Una regola in entrata che consente l'indirizzo IP del client.
  - Una regola in uscita che consente l'intervallo di indirizzi IP (blocco CIDR) di tutte le sottoreti fornite per l'utilizzo di Redshift. Oppure puoi specificare 0.0.0.0/0, che rappresenta tutti gli intervalli di indirizzi IP.
- Per il cluster o gruppo di lavoro Redshift:
  - Una regola in entrata che consente gruppo di sicurezza client.
  - Una regola in uscita che consente il traffico verso 0.0.0.0/0. In genere, la regola in uscita consente tutto il traffico in uscita. Facoltativamente, puoi aggiungere una regola in uscita per consentire il traffico verso il gruppo di sicurezza del client. In questo caso facoltativo, non è sempre necessaria una regola in uscita, poiché il traffico di risposta per ogni richiesta può

raggiungere l'istanza. Per ulteriori dettagli sul comportamento di richiesta e risposta, consulta [Gruppi di sicurezza](#) nella Guida per l'utente di Amazon VPC.

Se modifichi la configurazione per qualsiasi sottorete o gruppo di sicurezza specificati per l'utilizzo di Redshift, potrebbe essere necessario modificare le regole del traffico di conseguenza per mantenere aperta la comunicazione. Per ulteriori informazioni sulla creazione di regole in entrata e in uscita, consulta [Blocchi CIDR del VPC](#) nella Guida per l'utente di Amazon VPC. Per informazioni sulla connessione ad Amazon Redshift da un client, consulta [Configurazione delle connessioni in Amazon Redshift](#).

## Come funziona Amazon Redshift con la condivisione di risorse tramite VPC AWS

La condivisione VPC consente di creare risorse AWS applicative, come istanze Amazon EC2 e AWS altri servizi, in un cloud privato virtuale (VPC) condiviso e gestito centralmente. L'account proprietario del VPC (proprietario) condivide una o più sottoreti con altri account (partecipanti) che appartengono alla stessa organizzazione. AWS Ciò descrive come creare e utilizzare un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless in un VPC condiviso.

I vantaggi della condivisione VPC includono il fatto che non è necessario gestire numerosi VPC e ciò può aiutare a semplificare la rete. Il vantaggio, in particolare per gli amministratori e gli utenti di Amazon Redshift, è che le risorse Redshift possono operare in modo produttivo nel VPC condiviso. Per ulteriori informazioni sulla condivisione VPC, consulta la pagina [Condividere il VPC con altri account](#), che ne approfondisce i vantaggi e il funzionamento.

### Come utilizzare le risorse dei data warehouse di Amazon Redshift in un VPC condiviso

Innanzitutto, è importante capire che un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless non può essere reso visibile ai partecipanti in una sottorete condivisa. Ma ciò non impedisce ai partecipanti di lavorare con il database del proprietario in un VPC condiviso. Ciò è illustrato nei dettagli in modo più completo nelle fasi che seguono.

Prima di creare un cluster Amazon Redshift con provisioning in un VPC condiviso, devi creare un gruppo di sottoreti che intendi utilizzare per Amazon Redshift. Questo gruppo deve includere le sottoreti del VPC condiviso che desideri utilizzare. Quando crei il cluster Amazon Redshift, devi scegliere questa sottorete e specificare anche il gruppo di sicurezza del VPC condiviso. Allo stesso modo, devi specificare le sottoreti condivise e il gruppo di sicurezza che hai creato nel VPC condiviso

quando crei il gruppo di lavoro e il database Amazon Redshift serverless. Dopo aver configurato le sottoreti, esegui questa procedura per configurare le risorse Redshift nell'ambiente condiviso:

1. Il proprietario del VPC crea un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless, utilizzando una sottorete nel VPC condiviso.
2. Il proprietario del VPC rende disponibile il cluster o il gruppo di lavoro in uno scenario tra VPC. Le fasi sono descritte in [Utilizzo degli endpoint VPC gestiti da RedShift in Amazon Redshift](#) per un cluster con provisioning o in [Connessione ad Amazon Redshift serverless da un endpoint VPC gestito da Amazon Redshift](#) per Amazon Redshift serverless. Abilitando la disponibilità tra VPC, possono rendere il database disponibile agli utenti nello stesso AWS account o in altri account.
3. Al contrario, tramite la condivisione VPC, un proprietario può condividere una sottorete con un partecipante e il partecipante può creare un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless nella sottorete. In questo caso, tuttavia, il proprietario non può visualizzare una risorsa Amazon Redshift creata da un partecipante. Il cluster o il gruppo di lavoro deve essere reso accessibile abilitando la disponibilità tra VPC nello stesso modo descritto nella fase precedente.

## Note sull'utilizzo delle risorse Amazon Redshift in un VPC condiviso

Tieni presente i seguenti comportamenti relativi all'uso di Amazon Redshift in una sottorete condivisa:

- Come descritto nella sezione precedente, il proprietario del VPC non può condividere un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless con un partecipante tramite la condivisione VPC. Tuttavia, il partecipante può creare un cluster o un gruppo di lavoro Amazon Redshift serverless nella sottorete del proprietario. In questo caso, Amazon Redshift non è visibile al proprietario tramite la condivisione VPC.
- Il proprietario del VPC non può visualizzare, aggiornare o eliminare un cluster con provisioning di Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless creato dal partecipante nella sottorete condivisa.
- Non sono disponibili autorizzazioni per consentire a un altro AWS account di accedere alle risorse Amazon Redshift che crei nel VPC condiviso.

# Gruppi di sottoreti dei cluster Amazon Redshift

## Panoramica

Crei un gruppo di sottoreti del cluster se effettui il provisioning del cluster nel cloud privato virtuale (VPC, Virtual Private Cloud). Per ulteriori informazioni su VPC, consultare la pagina sui dettagli del prodotto di [Amazon VPC](#).

Il VPC può avere una o più sottoreti, un subset di indirizzi IP nel VPC, che permettono di raggruppare le risorse in base alle esigenze di sicurezza e operative. Un gruppo di sottoreti del cluster permette di specificare un set di sottoreti nel VPC. Quando si effettua il provisioning di un cluster, viene fornito il gruppo di sottoreti e Amazon Redshift crea il cluster in una delle sottoreti nel gruppo.

Per ulteriori informazioni sulla creazione di un VPC, consultare la [Guida per l'utente di Amazon VPC](#).

Dopo aver creato un gruppo di sottoreti, è possibile rimuovere le sottoreti aggiunte in precedenza o aggiungerne di altre. Amazon Redshift fornisce operazioni API per creare, modificare o eliminare un gruppo di sottoreti di un cluster. Puoi eseguire le stesse operazioni anche nella console.

## Gestione di gruppi di sottoreti del cluster mediante la console

È possibile gestire i gruppi di sottoreti del cluster mediante la console Amazon Redshift. È possibile creare, eliminare o gestire un gruppo di sottoreti del cluster. Tutte queste attività iniziano dall'elenco dei gruppi di sottoreti del cluster. Per gestire un gruppo di sottoreti del cluster, è necessario selezionarlo.

Puoi eseguire il provisioning di un cluster su una delle sottoreti fornite al gruppo di sottoreti. Un gruppo di sottoreti del cluster permette di specificare un set di sottoreti nel VPC.

### Creazione di un gruppo di sottoreti del cluster

Per eseguire il provisioning di un cluster in un VPC, è necessario che sia definito almeno un gruppo di sottoreti del cluster.

### Per creare un gruppo di sottoreti del cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Configurations (Configurazioni), quindi scegliere Subnet groups (Gruppi di sottoreti). Viene visualizzato l'elenco dei gruppi di sottoreti.

3. Scegli **Create cluster subnet group** (Crea gruppo di sottoreti del cluster) per visualizzare la pagina di creazione.
4. Inserisci le informazioni sul gruppo di sottoreti, incluse le sottoreti da aggiungere.
5. Scegli **Create cluster subnet group** (Crea gruppo di sottoreti del cluster) per creare il gruppo con le sottoreti prescelte.

## Modifica di un gruppo di sottoreti di cluster

Per modificare un gruppo di sottoreti del cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere **Configurations** (Configurazioni), quindi scegliere **Subnet groups** (Gruppi di sottoreti). Viene visualizzato l'elenco dei gruppi di sottoreti.
3. Scegli il gruppo di sottoreti da modificare.
4. Alla voce **Actions** (Operazioni), scegli **Modify** (Modifica) per visualizzare i dettagli del gruppo di sottoreti.
5. Aggiorna le informazione del gruppo di sottoreti.
6. Scegli **Save** (Salva) per modificare il gruppo.

In alcuni casi, per la modifica o la rimozione delle sottoreti sono necessarie fasi aggiuntive. Ad esempio, questo articolo del AWS Knowledge Center, [Come posso spostare il mio cluster Amazon Redshift fornito in una sottorete diversa?](#), descrive un caso d'uso che riguarda lo spostamento di un cluster.

## Eliminazione di un gruppo di sottoreti del cluster

Non è possibile eliminare un gruppo di sottoreti utilizzato da un cluster.

Per eliminare un gruppo di sottoreti del cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere **Configurations** (Configurazioni), quindi scegliere **Subnet groups** (Gruppi di sottoreti). Viene visualizzato l'elenco dei gruppi di sottoreti.
3. Scegli il gruppo di sottoreti da eliminare, scegli quindi **Delete** (Elimina).

## Gestisci i gruppi di sottoreti del cluster utilizzando AWS CLI l'API Amazon Redshift

Per gestire i gruppi di sottoreti del cluster, è possibile usare le seguenti operazioni della CLI di Amazon Redshift.

- [create-cluster-subnet-group](#)
- [delete-cluster-subnet-group](#)
- [describe-cluster-subnet-groups](#)
- [modify-cluster-subnet-group](#)

Per gestire i gruppi di sottoreti del cluster, è possibile usare le seguenti operazioni API di Amazon Redshift.

- [CreateClusterSubnetGroup](#)
- [DeleteClusterSubnetGroup](#)
- [DescribeClusterSubnetGroups](#)
- [ModifyClusterSubnetGroup](#)

## Cronologia delle versioni del cluster

Amazon Redshift rilascia periodicamente nuove versioni del cluster utilizzate per aggiornare il cluster.

### Important

Per le informazioni sulle versioni dei cluster di Amazon Redshift disponibili e sulle relative caratteristiche, miglioramenti e correzioni, consulta [Versioni dei cluster per Amazon Redshift](#).

# Utilizzo delle integrazioni Zero-ETL

Questa è una documentazione di pre-rilascio per le integrazioni Zero-ETL di Aurora PostgreSQL e RDS per MySQL con Amazon Redshift, che è in versione di anteprima. La documentazione e le funzionalità sono soggette a modifiche. Ti consigliamo di utilizzare le integrazioni Zero-ETL di RDS per MySQL e Aurora PostgreSQL solo in ambienti di test e non in ambienti di produzione. Per i termini e condizioni dell'anteprima, consulta la sezione su beta e anteprime nei [AWS termini del servizio](#).

L'integrazione Zero-ETL è una soluzione completamente gestita che rende disponibili i dati transazionali o operativi in Amazon Redshift pressoché in tempo reale. Con questa soluzione, puoi configurare l'integrazione della tua origine con un data warehouse Amazon Redshift. Non c'è bisogno di gestire una pipeline di estrazione, trasformazione e caricamento (ETL). Le operazioni ETL vengono gestite automaticamente automatizzando la creazione e la gestione della replica dei dati dall'origine dati al cluster Amazon Redshift o allo spazio dei nomi Redshift serverless. Puoi continuare ad aggiornare e a eseguire query sui dati di origine e contemporaneamente utilizzare Amazon Redshift per carichi di lavoro analitici come report e pannelli di controllo.

Con l'integrazione zero-ETL hai a disposizione dati più aggiornati per analisi, AI/ML e reportistica. Ottieni informazioni più accurate e tempestive per casi d'uso come dashboard in tempo reale, esperienza di gioco ottimizzata, monitoraggio della qualità dei dati e analisi del comportamento dei clienti. Puoi fare previsioni basate sui dati con maggiore sicurezza, migliorare le esperienze dei clienti e promuovere approfondimenti basati sui dati in tutta l'azienda.

Per le integrazioni Zero-ETL sono attualmente supportate le seguenti origini:

- Aurora edizione compatibile con MySQL
- Aurora edizione compatibile con PostgreSQL (anteprima)
- RDS per MySQL (anteprima)

Per creare un'integrazione Zero-ETL, devi specificare l'origine di integrazione e un data warehouse Amazon Redshift come destinazione. L'integrazione replica i dati dall'origine nel data warehouse di destinazione. I dati diventano disponibili in Amazon Redshift in pochi secondi. L'integrazione monitora lo stato della pipeline dei dati ed esegue il ripristino in caso di problemi quando possibile. Puoi creare

integrazioni da origini dello stesso tipo in un unico data warehouse Amazon Redshift per ottenere approfondimenti olistici da più applicazioni.

Con i dati in Amazon Redshift, puoi utilizzare le analisi fornite da Amazon Redshift. Ad esempio, il machine learning (ML) integrato, le viste materializzate, la condivisione dei dati e l'accesso diretto a più datastore e data lake. L'integrazione Zero-ETL mantiene le risorse di calcolo isolate dalle risorse di dati, quindi gli strumenti per elaborare i dati sono più efficienti. Per i data engineer, le integrazioni Zero-ETL forniscono l'accesso a dati sensibili al fattore tempo che altrimenti potrebbe essere ritardato da errori intermittenti in pipeline di dati complesse. Puoi eseguire query analitiche e modelli di ML sui dati transazionali per ottenere informazioni pressoché in tempo reale per eventi e decisioni aziendali sensibili al fattore tempo.

Puoi creare un abbonamento per le notifiche di eventi Amazon Redshift per ricevere una notifica quando si verifica un evento per un'integrazione Zero-ETL. Per l'elenco delle notifiche di eventi relativi all'integrazione, consulta [Notifiche di eventi di integrazione zero-ETL con Amazon EventBridge](#).

Il modo più semplice per creare una sottoscrizione è utilizzare la console Amazon SNS. Per informazioni sulla creazione di un argomento Amazon SNS e sul relativo abbonamento, consulta [Nozioni di base su Amazon SNS](#) nella Guida per sviluppatori di Amazon Simple Notification Service.

Per iniziare a utilizzare le integrazioni Zero-ETL, tieni presente i seguenti concetti:

- Un database di origine è quello i cui dati vengono replicati in Amazon Redshift.
- Un data warehouse di destinazione è il cluster con provisioning Amazon Redshift o il gruppo di lavoro Redshift serverless in cui vengono replicati i dati.
- Un database di destinazione è quello che crei da un'integrazione Zero-ETL nel data warehouse di destinazione.

Puoi monitorare le integrazioni Zero-ETL eseguendo query sulle seguenti viste di sistema in Amazon Redshift.

- [SVV\\_INTEGRATION](#) fornisce informazioni sui dettagli di configurazione delle integrazioni Zero-ETL.
- [SYS\\_INTEGRATION\\_ACTIVITY](#) fornisce informazioni sulle integrazioni Zero-ETL completate.
- [SVV\\_INTEGRATION\\_TABLE\\_STATE](#) fornisce informazioni sullo stato dell'integrazione.
- [SYS\\_INTEGRATION\\_TABLE\\_STATE\\_CHANGE](#) fornisce informazioni sul registro delle modifiche dello stato della tabella per le integrazioni.

Per informazioni sui prezzi delle integrazioni Zero-ETL, consulta la pagina dei prezzi appropriata:

- [Prezzi di Amazon Redshift](#)
- [Prezzi di Amazon Aurora](#)
- [Prezzi di Amazon SQS](#)

Per ulteriori informazioni sulle origini dell'integrazione Zero-ETL, consulta i seguenti argomenti:

- Per le integrazioni Zero-ETL di Aurora, consulta [Vantaggi](#), [Concetti chiave](#), [Limitazioni](#), [Quote](#) e [Regioni supportate](#) nella Guida per l'utente di Amazon Aurora.
- Per le integrazioni Zero-ETL di RDS, consulta [Vantaggi](#), [Concetti chiave](#), [Limitazioni](#), [Quote](#) e [Regioni supportate](#) nella Guida per l'utente di Amazon RDS.

### Argomenti

- [Considerazioni sull'utilizzo delle integrazioni Zero-ETL con Amazon Redshift](#)
- [Guida introduttiva alle integrazioni Zero-ETL](#)
- [Creazione di database di destinazione in Amazon Redshift](#)
- [Esecuzione di query e creazione di viste materializzate con i dati replicati](#)
- [Gestione delle integrazioni Zero-ETL](#)
- [Metriche per le integrazioni Zero-ETL](#)
- [Risoluzione dei problemi delle integrazioni Zero-ETL](#)

## Considerazioni sull'utilizzo delle integrazioni Zero-ETL con Amazon Redshift

Le seguenti considerazioni si applicano alle integrazioni Zero-ETL con Amazon Redshift.

- Il data warehouse Amazon Redshift di destinazione deve soddisfare i seguenti prerequisiti:
  - Deve eseguire un tipo di nodo RA3 (ra3.16xlarge, ra3.4xlarge e ra3.xlplus) o Amazon Redshift serverless.
  - Deve essere crittografato (se si utilizza un cluster con provisioning).
  - È abilitata la distinzione tra maiuscole e minuscole.
- Non puoi abilitare il supporto VPC avanzato nei data warehouse con integrazioni configurate.

- Se elimini un'origine di integrazione autorizzata per un data warehouse Amazon Redshift, tutte le integrazioni associate avranno lo stato FAILED.
- Il database di destinazione è di sola lettura. Non puoi creare tabelle, viste o viste materializzate nel database di destinazione. Tuttavia, puoi utilizzare le viste materializzate su altre tabelle nel data warehouse di destinazione.
- Le viste materializzate sono supportate se utilizzate nelle query tra database. L'aggiornamento delle viste materializzate con i dati replicati dalle integrazioni Zero-ETL comporta l'aggiornamento completo della vista. L'aggiornamento incrementale, la riscrittura automatica delle query, l'aggiornamento automatico e le viste materializzate automatizzate non sono supportati. Per informazioni sulla creazione delle viste materializzate con i dati replicati dalle integrazioni Zero-ETL, consulta [Creazione di viste materializzate con i dati replicati](#).
- Puoi eseguire query solo sulle tabelle con stato Synced presenti nel data warehouse di destinazione. Per ulteriori informazioni, consulta [Metriche per le integrazioni Zero-ETL](#).
- Amazon Redshift accetta solo caratteri UTF-8, quindi potrebbe non rispettare le regole di confronto definite nell'origine. Le regole di ordinamento e confronto potrebbero essere diverse, il che può in ultima analisi modificare i risultati delle query.
- La lunghezza massima di un tipo di dati Amazon Redshift VARCHAR è di 65.535 byte. Quando il contenuto della fonte non rientra in questo limite, la replica non procede e la tabella viene messa in uno stato di errore. Per ulteriori informazioni sulle differenze tra i tipi di dati tra le fonti di integrazione zero-ETL e i database Amazon Redshift, consulta [Differenze tra i tipi di dati tra Aurora e Amazon Redshift nella Guida per l'utente di Amazon Aurora](#).
- Le tabelle nella fonte di integrazione devono avere una chiave primaria. Altrimenti, le tabelle non possono essere replicate nel data warehouse di destinazione in Amazon Redshift.
- Per le integrazioni Zero-ETL di Aurora PostgreSQL e RDS per MySQL con Amazon Redshift, crea il data warehouse di destinazione in Anteprema. Per ulteriori informazioni, consulta [Creazione e configurazione di un data warehouse Amazon Redshift di destinazione](#).
- L'integrazione zero-ETL non supporta le trasformazioni durante la replica dei dati dagli archivi di dati transazionali ad Amazon Redshift. I dati vengono replicati così come sono dal database di origine. Tuttavia, puoi applicare trasformazioni ai dati replicati in Amazon Redshift.
- Questo può avere un impatto su altri carichi di lavoro in esecuzione in Amazon Redshift. Per eliminare l'impatto dell'integrazione zero-ETL su altri carichi di lavoro, prendi in considerazione l'utilizzo di un endpoint separato per l'integrazione zero-ETL e condividi i dati con altri endpoint che devono accedere a questi dati utilizzando la condivisione dei dati.

- L'integrazione zero-ETL viene eseguita in Amazon Redshift utilizzando connessioni parallele. Viene eseguita utilizzando le credenziali dell'utente che ha creato il database dall'integrazione. Quando la query viene eseguita, il ridimensionamento della concorrenza non si attiva per queste connessioni durante la sincronizzazione (scrittura). Le letture di scalabilità simultanea (dai client Amazon Redshift) funzionano per oggetti sincronizzati.

Per le considerazioni che si applicano anche all'origine di integrazione, consulta uno degli argomenti seguenti:

- Per le origini Aurora, consulta [Limitazioni](#) nella Guida per l'utente di Amazon Aurora.
- Per le origini Amazon RDS, consulta [Limitazioni](#) nella Guida per l'utente di Amazon RDS.

## Guida introduttiva alle integrazioni Zero-ETL

Prima di configurare l'integrazione Zero-ETL in Amazon Redshift, configura l'origine di integrazione e configurala con i parametri e le autorizzazioni richiesti. Quindi, passa al resto della configurazione iniziale dalla console Amazon Redshift e. AWS CLI

Per creare un'integrazione Zero-ETL di Aurora con Amazon Redshift

Puoi creare un'integrazione Zero-ETL di Aurora con Amazon Redshift, procedi come indicato di seguito:

1. Dalla console Amazon RDS, [crea un gruppo di parametri del cluster di database personalizzato](#) come descritto nella Guida per l'utente di Amazon Aurora.
2. Dalla console Amazon RDS, [crea un cluster di database Amazon Aurora di origine](#) come descritto nella Guida per l'utente di Amazon Aurora.
3. Dalla console Amazon Redshift: [Creazione e configurazione di un data warehouse Amazon Redshift di destinazione](#).
  - Dalla nostra AWS CLI console Amazon Redshift: [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#)
  - Dalla console Amazon Redshift: [Configurazione dell'autorizzazione per il data warehouse Amazon Redshift](#).
4. Dalla console Amazon RDS, [crea un'integrazione Zero-ETL](#) come descritto nella Guida per l'utente di Amazon Aurora.

5. Dalla console Amazon Redshift o dall'editor di query v2, [crea un database Amazon Redshift dall'integrazione](#).

Quindi, [esegui le query e crea le viste materializzate con i dati replicati](#).

Per creare un'integrazione Zero-ETL con Amazon Redshift

Per creare un'integrazione Zero-ETL RDS con Amazon Redshift, procedi come segue:

1. Dalla console Amazon RDS, [crea un gruppo di parametri di database personalizzato](#) come descritto nella Guida per l'utente di Amazon RDS.
2. Dalla console Amazon RDS, [crea un'istanza Amazon RDS di origine](#) come descritto nella Guida per l'utente di Amazon RDS.
3. Dalla console Amazon Redshift: [Creazione e configurazione di un data warehouse Amazon Redshift di destinazione](#).
  - Dalla nostra AWS CLI console Amazon Redshift: [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#)
  - Dalla console Amazon Redshift: [Configurazione dell'autorizzazione per il data warehouse Amazon Redshift](#).
4. Dalla console Amazon RDS, [crea un'integrazione Zero-ETL](#) come descritto nella Guida per l'utente di Amazon RDS.
5. Dalla console Amazon Redshift o dall'editor di query v2, [crea un database Amazon Redshift dall'integrazione](#).

Quindi, [esegui le query e crea le viste materializzate con i dati replicati](#).

La console Amazon RDS offre un flusso di creazione step-by-step dell'integrazione, in cui specifichi il database di origine e il data warehouse Amazon Redshift di destinazione. Se si verificano problemi, puoi scegliere che Amazon RDS risolva i problemi automaticamente anziché correggerli manualmente sulla console Amazon RDS o Amazon Redshift.

## Creazione e configurazione di un data warehouse Amazon Redshift di destinazione

Prima di questo passaggio, crea l'origine di integrazione e configura i parametri richiesti dal tipo di origine per le integrazioni Zero-ETL.

In questo passaggio crei e configuri un data warehouse Amazon Redshift di destinazione, ad esempio un gruppo di lavoro Redshift serverless o un cluster con provisioning.

Il data warehouse di destinazione deve avere le seguenti caratteristiche:

- Eseguire Amazon Redshift Serverless o un cluster con provisioning con tipo di istanza ra3.16xlarge, ra3.4xlarge o ra3.xplus.
- La distinzione tra maiuscole e minuscole (`enable_case_sensitive_identifier`) è attivata. Per ulteriori informazioni, consulta [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#).
- Essere crittografato se il data warehouse di destinazione è un cluster con provisioning Amazon Redshift. Per ulteriori informazioni, consulta [Crittografia dei database di Amazon Redshift](#).
- Creato nella stessa AWS regione della fonte di integrazione.

#### Note

Per le integrazioni Zero-ETL Aurora PostgreSQL e RDS per MySQL con Amazon Redshift, tieni presenti anche i seguenti requisiti per il data warehouse di destinazione:

- Devi creare il data warehouse in Anteprima nella traccia `preview_2023`. Non puoi utilizzare le funzionalità di anteprima in produzione o spostare il data warehouse di anteprima in un'implementazione di produzione.
- Se scegli di creare un cluster con provisioning Amazon Redshift, il cluster deve avere almeno due nodi.
- Per le sorgenti Aurora PostgreSQL, è necessario creare il data warehouse di destinazione nella regione Stati Uniti orientali (Ohio). AWS Tieni presente che devi creare il database di origine per le integrazioni Zero-ETL Aurora PostgreSQL utilizzando l'[ambiente di anteprima del database Amazon RDS](#).

Per le sorgenti RDS for MySQL, è necessario creare il data warehouse di destinazione in una regione supportata. AWS Per un elenco delle regioni AWS in cui sono disponibili le integrazioni Zero-ETL RDS per MySQL, consulta la sezione [Supported Regions for zero-ETL integrations with Amazon Redshift](#) nella Guida per l'utente di Amazon RDS.

Per creare il data warehouse di destinazione in Anteprima per le integrazioni Zero-ETL Aurora PostgreSQL e RDS per MySQL, consulta uno degli argomenti seguenti a seconda del tipo di implementazione:

- Per creare un'anteprima del cluster con provisioning Amazon Redshift, consulta [Creazione di un cluster di anteprima](#). Assicurati di scegliere la traccia `preview_2023` per utilizzare le integrazioni Zero-ETL.
- Per creare un'anteprima del gruppo di lavoro Amazon Redshift serverless, consulta [Creazione di un gruppo di lavoro di anteprima](#).

Per creare il data warehouse di destinazione per le integrazioni Zero-ETL Aurora MySQL, consulta uno degli argomenti seguenti a seconda del tipo di implementazione:

- Per creare un cluster con provisioning Amazon Redshift, consulta [Creazione di un cluster](#).
- Per creare un gruppo di lavoro Amazon Redshift serverless con uno spazio dei nomi, consulta [Creazione di un gruppo di lavoro con uno spazio dei nomi](#).

Quando crei un cluster con provisioning, Amazon Redshift crea anche un gruppo di parametri predefinito. Non è consentito modificare il gruppo di parametri predefinito. Tuttavia, è possibile creare un gruppo di parametri personalizzato prima di creare un nuovo cluster e associarlo al cluster. In alternativa, è possibile modificare il gruppo di parametri che verrà associato al cluster creato. È inoltre necessario attivare la distinzione tra maiuscole e minuscole per il gruppo di parametri quando crei il gruppo di parametri personalizzato o quando ne modifichi uno corrente per utilizzare le integrazioni Zero-ETL.

Puoi creare un gruppo di parametri personalizzato utilizzando la console Amazon Redshift o AWS CLI come segue:

- Mediante la console Amazon Redshift: [Gestione di gruppi di parametri mediante la console](#)
- Utilizzando il AWS CLI — [Gestione dei gruppi di parametri utilizzando AWS CLI l'API Amazon Redshift](#)

## Attivazione della distinzione tra maiuscole e minuscole per il data warehouse

Puoi collegare un gruppo di parametri e abilitare la distinzione tra maiuscole e minuscole per un cluster con provisioning durante la creazione. Tuttavia, è possibile aggiornare un gruppo di lavoro serverless tramite la AWS Command Line Interface (AWS CLI) solo dopo averlo creato. Questa operazione è necessaria per supportare la distinzione tra maiuscole e minuscole di MySQL e PostgreSQL. `enable_case_sensitive_identifier` è un valore di configurazione che determina se gli identificatori dei nomi di database, tabelle e colonne fanno distinzione tra maiuscole e minuscole. Questo parametro deve essere attivato per creare integrazioni Zero-ETL nel data warehouse. Per ulteriori informazioni, consulta [enable\\_case\\_sensitive\\_identifier](#).

Per Amazon Redshift Serverless: [Attiva la distinzione tra maiuscole e minuscole per Amazon Redshift Serverless utilizzando AWS CLI](#). Tieni presente che puoi attivare la distinzione tra maiuscole e minuscole per Amazon Redshift Serverless solo dalla AWS CLI.

Per i cluster con provisioning Amazon Redshift, abilita la distinzione tra maiuscole e minuscole per il cluster di destinazione facendo riferimento a uno dei seguenti argomenti:

- [Attivazione della distinzione tra maiuscole e minuscole per i cluster con provisioning di Amazon Redshift mediante la console Amazon Redshift](#)
- [Attiva la distinzione tra maiuscole e minuscole per i cluster con provisioning di Amazon Redshift utilizzando AWS CLI](#)

### Attiva la distinzione tra maiuscole e minuscole per Amazon Redshift Serverless utilizzando AWS CLI

Esegui il AWS CLI comando seguente per attivare la distinzione tra maiuscole e minuscole per il tuo gruppo di lavoro.

```
aws redshift-serverless update-workgroup \  
    --workgroup-name target-workgroup \  
    --config-parameters  
parameterKey=enable_case_sensitive_identifier,parameterValue=true
```

Attendi che lo stato del gruppo di lavoro sia `Active` prima di continuare con la fase successiva.

## Attivazione della distinzione tra maiuscole e minuscole per i cluster con provisioning di Amazon Redshift mediante la console Amazon Redshift

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel riquadro di navigazione a sinistra scegli Pannello di controllo dei cluster con provisioning.
3. Scegli il cluster con provisioning in cui desideri replicare i dati.
4. Nel riquadro di navigazione a sinistra scegli Configurazioni > Gestione del carico di lavoro.
5. Nella pagina Gestione del carico di lavoro seleziona il gruppo di parametri.
6. Scegli la scheda Parametri.
7. Scegli Modifica parametri, quindi modifica `enable_case_sensitive_identifier` su `true`.
8. Quindi, scegliere Save (Salva).

## Attiva la distinzione tra maiuscole e minuscole per i cluster con provisioning di Amazon Redshift utilizzando AWS CLI

1. Poiché non puoi modificare il gruppo di parametri predefinito, dal tuo programma di terminale esegui il seguente AWS CLI comando per creare un gruppo di parametri personalizzato. quindi associarlo al cluster con provisioning.

```
aws redshift create-cluster-parameter-group \  
  --parameter-group-name zero-etl-params \  
  --parameter-group-family redshift-1.0 \  
  --description "Param group for zero-ETL integrations"
```

2. Esegui il AWS CLI comando seguente per attivare la distinzione tra maiuscole e minuscole per il gruppo di parametri.

```
aws redshift modify-cluster-parameter-group \  
  --parameter-group-name zero-etl-params \  
  --parameters ParameterName=enable_case_sensitive_identifier,ParameterValue=true
```

3. Esegui il seguente comando per associare il gruppo di parametri al cluster.

```
aws redshift modify-cluster \  
  --cluster-identifier target-cluster \  
  --cluster-parameter-group-name zero-etl-params
```

4. Attendi che il cluster con provisioning sia disponibile. Puoi anche controllare lo stato del cluster utilizzando il comando `describe-cluster`. Esegui quindi il seguente comando per riavviare il cluster.

```
aws redshift reboot-cluster \  
  --cluster-identifier target-cluster
```

## Configurazione dell'autorizzazione per il data warehouse Amazon Redshift

Per replicare i dati dall'origine di integrazione nel data warehouse Amazon Redshift, devi inizialmente aggiungere le due entità seguenti:

- Principale autorizzato: identifica l'utente o il ruolo che può creare integrazioni Zero-ETL nel data warehouse.
- Origine di integrazione autorizzata: identifica il database di origine che può aggiornare il data warehouse.

Puoi configurare i principali autorizzati e le origini dell'integrazione autorizzate dalla scheda Policy delle risorse sulla console Amazon Redshift o utilizzando l'operazione API `PutResourcePolicy` Amazon Redshift.

### Aggiunta di principali autorizzati

Per creare un'integrazione zero-ETL nel gruppo di lavoro Redshift Serverless o nel cluster con provisioning, autorizza l'accesso allo spazio dei nomi o al cluster con provisioning associato.

Puoi ignorare questa fase se si verificano entrambe le seguenti condizioni:

- Il Account AWS proprietario del gruppo di lavoro Redshift Serverless o del cluster provisionato possiede anche il database di origine.
- Questo principale è associato a una policy IAM basata sull'identità con autorizzazioni per creare integrazioni Zero-ETL in questo spazio dei nomi Redshift Serverless o nel cluster con provisioning.

### Aggiunta di principali autorizzati a uno spazio dei nomi Amazon Redshift Serverless

1. Nella console Amazon Redshift, scegli Redshift serverless dal riquadro di navigazione a sinistra.

2. Seleziona Configurazione dello spazio dei nomi, quindi scegli lo spazio dei nomi e vai alla scheda Policy delle risorse.
3. Scegli Aggiungi principali autorizzati.
4. Per ogni principale autorizzato che desideri aggiungere, inserisci nel namespace l'ARN AWS dell'utente o del ruolo o l'ID di chi desideri concedere l'accesso per creare Account AWS integrazioni zero-ETL. L'ID dell'account viene archiviato come ARN.
5. Seleziona Salvataggio delle modifiche.

### Aggiunta di principali autorizzati a un cluster con provisioning di Amazon Redshift

1. Nel riquadro di navigazione a sinistra della console Amazon Redshift scegli Pannello di controllo dei cluster con provisioning.
2. Seleziona Cluster, quindi scegli il cluster e vai alla scheda Policy delle risorse.
3. Scegli Aggiungi principali autorizzati.
4. Per ogni principale autorizzato che desideri aggiungere, inserisci nel cluster l'ARN dell' AWS utente o del ruolo o l'ID di chi desideri concedere l' Account AWS accesso per creare integrazioni zero-ETL. L'ID dell'account viene archiviato come ARN.
5. Seleziona Salvataggio delle modifiche.

### Aggiunta di origini di integrazione autorizzate

Per consentire all'origine di aggiornare il data warehouse Amazon Redshift, devi aggiungerla come origine di integrazione autorizzata allo spazio dei nomi.

### Aggiunta di un'origine di integrazione autorizzata a uno spazio dei nomi Amazon Redshift Serverless

1. Nella console Amazon Redshift, vai a Pannello di controllo serverless.
2. Scegli il nome dello spazio dei nomi.
3. Vai alla scheda Policy delle risorse.
4. Scegli Aggiungi un'origine di integrazione autorizzata.
5. Specifica l'ARN dell'origine per l'integrazione Zero-ETL.

**Note**

La rimozione di un'origine di integrazione autorizzata blocca la replica dei dati nello spazio dei nomi. L'azione disattiva tutte le integrazioni Zero-ETL dall'origine nello spazio dei nomi.

Aggiunta di un'origine di integrazione autorizzata a un cluster con provisioning di Amazon Redshift

1. Nella console Amazon Redshift, vai a Pannello di controllo dei cluster con provisioning.
2. Scegli il nome del cluster con provisioning.
3. Vai alla scheda Policy delle risorse.
4. Scegli Aggiungi un'origine di integrazione autorizzata.
5. Specifica l'ARN dell'origine dati per l'integrazione Zero-ETL.

**Note**

La rimozione di un'origine di integrazione autorizzata blocca la replica dei dati nel cluster con provisioning. L'azione disattiva tutte le integrazioni Zero-ETL dall'origine nel cluster con provisioning Amazon Redshift.

## Configurazione dell'autorizzazione usando l'API Amazon Redshift

Puoi utilizzare le operazioni API Amazon Redshift per configurare le policy delle risorse che funzionano con le integrazioni Zero-ETL.

Per controllare l'origine che può creare un'integrazione in entrata nello spazio dei nomi, crea una policy delle risorse e collegala allo spazio dei nomi. Con la policy delle risorse, puoi specificare l'origine che ha accesso all'integrazione. La policy delle risorse è collegata allo spazio dei nomi del data warehouse di destinazione per consentire all'origine di creare un'integrazione in entrata per replicare i dati in tempo reale dall'origine in Amazon Redshift.

Di seguito è riportata una policy delle risorse di esempio.

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

```

```

{
  "Effect": "Allow",
  "Principal": {
    "Service": "redshift.amazonaws.com"
  },
  "Action": "redshift:AuthorizeInboundIntegration",
  "Condition": {
    "StringEquals": {
      "aws:SourceArn": "source_arn"
    }
  }
},
{
  "Effect": "Allow",
  "Principal": {
    "AWS": "source_principal"
  },
  "Action": "redshift:CreateInboundIntegration"
}
]
}

```

Di seguito sono riepilogate le operazioni API Amazon Redshift applicabili alla configurazione delle policy delle risorse per le integrazioni:

- Utilizza l'operazione [PutResourcePolicy API per rendere](#) persistente la politica delle risorse. Quando si fornisce un'altra policy delle risorse, quella precedente viene sostituita. Utilizza la policy delle risorse di esempio precedente, che assegna le autorizzazioni per le seguenti azioni:
  - `CreateInboundIntegration`: consente al principale di origine di creare un'integrazione in entrata per la replica dei dati dall'origine al data warehouse di destinazione.
  - `AuthorizeInboundIntegration`: consente ad Amazon Redshift di verificare continuamente che il data warehouse di destinazione possa ricevere dati replicati dall'ARN di origine.
- Utilizzare l'operazione [GetResourcePolicy](#) API per visualizzare le politiche delle risorse esistenti.
- Utilizza l'operazione [DeleteResourcePolicy](#) API per rimuovere una politica delle risorse dalla risorsa.

Per aggiornare una policy delle risorse, puoi anche utilizzare il comando della AWS CLI [put-resource-policy](#).

## Passaggi successivi

Ora che hai configurato l'autorizzazione per il data warehouse Amazon Redshift di destinazione, puoi creare un'integrazione zero-ETL e iniziare la replica dei dati.

A seconda dell'origine, esegui una delle seguenti operazioni:

- Per creare le integrazioni Zero-ETL Aurora, consulta [Creazione di integrazioni Zero-ETL di Aurora con Amazon Redshift](#) nella Guida per l'utente di Amazon Aurora.
- Per creare integrazioni Zero-ETL di RDS, consulta [Creating Amazon RDS zero-ETL integrations with Amazon Redshift](#) nella Guida per l'utente di Amazon RDS.

## Creazione di database di destinazione in Amazon Redshift

Per replicare i dati dall'origine in Amazon Redshift, devi creare un database dall'integrazione in Amazon Redshift.

Connettiti al gruppo di lavoro Redshift serverless o al cluster con provisioning di destinazione e crea un database con un riferimento all'identificatore di integrazione. Questo identificatore è il valore restituito per `integration_id` quando si esegue una query sulla vista [SVV\\_INTEGRATION](#).

### Important

Prima di creare un database dall'integrazione, devi creare un'integrazione Zero-ETL con stato Active sulla console Amazon RDS o Amazon Redshift.

## Creazione di un database di destinazione in Amazon Redshift

Prima di iniziare a replicare i dati dall'origine in Amazon Redshift, crea un database dall'integrazione in Amazon Redshift. Puoi creare il database utilizzando la console Amazon Redshift o l'editor di query v2.

### Creazione di un database di destinazione mediante la console Amazon Redshift

1. Nel pannello di navigazione a sinistra, scegli Interfacce di rete.
2. Dall'elenco delle integrazioni, scegli un'integrazione.

3. Se utilizzi un cluster con provisioning, devi prima connetterti al database. Scegliere Connect to database (Connetti al database). Puoi connetterti utilizzando una connessione recente o creando una nuova connessione.
4. Per creare un database dall'integrazione, scegli Crea database dall'integrazione.
5. Inserire un Nome database. L'ID di integrazione e il nome del data warehouse sono precompilati.

Per le origini Aurora PostgreSQL, inserisci anche il database che hai specificato durante la creazione dell'integrazione Zero-ETL.

6. Scegliere Crea database.

## Creazione di un database di destinazione mediante l'editor di query v2

1. Accedi alla console Amazon Redshift e scegli Editor di query v2.
2. Nel pannello a sinistra, scegli il gruppo di lavoro Amazon Redshift serverless o il cluster con provisioning Amazon Redshift, quindi esegui la connessione.
3. Per ottenere l'ID di integrazione, accedi all'elenco delle integrazioni sulla console Amazon Redshift.

In alternativa, esegui il seguente comando per ottenere il valore `integration_id`:

```
SELECT integration_id FROM SVV_INTEGRATION;
```

4. Quindi, per creare il database, esegui il seguente comando. Specificando l'ID di integrazione, crei una connessione tra il database e l'origine.

Sostituisci `integration_id` con il valore restituito dal comando precedente.

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id';
```

Per le origini Aurora PostgreSQL, devi includere anche un riferimento al database denominato all'interno del cluster specificato al momento della creazione dell'integrazione. Per esempio:

```
CREATE DATABASE destination_db_name FROM INTEGRATION 'integration_id'  
DATABASE named_db;
```

**Note**

Solo l'origine di integrazione può aggiornare i dati nel database creato dall'integrazione. Per modificare lo schema di una tabella, esegui i comandi DDL o DML sulle tabelle dell'origine. Puoi eseguire i comandi DDL e DML sulle tabelle nell'origine, ma puoi eseguire solo comandi DDL e query di sola lettura sul database di destinazione.

Per informazioni sulla visualizzazione dello stato di un database di destinazione, consulta [Gestione delle integrazioni Zero-ETL](#).

## Aggiunta dei dati all'origine

Dopo aver creato un database di destinazione, puoi aggiungere i dati all'origine. Per aggiungere i dati all'origine, consulta uno degli argomenti seguenti:

- Per le origini Aurora, consulta [Aggiungere dati al cluster DB](#) nella Guida per l'utente di Amazon Aurora.
- Per le origini Amazon RDS, consulta [Add data to the source DB instance](#) nella Guida per l'utente di Amazon RDS.

## Esecuzione di query e creazione di viste materializzate con i dati replicati

### Esecuzione di query sui dati replicati in Amazon Redshift

Dopo aver aggiunto i dati all'origine, questi vengono replicati pressoché in tempo reale nel data warehouse Amazon Redshift e sono pronti per l'esecuzione di query. Per informazioni sulle metriche di integrazione e sulle statistiche delle tabelle, consulta [Metriche per le integrazioni Zero-ETL](#).

**Note**

Poiché un database è identico a uno schema in MySQL, il livello di database MySQL è mappato al livello dello schema di Amazon Redshift. Tieni presente questa differenza di mappatura quando esegui le query sui dati replicati da Aurora MySQL o RDS per MySQL.

## Per eseguire query sui dati replicati

1. Accedi alla console Amazon Redshift e scegli Editor di query v2.
2. Connettiti al gruppo di lavoro Amazon Redshift serverless o al cluster con provisioning di Amazon Redshift e scegli il database dall'elenco a discesa.
3. Utilizza un'istruzione SELECT per selezionare tutti i dati replicati dallo schema e dalla tabella che hai creato nell'origine. Per distinguere tra maiuscole e minuscole, usa le virgolette doppie (" ") per i nomi di schemi, tabelle e colonne. Per esempio:

```
SELECT * FROM "schema_name". "table_name";
```

Puoi anche eseguire query sui dati utilizzando la CLI di Amazon Redshift.

## Creazione di viste materializzate con i dati replicati

Puoi creare viste materializzate nel database Amazon Redshift locale per trasformare i dati replicati tramite le integrazioni Zero-ETL. Connettiti al database locale e utilizza le query tra database per accedere ai database di destinazione. Puoi utilizzare nomi di oggetti completi con la notazione in tre parti (destination-database-name.schema-name.table-name) oppure creare uno schema esterno che faccia riferimento alla coppia database-schema di destinazione e utilizzare la notazione in due parti (external-schema-name.table-name). Per ulteriori informazioni sulle query tra database, consulta [Esecuzione di query sui dati tra database](#).

Utilizza l'esempio seguente per creare e inserire dati di esempio nelle tabelle *sales\_zetl* e *event\_zetl* dall'origine *ticket\_zetl*. Le tabelle vengono replicate nel database Amazon Redshift *zetl\_int\_db*.

```
CREATE TABLE sales_zetl (  
    salesid integer NOT NULL primary key,  
    eventid integer NOT NULL,  
    pricepaid decimal(8, 2)  
);  
  
CREATE TABLE event_zetl (  
    eventid integer NOT NULL PRIMARY KEY,  
    eventname varchar(200)  
);  
  
INSERT INTO sales_zetl VALUES(1, 1, 3.33);
```

```
INSERT INTO sales_zet1 VALUES(2, 2, 4.44);
INSERT INTO sales_zet1 VALUES(3, 2, 5.55);

INSERT INTO event_zet1 VALUES(1, "Event 1");
INSERT INTO event_zet1 VALUES(2, "Event 2");
```

Puoi creare una vista materializzata per ottenere le vendite totali per ogni evento utilizzando la notazione in tre parti:

```
--three part notation zet1-database-name.schema-name.table-name
CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_3p as
(SELECT eventname, sum(pricepaid) as total_price
FROM zet1_int_db.tickit_zet1.sales_zet1 S, zet1_int_db.tickit_zet1.event_zet1 E
WHERE S.eventid = E.eventid
GROUP BY 1);
```

Puoi creare una vista materializzata per ottenere le vendite totali per ogni evento utilizzando la notazione in due parti:

```
--two part notation external-schema-name.table-name notation
CREATE EXTERNAL schema ext_tickit_zet1
FROM REDSHIFT
DATABASE zet1_int_db
SCHEMA tickit_zet1;

CREATE MATERIALIZED VIEW mv_transformed_sales_per_event_2p
AS
(
  SELECT eventname, sum(pricepaid) as total_price
  FROM ext_tickit_zet1.sales_zet1 S, ext_tickit_zet1.event_zet1 E
  WHERE S.eventid = E.eventid
  GROUP BY 1
);
```

Per visualizzare le viste materializzate create usa l'esempio seguente.

```
SELECT * FROM mv_transformed_sales_per_event_3p;

+-----+-----+
| eventname | total_price |
+-----+-----+
| Event 1   | 3.33       |
```

```

| Event 2 | 9.99 |
+-----+-----+

SELECT * FROM mv_transformed_sales_per_event_2p;

+-----+-----+
| eventname | total_price |
+-----+-----+
| Event 1 | 3.33 |
| Event 2 | 9.99 |
+-----+-----+

```

## Gestione delle integrazioni Zero-ETL

Puoi visualizzare i dettagli di un'integrazione Zero-ETL per ottenere le informazioni di configurazione e lo stato sulla console Amazon Redshift.

Visualizzazione dei dettagli di un'integrazione Zero-ETL

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel riquadro di navigazione sinistro, scegli il pannello di controllo Serverless o Cluster con provisioning. Quindi, scegli Integrazioni Zero-ETL.
3. Seleziona l'integrazione zero-ETL che desideri visualizzare. Per ogni integrazione, vengono fornite le informazioni seguenti:
  - ID di integrazione è l'identificatore restituito al momento della creazione dell'integrazione.
  - Stato può essere uno dei seguenti:
    - **Active**— L'integrazione Zero-ETL invia dati transazionali al data warehouse Amazon Redshift di destinazione.
    - **Syncing**— L'integrazione zero-ETL ha riscontrato un errore recuperabile e sta effettuando il reseed dei dati. Le tabelle interessate non sono disponibili per l'esecuzione di query in Amazon Redshift fino al termine della risincronizzazione.
    - **Failed**— L'integrazione zero-ETL ha rilevato un evento o un errore irreversibile che non può essere corretto. È necessario eliminare e ricreare l'integrazione zero-ETL.
    - **Creating**— L'integrazione zero-ETL è in fase di creazione.
    - **Deleting**— L'integrazione zero-ETL viene eliminata.

- **Needs attention**— L'integrazione zero-ETL ha rilevato un evento o un errore che richiede un intervento manuale per risolverlo. Per risolvere il problema, segui la procedura indicata nel messaggio di errore.
- **ARN di origine** è l'ARN dei dati di origine.
- **Destinazione** è l'ARN dello spazio dei nomi del data warehouse di destinazione.
- **Database** può essere uno dei seguenti:
  - **No database**: non esiste un database di destinazione per l'integrazione.
  - **Creating**: Amazon Redshift sta creando il database di destinazione per l'integrazione.
  - **Active**: i dati vengono replicati dall'origine di integrazione in Amazon Redshift.
  - **Error**: si è verificato un errore nell'integrazione.
  - **Recovering**: l'integrazione viene ripristinata dopo il riavvio del data warehouse.
  - **Resyncing**: Amazon Redshift sta risincronizzando le tabelle nell'integrazione.
- **Tipo di destinazione** è il tipo di data warehouse Amazon Redshift.
- **Data di creazione** è la data e l'ora (UTC) in cui è stata creata l'integrazione.

#### Note

Per visualizzare i dettagli dell'integrazione per un data warehouse, scegli la pagina dei dettagli del cluster con provisioning o dello spazio dei nomi serverless, quindi seleziona la scheda Integrazioni Zero-ETL.

Nell'elenco Integrazioni Zero-ETL puoi scegliere Esegui query sui dati per passare all'Editor di query Amazon Redshift v2. Il database di destinazione Amazon Redshift ha il parametro [enable\\_case\\_sensitive\\_identifier](#) abilitato. Quando scrivi l'istruzione SQL, potrebbe essere necessario racchiudere i nomi di schemi, tabelle e colonne tra virgolette doppie ("**<nome>**"). Per ulteriori informazioni sull'esecuzione di query sui dati nel data warehouse Amazon Redshift, consulta [Esecuzione di query in un database con l'editor di query v2 di Amazon Redshift](#).

Nell'elenco Integrazioni zero-ETL puoi scegliere Condividi dati per creare un'unità di condivisione dati. Per creare un'unità di condivisione dati per il database Amazon Redshift, segui le istruzioni visualizzate nella pagina Crea unità di condivisione dati. Prima di poter condividere i dati nel database Amazon Redshift devi creare un database di destinazione. Per ulteriori informazioni sulla condivisione dei dati, consulta [Concetti di condivisione dei dati per Amazon Redshift](#).

Per aggiornare l'integrazione puoi utilizzare il comando [ALTER DATABASE](#). In questo modo tutti i dati dall'origine di integrazione vengono replicati nel database di destinazione. L'esempio seguente aggiorna tutte le tabelle sincronizzate e non riuscite nell'integrazione Zero-ETL.

```
ALTER DATABASE sample_integration_db INTEGRATION REFRESH ALL tables;
```

## Condivisione dei dati in Amazon Redshift

Dopo aver aggiunto i dati all'origine, questi vengono immediatamente replicati in Amazon Redshift e sono pronti per essere condivisi creando unità di condivisione dati.

Per condividere i dati, devi innanzitutto creare un database di destinazione.

### Important

Per condividere i dati da un data warehouse di anteprima Amazon Redshift a un data warehouse consumer Amazon Redshift, il data warehouse consumer deve essere nella traccia `preview_2023`. Per ulteriori informazioni sulle unità di condivisione dati, consulta [Che cos'è una unità di condivisione dati?](#) nella Guida per sviluppatori di database di Amazon Redshift.

Per creare un data warehouse di destinazione in anteprima, consulta uno dei seguenti argomenti a seconda del tipo di implementazione:

- Cluster con provisioning di Amazon Redshift: [Creazione di un cluster di anteprima](#).
- Gruppo di lavoro Amazon Redshift serverless: [Creazione di un gruppo di lavoro di anteprima](#).

## Condivisione dei dati in Amazon Redshift serverless mediante la console Amazon Redshift

1. Nel riquadro di navigazione a sinistra della console Amazon Redshift scegli Amazon Redshift serverless > Pannello di controllo serverless.
2. Nel riquadro di navigazione sinistro, scegli Integrazioni zero-ETL.
3. Scegliere Share data (Condividi dati).
4. Nella pagina Crea unità di condivisione dati effettua i passaggi descritti in [Creazione di unità di condivisione dati](#).

## Condivisione dei dati nei cluster con provisioning di Amazon Redshift mediante la console Amazon Redshift

1. Nel riquadro di navigazione a sinistra della console Amazon Redshift scegli Pannello di controllo dei cluster con provisioning.
2. Nel riquadro di navigazione sinistro, scegli Integrazioni zero-ETL.
3. Dall'elenco delle integrazioni, scegli un'integrazione.
4. Nella pagina dei dettagli dell'integrazione scegli Connetti al database.
5. Nella pagina Connessione al database puoi creare una nuova connessione o utilizzarne una recente. Assicurati che la connessione sia stata stabilita al database di destinazione.
6. Se crei una nuova connessione, inserisci un Nome database per il database. Quindi, fai clic su Connetti.
7. Nella pagina dei dettagli dell'integrazione scegli Condividi dati.
8. Nella pagina Crea unità di condivisione dati effettua i passaggi descritti in [Creazione di unità di condivisione dati](#).

## Metriche per le integrazioni Zero-ETL

Puoi utilizzare i parametri nella console Amazon Redshift e CloudWatch Amazon per conoscere lo stato e le prestazioni delle tue integrazioni zero-ETL. Puoi modificare le metriche per visualizzare i dati per una durata più o meno lunga oppure scegliere di visualizzare le metriche in CloudWatch. Per visualizzare le metriche per l'integrazione sulla console Amazon Redshift, scegli Integrazioni Zero-ETL nel riquadro di navigazione a sinistra e seleziona l'ID di integrazione.

Per le integrazioni Zero-ETL Aurora e Amazon RDS, Amazon Redshift fornisce due tipi di metriche nella pagina dei dettagli dell'integrazione. I tipi di metriche sono i seguenti:

- Dalla scheda Metriche di integrazione, questi sono i grafici disponibili:

Parametro	Descrizione
Lag	L'intervallo tra il momento in cui viene eseguito il commit dei dati sull'origine e il momento in cui i dati sono disponibili per le query in Amazon Redshift.  Unità: secondi

Parametro	Descrizione
	Dimensioni: IntegrationLag
Tables replicated	<p>Il numero di tabelle che sono state replicate dal database di origine ad Amazon Redshift.</p> <p>Unità: numero</p> <p>Dimensioni: IntegrationNumTablesReplicated</p>
Tables failed	<p>Il numero di tabelle che hanno restituito un errore di replica.</p> <p>Unità: numero</p> <p>Dimensioni: IntegrationNumTablesFailedReplication</p>

- Dalla scheda Statistiche della tabella, è possibile visualizzare l'elenco delle tabelle attualmente attive o con errori. Le statistiche presenti in questa scheda sono le seguenti:
  - Nome dello schema: il nome dello schema in cui si trova la tabella.
  - Nome della tabella: il nome della tabella nel database di origine.
  - Stato: lo stato della tabella. I valori possibili sono Synced, Failed, Deleted, Resync Required e Resync Initiated.
  - Database: il database Amazon Redshift in cui si trova la tabella.
  - Ultimo aggiornamento: la data e l'ora (UTC) dell'ultimo aggiornamento della tabella.

## Risoluzione dei problemi delle integrazioni Zero-ETL

### Risoluzione dei problemi delle integrazioni Zero-ETL con Aurora MySQL

Utilizza le informazioni riportate di seguito per risolvere i problemi più comuni riscontrati per le integrazioni Zero-ETL con Aurora MySQL.

#### Argomenti

- [La creazione dell'integrazione non è riuscita](#)
- [Le tabelle non hanno chiavi primarie](#)

- [Tipi di dati non supportati nelle tabelle](#)
- [Comandi DML \(Data manipulation language\) non riusciti](#)
- [Le modifiche tracciate tra le origini dati non corrispondono](#)
- [Autorizzazione non riuscita](#)
- [Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950](#)
- [Amazon Redshift non è in grado di caricare i dati](#)
- [Le impostazioni dei parametri del gruppo di lavoro non sono corrette](#)
- [Il database non è stato creato per attivare un'integrazione Zero-ETL](#)
- [La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata](#)

La creazione dell'integrazione non è riuscita

Se la creazione dell'integrazione Zero-ETL non è riuscita, lo stato dell'integrazione è `Inactive`. Assicurati che quanto segue sia corretto per il cluster DB Aurora di origine:

- Hai creato il cluster nella console Amazon RDS.
- Il cluster Aurora DB di origine esegue MySQL versione 3.05 o successiva. Per la convalida, vai alla scheda Configurazione del cluster e controlla la Versione del motore.
- Hai configurato correttamente le impostazioni dei parametri binlog per il cluster. Se i parametri binlog di Aurora MySQL sono impostati in modo errato o non sono associati al cluster database Aurora di origine, la creazione non riesce. Consulta [Configure DB cluster parameters](#) (Configurazione dei parametri del cluster database).

Inoltre, assicurati che quanto segue sia corretto per il data warehouse Amazon Redshift:

- La distinzione tra maiuscole e minuscole è attivata. Per informazioni, consulta [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#).
- Hai aggiunto il principale autorizzato e l'origine di integrazione corretti per lo spazio dei nomi. Per informazioni, consulta [Configurazione dell'autorizzazione per il data warehouse Amazon Redshift](#).

Le tabelle non hanno chiavi primarie

Nel database di destinazione, una o più tabelle non dispongono di una chiave primaria e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Puoi aggiungere alle tabelle le chiavi primarie e Amazon Redshift risincronizza le tabelle. In alternativa, sebbene non consigliabile, puoi rilasciare queste tabelle in Aurora e crearle con una chiave primaria. Per ulteriori informazioni, consulta [Best practice di Amazon Redshift per la progettazione di tabelle](#).

#### Tipi di dati non supportati nelle tabelle

Nel database che hai creato dall'integrazione in Amazon Redshift e in cui i dati vengono replicati dal cluster di database Aurora, una o più tabelle hanno tipi di dati non supportati e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Rimuovi quindi queste tabelle e ricreane di nuove su Amazon RDS. Per ulteriori informazioni sui tipi di dati non supportati, consulta [Differenze tra i tipi di dati tra i database Aurora e Amazon Redshift](#) nella Guida per l'utente di Amazon Aurora.

#### Comandi DML (Data manipulation language) non riusciti

Amazon Redshift non è riuscito a eseguire comandi DML sulle tabelle Redshift. Per risolvere questo problema, utilizza `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Amazon Redshift risincronizza automaticamente le tabelle per correggere questo errore.

#### Le modifiche tracciate tra le origini dati non corrispondono

Questo errore si verifica quando le modifiche tra Amazon Aurora e Amazon Redshift non corrispondono, portando l'integrazione in uno stato `Failed`.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

#### Autorizzazione non riuscita

L'autorizzazione non è riuscita perché il cluster DB Aurora di origine è stato rimosso come origine di integrazione autorizzata per il data warehouse Amazon Redshift.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950

Per un data warehouse di destinazione, il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950. Amazon Aurora non può inviare dati ad Amazon Redshift. Il numero di tabelle e schemi supera il limite impostato. Per risolvere questo problema, rimuovi gli schemi o le tabelle non necessari dal database di origine.

Amazon Redshift non è in grado di caricare i dati

Amazon Redshift non è in grado di caricare i dati nell'integrazione Zero-ETL.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Le impostazioni dei parametri del gruppo di lavoro non sono corrette

La distinzione tra maiuscole e minuscole non è attivata per il gruppo di lavoro.

Per risolvere questo problema, vai alla scheda Proprietà nella pagina dei dettagli delle integrazioni, scegli il gruppo di parametri e attiva l'identificatore con distinzione tra maiuscole e minuscole dalla scheda Proprietà. Se non disponi di un gruppo di parametri esistente, creane uno con l'identificatore con distinzione tra maiuscole e minuscole attivato. Quindi, crea una nuova integrazione zero-ETL su Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL).

Il database non è stato creato per attivare un'integrazione Zero-ETL

Non esiste un database creato per attivare un'integrazione Zero-ETL.

Per risolvere questo problema, crea un database per l'integrazione. Per ulteriori informazioni, consulta [Creazione di un database di destinazione in Amazon Redshift](#).

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata.

Per raccogliere informazioni più dettagliate sugli errori relativi al motivo per cui la tabella si trova in questo stato, utilizza la vista di sistema [SYS\\_LOAD\\_ERROR\\_DETAIL](#).

## Risoluzione dei problemi delle integrazioni Zero-ETL con Aurora PostgreSQL

Utilizza le informazioni riportate di seguito per risolvere i problemi più comuni riscontrati per le integrazioni Zero-ETL con Aurora PostgreSQL.

### Argomenti

- [La creazione dell'integrazione non è riuscita](#)
- [Le tabelle non hanno chiavi primarie](#)
- [Tipi di dati non supportati nelle tabelle](#)
- [Comandi DML \(Data manipulation language\) non riusciti](#)
- [Le modifiche tracciate tra le origini dati non corrispondono](#)
- [Autorizzazione non riuscita](#)
- [Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950](#)
- [Amazon Redshift non è in grado di caricare i dati](#)
- [Le impostazioni dei parametri del gruppo di lavoro non sono corrette](#)
- [Il database non è stato creato per attivare un'integrazione Zero-ETL](#)
- [La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata](#)

La creazione dell'integrazione non è riuscita

Se la creazione dell'integrazione Zero-ETL non è riuscita, lo stato dell'integrazione è `Inactive`. Assicurati che quanto segue sia corretto per il cluster DB Aurora di origine:

- Hai creato il cluster nella console Amazon RDS.
- Il cluster di database Aurora di origine esegue Aurora PostgreSQL 15.4.99 o versioni successive. Per la convalida, vai alla scheda Configurazione del cluster e controlla la Versione del motore.
- Hai configurato correttamente le impostazioni dei parametri binlog per il cluster. Se i parametri binlog di Aurora PostgreSQL sono impostati in modo errato o non sono associati al cluster di database Aurora di origine, la creazione non riesce. Consulta [Configure DB cluster parameters](#) (Configurazione dei parametri del cluster database).

Inoltre, assicurati che quanto segue sia corretto per il data warehouse Amazon Redshift:

- La distinzione tra maiuscole e minuscole è attivata. Per informazioni, consulta [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#).

- Hai aggiunto il principale autorizzato e la fonte di integrazione corretti per `endterm="zero-etl-using.redshift-iam.title» />`.

### Le tabelle non hanno chiavi primarie

Nel database di destinazione, una o più tabelle non dispongono di una chiave primaria e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Puoi aggiungere alle tabelle le chiavi primarie e Amazon Redshift risincronizza le tabelle. In alternativa, sebbene non consigliabile, puoi rilasciare queste tabelle in Aurora e crearle con una chiave primaria. Per ulteriori informazioni, consulta [Best practice di Amazon Redshift per la progettazione di tabelle](#).

### Tipi di dati non supportati nelle tabelle

Nel database che hai creato dall'integrazione in Amazon Redshift e in cui i dati vengono replicati dal cluster di database Aurora, una o più tabelle hanno tipi di dati non supportati e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Rimuovi quindi queste tabelle e ricreane di nuove su Amazon RDS. Per ulteriori informazioni sui tipi di dati non supportati, consulta [Differenze tra i tipi di dati tra i database Aurora e Amazon Redshift](#) nella Guida per l'utente di Amazon Aurora.

### Comandi DML (Data manipulation language) non riusciti

Amazon Redshift non è riuscito a eseguire comandi DML sulle tabelle Redshift. Per risolvere questo problema, utilizza `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Amazon Redshift risincronizza automaticamente le tabelle per correggere questo errore.

### Le modifiche tracciate tra le origini dati non corrispondono

Questo errore si verifica quando le modifiche tra Amazon Aurora e Amazon Redshift non corrispondono, portando l'integrazione in uno stato `Failed`.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

## Autorizzazione non riuscita

L'autorizzazione non è riuscita perché il cluster DB Aurora di origine è stato rimosso come origine di integrazione autorizzata per il data warehouse Amazon Redshift.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950

Per un data warehouse di destinazione, il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950. Amazon Aurora non può inviare dati ad Amazon Redshift. Il numero di tabelle e schemi supera il limite impostato. Per risolvere questo problema, rimuovi gli schemi o le tabelle non necessari dal database di origine.

Amazon Redshift non è in grado di caricare i dati

Amazon Redshift non è in grado di caricare i dati nell'integrazione Zero-ETL.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Le impostazioni dei parametri del gruppo di lavoro non sono corrette

La distinzione tra maiuscole e minuscole non è attivata per il gruppo di lavoro.

Per risolvere questo problema, vai alla scheda Proprietà nella pagina dei dettagli delle integrazioni, scegli il gruppo di parametri e attiva l'identificatore con distinzione tra maiuscole e minuscole dalla scheda Proprietà. Se non disponi di un gruppo di parametri esistente, creane uno con l'identificatore con distinzione tra maiuscole e minuscole attivato. Quindi, crea una nuova integrazione zero-ETL su Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL).

Il database non è stato creato per attivare un'integrazione Zero-ETL

Non esiste un database creato per attivare un'integrazione Zero-ETL.

Per risolvere questo problema, crea un database per l'integrazione. Per ulteriori informazioni, consulta [Creazione di un database di destinazione in Amazon Redshift](#).

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata.

Per raccogliere informazioni più dettagliate sugli errori relativi al motivo per cui la tabella si trova in questo stato, utilizza la vista di sistema [SYS\\_LOAD\\_ERROR\\_DETAIL](#).

## Risoluzione dei problemi delle integrazioni Zero-ETL con RDS per MySQL

Utilizza le informazioni riportate di seguito per risolvere i problemi più comuni riscontrati per le integrazioni Zero-ETL con RDS per MySQL.

### Argomenti

- [La creazione dell'integrazione non è riuscita](#)
- [Le tabelle non hanno chiavi primarie](#)
- [Tipi di dati non supportati nelle tabelle](#)
- [Comandi DML \(Data manipulation language\) non riusciti](#)
- [Le modifiche tracciate tra le origini dati non corrispondono](#)
- [Autorizzazione non riuscita](#)
- [Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950](#)
- [Amazon Redshift non è in grado di caricare i dati](#)
- [Le impostazioni dei parametri del gruppo di lavoro non sono corrette](#)
- [Il database non è stato creato per attivare un'integrazione Zero-ETL](#)
- [La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata](#)

La creazione dell'integrazione non è riuscita

Se la creazione dell'integrazione Zero-ETL non è riuscita, lo stato dell'integrazione è `Inactive`. Assicurati di aver eseguito le seguenti operazioni per l'istanza database RDS di origine:

- L'istanza è stata creata nella console Amazon RDS.
- L'istanza DB RDS di origine esegue RDS for MySQL versione 8.0.32 o successiva. Per la verifica, vai alla scheda Configurazione dell'istanza e controlla la Versione del motore.
- Le impostazioni dei parametri binlog sono state correttamente impostate per l'istanza. Se i parametri binlog di RDS per MySQL sono impostati in modo errato o non sono associati all'istanza database RDS di origine, la creazione non riesce. Consulta [Configure DB instance parameters](#).

Inoltre, assicurati che quanto segue sia corretto per il data warehouse Amazon Redshift:

- La distinzione tra maiuscole e minuscole è attivata. Per informazioni, consulta [Attivazione della distinzione tra maiuscole e minuscole per il data warehouse](#).
- Hai aggiunto il principale autorizzato e l'origine di integrazione corretti per lo spazio dei nomi. Per informazioni, consulta [Configurazione dell'autorizzazione per il data warehouse Amazon Redshift](#).

### Le tabelle non hanno chiavi primarie

Nel database di destinazione, una o più tabelle non dispongono di una chiave primaria e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Puoi aggiungere alle tabelle le chiavi primarie e Amazon Redshift risincronizza le tabelle. In alternativa, sebbene non consigliabile, puoi rilasciare queste tabelle in RDS e crearle con una chiave primaria. Per ulteriori informazioni, consulta [Best practice di Amazon Redshift per la progettazione di tabelle](#).

### Tipi di dati non supportati nelle tabelle

Nel database di destinazione che hai creato in Amazon Redshift e in cui i dati vengono replicati dall'istanza database RDS, una o più tabelle hanno tipi di dati non supportati e non possono essere sincronizzate.

Per risolvere questo problema, vai alla scheda Statistiche della tabella nella pagina dei dettagli delle integrazioni oppure usa `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Rimuovi quindi queste tabelle e ricreane di nuove su Amazon RDS. Per ulteriori informazioni sui tipi di dati non supportati, consulta [Differenze tra i tipi di dati tra i database Aurora e Amazon Redshift](#) nella Guida per l'utente di Amazon RDS.

### Comandi DML (Data manipulation language) non riusciti

Amazon Redshift non è riuscito a eseguire comandi DML sulle tabelle Redshift. Per risolvere questo problema, utilizza `SVV_INTEGRATION_TABLE_STATE` per visualizzare le tabelle con errori. Amazon Redshift risincronizza automaticamente le tabelle per correggere questo errore.

Le modifiche tracciate tra le origini dati non corrispondono

Questo errore si verifica quando le modifiche tra Amazon Aurora e Amazon Redshift non corrispondono, portando l'integrazione in uno stato `Failed`.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Autorizzazione non riuscita

L'autorizzazione non è riuscita perché l'istanza database RDS di origine è stata rimossa come origine di integrazione autorizzata per il data warehouse Amazon Redshift.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950

Per un data warehouse di destinazione, il numero di tabelle è superiore a 100.000 o il numero di schemi è superiore a 4950. Amazon Aurora non può inviare dati ad Amazon Redshift. Il numero di tabelle e schemi supera il limite impostato. Per risolvere questo problema, rimuovi gli schemi o le tabelle non necessari dal database di origine.

Amazon Redshift non è in grado di caricare i dati

Amazon Redshift non è in grado di caricare i dati nell'integrazione Zero-ETL.

Per risolvere il problema, elimina l'integrazione Zero-ETL e creala nuovamente in Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL) e [Deleting zero-ETL integrations](#) (Eliminazione di integrazioni Zero-ETL).

Le impostazioni dei parametri del gruppo di lavoro non sono corrette

La distinzione tra maiuscole e minuscole non è attivata per il gruppo di lavoro.

Per risolvere questo problema, vai alla scheda Proprietà nella pagina dei dettagli delle integrazioni, scegli il gruppo di parametri e attiva l'identificatore con distinzione tra maiuscole e minuscole dalla scheda Proprietà. Se non disponi di un gruppo di parametri esistente, creane uno con l'identificatore con distinzione tra maiuscole e minuscole attivato. Quindi, crea una nuova integrazione zero-ETL

su Amazon RDS. Per ulteriori informazioni, consulta [Creating zero-ETL integrations](#) (Creazione di integrazioni Zero-ETL).

Il database non è stato creato per attivare un'integrazione Zero-ETL.

Non esiste un database creato per attivare un'integrazione Zero-ETL.

Per risolvere questo problema, crea un database per l'integrazione. Per ulteriori informazioni, consulta [Creazione di un database di destinazione in Amazon Redshift](#).

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata.

La tabella è nello stato Risincronizzazione richiesta o Risincronizzazione avviata.

Per raccogliere informazioni più dettagliate sugli errori relativi al motivo per cui la tabella si trova in questo stato, utilizza la vista di sistema [SYS\\_LOAD\\_ERROR\\_DETAIL](#).

# Esecuzione di query su un database

Per eseguire query sui database ospitati dal cluster Amazon Redshift, sono disponibili due opzioni:

- Connect al cluster ed esegui query AWS Management Console con l'editor di query.

Se l'editor di query viene utilizzato sulla console Amazon Redshift, non è necessario scaricare e configurare un'applicazione client SQL.

- Connettiti al cluster con uno strumento client SQL, ad esempio SQL Workbench/J.

Amazon Redshift supporta strumenti client SQL che si connettono tramite Java Database Connectivity (JDBC) e Open Database Connectivity (ODBC). Amazon Redshift non fornisce né installa alcuna libreria o alcuno strumento client SQL, pertanto al fine di utilizzarli è necessario installarli sul computer client o su un'istanza Amazon EC2. Puoi usare la maggior parte degli strumenti del client SQL che supportano i driver JDBC o ODBC.

## Note

Quando si scrivono le stored procedure, si consiglia di attenersi a una best practice per proteggere i valori sensibili:

Non eseguire la codifica fissa delle informazioni sensibili nella logica delle procedure archiviate. Ad esempio, non assegnare una password utente in un'istruzione CREATE USER nel corpo di una procedura archiviata. Ciò rappresenta un rischio per la sicurezza, poiché i valori con codifica fissa possono essere registrati come metadati dello schema nelle tabelle del catalogo. È invece consigliabile passare i valori sensibili, ad esempio le password, come argomenti alla procedura archiviata, mediante parametri.

Per ulteriori informazioni sulle procedure archiviate, consulta [CREATE PROCEDURE](#) e [Creazione di procedure archiviate in Amazon Redshift](#). Per ulteriori informazioni sulle tabelle di catalogo, consulta [Tabelle di catalogo di sistema](#).

## Argomenti

- [Connessione ad Amazon Redshift](#)
- [Esecuzione di query in un database con l'editor di query v2 di Amazon Redshift](#)
- [Esecuzione di query in un database con l'editor della query](#)
- [Connessione a un data warehouse Amazon Redshift tramite strumenti client SQL](#)

- [Usò dell'API dati di Amazon Redshift](#)

## Connessione ad Amazon Redshift

Puoi connetterti al tuo database utilizzando la seguente sintassi.

```
cluster-name.account-number.aws-region.redshift.amazonaws.com/database-name
```

Gli elementi della sintassi sono definiti come segue.

- `cluster-name`

Il nome del tuo cluster.

- `account-number`

L'identificatore univoco associato al tuo numero di AWS conto in un determinato Regione AWS caso. Tutti i cluster creati da un determinato account in un determinato account Regione AWS hanno lo stesso valore. `account-number`

- `aws-region`

Il codice in cui Regione AWS si trova il cluster.

- `database-name`

Il nome del tuo database.

Ad esempio, la seguente stringa di connessione specifica il `my-db` database nel `my-cluster` cluster Regione AWS `us-east-1`.

```
my-cluster.123456789012.us-east-1.redshift.amazonaws.com/my-db
```

## Esecuzione di query in un database con l'editor di query v2 di Amazon Redshift

L'editor di query v2 è un'applicazione client SQL basata sul Web separata che utilizzi per creare ed eseguire query sul data warehouse Amazon Redshift. Puoi visualizzare i risultati nei grafici e

collaborare condividendo le tue domande con altri membri del tuo team. L'editor di query v2 è un sostituto del precedente editor di query.

### Note

L'editor di query v2 è disponibile in commercio Regioni AWS. Per un elenco delle aree Regioni AWS in cui è disponibile l'editor di query v2, consulta gli endpoint elencati per [Redshift query editor](#) v2 in. Riferimenti generali di Amazon Web Services

Per una demo dell'editor di query v2, guardare il video seguente. [Editor di query Amazon Redshift v2](#).

Per una demo dell'analisi dei dati, guardare il video seguente. [Analisi dei dati con l'editor di query Amazon Redshift v2](#).

Per una demo sull'utilizzo dell'editor di query v2 per eseguire più query con una connessione isolata o condivisa, guarda questo video: [Concurrent Query Execution using Query Editor v2](#) (Esecuzione simultanea di query mediante l'editor di query v2).

L'editor di query v2 ha un ricco set di funzionalità per gestire ed eseguire le istruzioni SQL. Gli argomenti nelle sezioni seguenti ti consentono di iniziare con molte di queste funzionalità. Esplora l'editor di query v2 da solo per familiarizzare con le sue capacità.

### Argomenti

- [Configurazione del Account AWS](#)
- [Utilizzo dell'editor di query v2](#)
- [Interazione con SQL generativo dell'editor di query v2 \(anteprima\)](#)
- [Caricamento dei dati in un database](#)
- [Autorizzazione e esecuzione di query](#)
- [Autorizzazione ed esecuzione di notebook](#)
- [Interrogare il AWS Glue Data Catalog](#)
- [Esecuzione di query in un data lake](#)
- [Utilizzo dell'unità di condivisione dati](#)
- [Pianificazione di una query con l'editor di query v2](#)
- [Visualizzazione dei risultati delle query](#)
- [Collaborazione e condivisione come team](#)

## Configurazione del Account AWS

Quando scegli l'editor di query v2 dalla console Amazon Redshift, si apre una nuova scheda del browser con l'interfaccia dell'editor di query v2. Con le autorizzazioni appropriate, puoi accedere ai dati in un cluster o gruppo di lavoro Amazon Redshift di Account AWS tua proprietà che si trova attualmente. Regione AWS

La prima volta che un amministratore configura l'editor di query v2 per te Account AWS, sceglie AWS KMS key quello da utilizzare per crittografare le risorse dell'editor di query v2. Per impostazione predefinita, viene utilizzata una chiave AWS proprietaria per crittografare le risorse. In alternativa, un amministratore può utilizzare una chiave gestita dal cliente scegliendo l'ARN (Amazon Resource Name) per la chiave nella pagina di configurazione. Dopo aver configurato un account, le impostazioni di AWS KMS crittografia non possono essere modificate. Per ulteriori informazioni sulla creazione e l'utilizzo di una chiave gestita dal cliente con l'editor di query v2, consultare [Creazione di una chiave gestita dal AWS KMS cliente da utilizzare con Query Editor v2](#). L'amministratore può anche scegliere facoltativamente S3 bucket (Bucket S3) e un percorso utilizzati per alcune funzionalità, come il caricamento di dati da un file. Per ulteriori informazioni, consulta [Caricamento di dati da una configurazione di file e da un flusso di lavoro locali](#).

L'editor di query v2 di Amazon Redshift supporta l'autenticazione, la crittografia, l'isolamento e la conformità per mantenere al sicuro i dati a riposo e i dati in transito. Per ulteriori informazioni sulla sicurezza dei dati e sull'editor di query v2, consultare:

- [Crittografia dei dati inattivi](#)
- [Crittografia in transito](#)
- [Analisi della configurazione e delle vulnerabilità in Amazon Redshift](#)

AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto tuo Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni su come l'editor di query V2 funziona su AWS CloudTrail, consulta [Registrazione con CloudTrail](#). Per ulteriori informazioni in merito CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

L'editor di query v2 ha quote regolabili per alcune delle sue risorse. Per ulteriori informazioni, consulta [Quote per gli oggetti Amazon Redshift](#).

## Risorse create con l'editor di query v2

All'interno dell'editor di query v2, è possibile creare risorse come query e grafici salvati. Tutte le risorse nell'editor di query v2 sono associate a un utente o un ruolo IAM. Consigliamo di collegare le policy a un ruolo IAM e di assegnare il ruolo a un utente.

Nell'editor di query v2, è possibile aggiungere e rimuovere tag per query e grafici salvati. È possibile utilizzare questi tag quando si impostano criteri IAM personalizzati o per cercare risorse. Puoi anche gestire i tag utilizzando il AWS Resource Groups Tag Editor.

Puoi configurare i ruoli IAM con le policy IAM per condividere le query con altri membri del Regione AWS tuo stesso account Account AWS in.

## Creazione di una chiave gestita dal AWS KMS cliente da utilizzare con Query Editor v2

Per creare una chiave di crittografia simmetrica gestita dal cliente:

È possibile creare una chiave di crittografia simmetrica gestita dal cliente per crittografare le risorse dell'editor di query v2 utilizzando le operazioni della AWS KMS console o dell'API. AWS KMS Per istruzioni sulla creazione di una chiave, consulta [Creazione di una chiave di crittografia AWS KMS simmetrica](#) nella Guida per gli sviluppatori.AWS Key Management Service

### Policy della chiave

Le policy della chiave controllano l'accesso alla chiave gestita dal cliente. Ogni chiave gestita dal cliente deve avere esattamente una policy della chiave, che contiene istruzioni che determinano chi può usare la chiave e come la possono usare. Quando crei la chiave gestita dal cliente, puoi specificare una policy della chiave. Per ulteriori informazioni, consulta [Gestire l'accesso alle AWS KMS chiavi nella Guida per](#) gli AWS Key Management Service sviluppatori.

Per utilizzare la chiave gestita dal cliente con Amazon Redshift query editor v2, è necessario che le seguenti operazioni API siano consentite nella policy chiave:

- `kms:GenerateDataKey` — Genera una chiave dati simmetrica univoca per crittografare i tuoi dati.
- `kms:Decrypt` — Decrittifica i dati crittografati con la chiave gestita dal cliente.
- `kms:DescribeKey` — Fornisce i dettagli della chiave gestiti dal cliente per consentire al servizio di convalidare la chiave.

Di seguito è riportato un esempio di AWS KMS politica per Account AWS 111122223333. Nella prima sezione, il `kms:ViaService` limita l'uso della chiave al servizio dell'editor di query v2 (che è denominato `sqlworkbench.region.amazonaws.com` nella policy). L' Account AWS utilizzo della chiave deve essere 111122223333. Nella seconda sezione, l'utente root e gli amministratori chiave di Account AWS 111122223333 possono accedere alla chiave.

Quando si crea un account Account AWS, si inizia con un'unica 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.

```
{
  "Version": "2012-10-17",
  "Id": "key-consolepolicy",
  "Statement": [
    {
      "Sid": "Allow access to principals authorized to use Amazon Redshift Query
Editor V2",
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": "sqlworkbench.region.amazonaws.com",
          "kms:CallerAccount": "111122223333"
        }
      }
    },
    {
      "Sid": "Allow access for key administrators",
      "Effect": "Allow",
      "Principal": {
```

```
    "AWS": "arn:aws:iam::111122223333:root"
  },
  "Action": [
    "kms:*"
  ],
  "Resource": "arn:aws:kms:region:111122223333:key/key_ID"
}
]
```

Le seguenti risorse forniscono ulteriori informazioni sulle AWS KMS chiavi:

- Per ulteriori informazioni sulle AWS KMS politiche, vedere [Specificare le autorizzazioni in una politica nella Guida](#) per gli AWS Key Management Service sviluppatori.
- Per informazioni sulla risoluzione dei problemi relativi alle AWS KMS politiche, consulta [Risoluzione dei problemi di accesso tramite chiave](#) nella Guida per gli AWS Key Management Service sviluppatori.
- Per ulteriori informazioni sulle chiavi, consultare [Chiavi KMS AWS](#) nella Guida per gli sviluppatori di AWS Key Management Service .

## Accesso all'editor di query v2

Per accedere all'editor di query v2, sono necessarie le opportune autorizzazioni. Un amministratore può allegare una delle seguenti politiche AWS gestite al ruolo per concedere l'autorizzazione. Consigliamo di collegare le policy a un ruolo IAM e di assegnare il ruolo a un utente. Queste politiche AWS gestite sono scritte con diverse opzioni che controllano il modo in cui l'etichettatura delle risorse consente la condivisione delle query. Per collegare le policy IAM è possibile utilizzare la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.

- AmazonRedshiftQueryEditorV2 FullAccess — Garantisce l'accesso completo alle operazioni e alle risorse dell'editor di query Amazon Redshift v2. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti.
- AmazonRedshiftQueryEditorV2 NoSharing: consente di lavorare con Amazon Redshift Query Editor v2 senza condividere risorse. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti.
- AmazonRedshiftQueryEditorV2 ReadSharing — Garantisce la possibilità di lavorare con Amazon Redshift Query Editor v2 con una condivisione limitata delle risorse. Il principale concesso

può leggere le risorse condivise con il suo team ma non può aggiornarle. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti.

- `AmazonRedshiftQueryEditorReadWriteCondivisione V2`: consente di lavorare con Amazon Redshift Query Editor v2 con condivisione di risorse. Il principale concesso può leggere e aggiornare le risorse condivise con il suo team. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti.

Puoi anche creare una policy in base alle autorizzazioni consentite e negate nelle policy gestite fornite. Se si utilizza l'editor policy della console IAM per creare le proprie policy, scegliere SQL Workbench come servizio per il quale si crea la policy nell'editor visivo. L'editor di query v2 utilizza il nome del servizio SQL Workbench di AWS nell'editor visivo e nel simulatore di policy IAM.

Affinché un principale (un utente con un ruolo IAM assegnato) si connetta a un cluster di Amazon Redshift, deve disporre delle autorizzazioni in una delle policy gestite dell'editor di query v2. Hanno anche bisogno dell'autorizzazione `redshift:GetClusterCredentials` per il cluster. Per ottenere questa autorizzazione, un utente con autorizzazione amministrativa può collegare una policy ai ruoli IAM utilizzati per la connessione al cluster utilizzando le credenziali temporanee. È possibile assegnare la policy a cluster specifici o essere più generici. Per ulteriori informazioni sull'autorizzazione all'uso di credenziali temporanee, consulta [Creare un ruolo o un utente IAM](#) con autorizzazioni di chiamata. `GetClusterCredentials`

Affinché un principale (un utente IAM con un ruolo IAM assegnato) attivi la possibilità nella pagina Impostazioni dell'account per altri nell'account impostando Esporta set di risultati, ha bisogno dell'autorizzazione `sqlworkbench:UpdateAccountExportSettings` collegata al ruolo. Questa autorizzazione è inclusa nella politica `AmazonRedshiftQueryEditorV2FullAccess` AWS gestita.

Man mano che vengono aggiunte nuove funzionalità all'editor di query v2, le politiche AWS gestite vengono aggiornate in base alle esigenze. Se crei policy in base alle autorizzazioni consentite e negate nelle policy gestite fornite, assicurati di includere nelle tue policy le modifiche apportate alle policy gestite. Per ulteriori informazioni sulle policy gestite in Amazon Redshift, consultare [AWS politiche gestite per Amazon Redshift](#).

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creating a role for a third-party identity provider \(federation\)](#) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:
  - Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina [Creating a role for an IAM user](#) (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
  - (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente di IAM.

#### Note

Se un amministratore AWS IAM Identity Center rimuove tutte le associazioni per un determinato set di autorizzazioni nell'intero account, l'accesso a tutte le risorse dell'editor di query originariamente associate al set di autorizzazioni rimosso non è più disponibile. Se in seguito vengono ricreate le stesse autorizzazioni, viene creato un nuovo identificatore interno. Poiché l'identificatore interno è cambiato, non è possibile accedere alle risorse dell'editor di query precedentemente di proprietà di un utente. Prima che gli amministratori eliminino un set di autorizzazioni, si consiglia agli utenti di tale set di autorizzazioni di esportare in un backup le risorse dell'editor di query, ad esempio notebook e query.

## Configurazione dei tag principali per la connessione a un cluster o un gruppo di lavoro dall'editor di query v2

Per connettersi al cluster o al gruppo di lavoro utilizzando l'opzione utente federato, imposta l'utente o il ruolo IAM con i tag principali. In alternativa, configura il gestore dell'identità digitale (IdP) per passare in `RedshiftDbUser` e (facoltativamente) in `RedshiftDbGroups`. Per ulteriori informazioni sull'utilizzo di IAM per gestire i tag, consulta [Passare i tag di sessione in AWS Security Token Service](#) nella Guida per l'utente IAM. Per configurare l'accesso utilizzando AWS Identity and Access Management, un amministratore può aggiungere tag utilizzando la console IAM (<https://console.aws.amazon.com/iam/>).

## Come aggiungere tag principali a un ruolo IAM

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 riquadro di navigazione scegliere Roles (Ruoli).
3. Scegli il ruolo che deve accedere all'editor di query v2 utilizzando un utente federato.
4. Seleziona la scheda Tags (Tag).
5. Scegliere Manage tags (Gestisci tag).
6. Scegli Add tag (Aggiungi tag), immetti la Key (Chiave) come RedshiftDbUser e immetti un Value (Valore) del nome utente federato.
7. Facoltativamente, scegli Add tag (Aggiungi tag), immetti la Key (Chiave) come RedshiftDbGroups e immetti un Value (Valore) del nome del gruppo da associare all'utente.
8. Scegli Save changes (Salva le modifiche) per visualizzare l'elenco dei tag associati al ruolo IAM scelto. La propagazione delle modifiche potrebbe richiedere alcuni secondi.
9. Per utilizzare l'utente federato, aggiorna la pagina dell'editor di query v2 dopo la propagazione delle modifiche.

## Configurazione del gestore dell'identità digitale (IdP) per passare i tag principali

La procedura per configurare i tag utilizzando un gestore dell'identità digitale (IdP) varia in base all'IdP. Consulta la documentazione IdP per istruzioni su come trasferire le informazioni di utente e gruppo agli attributi SAML. Se configurati correttamente, i seguenti attributi vengono visualizzati nella risposta SAML che viene utilizzata da AWS Security Token Service per compilare i tag principali per RedshiftDbUser e RedshiftDbGroups

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbUser">
  <AttributeValue>db-user-name</AttributeValue>
</Attribute>
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:RedshiftDbGroups">
  <AttributeValue>db-groups</AttributeValue>
</Attribute>
```

L'opzionale *db\_groups* deve essere un elenco separato da due punti come group1:group2:group3.

Inoltre, è possibile impostare l'opzione TransitiveTagKeys per conservare i tag durante il concatenamento dei ruoli.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/TransitiveTagKeys">
  <AttributeValue>RedshiftDbUser</AttributeValue>
  <AttributeValue>RedshiftDbGroups</AttributeValue>
</Attribute>
```

Per ulteriori informazioni su come impostare l'editor di query v2, consulta [Autorizzazioni necessarie per utilizzare l'editor della query v2](#).

### Note

Quando ti connetti al cluster o al gruppo di lavoro utilizzando l'opzione di connessione Utente federato dell'editor di query v2, il gestore dell'identità digitale può fornire tag principali personalizzati per RedshiftDbUser e RedshiftDbGroups. Attualmente, AWS IAM Identity Center non supporta il passaggio di tag principali personalizzati direttamente all'editor di query v2.

## Utilizzo dell'editor di query v2

L'editor di query v2 viene utilizzato principalmente per modificare ed eseguire query, visualizzare i risultati e condividere il lavoro con il team. Con l'editor di query v2, è possibile creare database, schemi, tabelle e funzioni definite dall'utente (FDU). In un pannello con struttura ad albero, per ciascuno dei database, puoi visualizzarne gli schemi. Per ogni schema, è possibile visualizzare le tabelle, le viste, le FDU e le procedure archiviate.

### Argomenti

- [Apertura editor di query v2](#)
- [Connessione a un database Amazon Redshift](#)
- [Navigazione in un database Amazon Redshift](#)
- [Creazione di oggetti di database](#)
- [Visualizzazione della cronologia delle query e delle schede](#)
- [Considerazioni sull'utilizzo dell'editor di query v2](#)
- [Modifica delle impostazioni dell'account](#)

## Apertura editor di query v2

Scopri come aprire l'editor di query v2

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu navigator, selezionare Editor, quindi Editor di query v2. L'editor di query v2 viene aperto in una nuova scheda del browser.

Nella pagina dell'editor di query è disponibile un menu di navigazione in cui è possibile scegliere una vista nel modo descritto di seguito.

### Editor



Puoi gestire ed eseguire query sui dati organizzati come tabelle e contenuti in un database. Il database può contenere dati archiviati o un riferimento a dati archiviati altrove, ad esempio in Amazon S3. È possibile connettersi a un database contenuto in un cluster o in un gruppo di lavoro serverless.

Quando si lavora nella vista Editor, si dispone dei seguenti controlli:

- Il campo Cluster o Workgroup (Gruppo di lavoro) visualizza il nome dell'elemento a cui si è attualmente connessi. Il campo Database visualizza i database all'interno del cluster o del gruppo di lavoro. Le azioni che esegui nella vista Database agiscono per impostazione predefinita sul database selezionato.
- Una vista gerarchica ad albero dei cluster o dei gruppi di lavoro, dei database e degli schemi. In schemi, è possibile lavorare con tabelle, viste, funzioni e procedure archiviate. Ogni oggetto nella vista ad albero supporta un menu contestuale per eseguire azioni associate, ad esempio Aggiorna o Elimina, per l'oggetto.
- Un'operazione



Crea per creare database, schemi, tabelle e funzioni.

- Un'operazione



dati per caricare i dati da Amazon S3 o da un file locale nel database.

- Un'icona



Salva per salvare la query.

- Un'icona



Shortcuts per visualizzare le scorciatoie da tastiera per l'editor.

- Un'icona



Altro per visualizzare più operazioni nell'editor. Ad esempio:

- Condividi con il mio team per condividere la query o il notebook con il team. Per ulteriori informazioni, consulta [Collaborazione e condivisione come team](#).
  - Tasti di scelta rapida per visualizzare i tasti di scelta rapida per l'editor.
  - Cronologia delle schede per visualizzare la cronologia delle schede di una scheda nell'editor.
  - Aggiorna il completamento automatico per aggiornare i suggerimenti visualizzati durante la creazione di SQL.
- Un'area Editor



in cui è possibile inserire ed eseguire la query.

Dopo aver eseguito una query, viene visualizzata la scheda Risultato con i risultati. Qui puoi abilitare Grafico per visualizzare i risultati. Puoi anche esportare i risultati usando il comando Export (Esporta).

- Un'area



Notebook in cui è possibile aggiungere sezioni per inserire ed eseguire istruzioni SQL o aggiungere markdown.

Dopo aver eseguito una query, viene visualizzata la scheda Risultato con i risultati. È in questa area che è possibile esportare i risultati mediante il comando Export (Esporta).

## Query



Una query contiene i comandi SQL per gestire i dati contenuti in un database ed eseguirvi query. Quando utilizzi l'editor di query v2 per caricare i dati di esempio, vengono automaticamente create e salvate anche query di esempio.

Quando si sceglie una query salvata, è possibile aprirla, rinominarla ed eliminarla usando il menu contestuale (clic con il pulsante destro del mouse). È possibile visualizzare attributi come l'ARN della query di una query salvata scegliendo Dettagli della query. È anche possibile visualizzarne la cronologia delle versioni, modificare i tag collegati alla query e condividerla con il proprio team.

## Notebook



Un notebook SQL contiene celle SQL e Markdown. È possibile utilizzare i notebook per organizzare, annotare e condividere più query SQL in un singolo documento.

Quando si sceglie un notebook salvato, è possibile aprirlo, rinominarlo ed eliminarlo usando il menu contestuale (clic con il pulsante destro del mouse). È possibile visualizzare attributi come l'ARN del notebook di un notebook salvato scegliendo Dettagli del notebook. È anche possibile visualizzarne la cronologia delle versioni, modificare i tag collegati al notebook, esportarlo e condividerlo con il proprio team. Per ulteriori informazioni, consulta [Autorizzazione ed esecuzione di notebook](#).

## Grafici



Un grafico è una rappresentazione visiva dei dati. Nell'editor di query v2 sono disponibili gli strumenti per la creazione e il salvataggio di molti tipi di grafici.

Quando si sceglie un grafico salvato, è possibile aprirlo, rinominarlo ed eliminarlo usando il menu contestuale (clic con il pulsante destro del mouse). È possibile visualizzare attributi come l'ARN del grafico di un grafico salvato scegliendo Dettagli del grafico. È anche possibile modificare i tag collegati al grafico ed esportarlo. Per ulteriori informazioni, consulta [Visualizzazione dei risultati delle query](#).

## Cronologia



La cronologia di query è un elenco di query eseguite utilizzando l'editor di query v2 di Amazon Redshift. Queste query sono state eseguite come singole query o come parte di un notebook SQL. Per ulteriori informazioni, consulta [Visualizzazione della cronologia delle query e delle schede](#).

## Query pianificate



Una query pianificata è una query impostata per essere avviata in orari specifici.

Tutte le visualizzazioni dell'editor di query v2 includono le seguenti icone:

- L'icona



(Modalità visiva) per passare dal tema chiaro al tema scuro.

- L'icona



(Impostazioni) per mostrare un menu per accedere alle diverse schermate delle impostazioni.

- L'icona



(Preferenze dell'editor) per modificare le preferenze quando utilizzi l'editor di query v2. Qui puoi scegliere Modifica delle impostazioni dell'area di lavoro per modificare la dimensione del carattere, la dimensione delle schede e altre impostazioni di visualizzazione. Puoi anche attivare (o disattivare) il Completamento automatico per mostrare suggerimenti quando inserisci il codice SQL.

- L'icona



(Connessioni) per visualizzare le connessioni utilizzate dalle schede dell'editor.

Per recuperare dati da un database, viene utilizzata una connessione. Viene creata una connessione per un database specifico. Con una connessione isolata, i risultati di un comando SQL che modifica il database in una scheda dell'editor, ad esempio la creazione di una tabella temporanea, non sono visibili in un'altra scheda dell'editor. Quando si apre una scheda nell'editor di query v2, l'impostazione predefinita è una connessione isolata. Quando si crea una connessione condivisa, ovvero si disattiva il parametro `Isolated session` (Sessione isolata), i risultati di altre connessioni condivise allo stesso database sono visibili tra loro. Tuttavia, le schede dell'editor che utilizzano una connessione condivisa a un database non vengono eseguite in parallelo. Le query che utilizzano la stessa connessione devono attendere che la connessione torni disponibile. Una connessione a un database non può essere condivisa con un altro database e pertanto i risultati SQL non sono visibili tra le varie connessioni.

Il numero di connessioni attive che qualsiasi utente nell'account può avere è gestito da un amministratore dell'editor di query v2.

- L'icona



(Impostazioni account) utilizzata da un amministratore per modificare alcune impostazioni di tutti gli utenti nell'account. Per ulteriori informazioni, consulta [Modifica delle impostazioni dell'account](#).

## Connessione a un database Amazon Redshift

Per connetterti a un database, scegli il nome del cluster o del gruppo di lavoro nel pannello con struttura ad albero. Se richiesto, immettere i parametri di connessione.

Quando ti connetti a un cluster o a un gruppo di lavoro e ai relativi database, di solito fornisci un nome per il database. È inoltre possibile fornire i parametri necessari per uno dei seguenti metodi di autenticazione:

### IAM Identity Center

Con questo metodo, esegui la connessione al data warehouse Amazon Redshift con le credenziali dell'autenticazione unica del tuo gestore dell'identità digitale. Il cluster o il gruppo di lavoro deve essere abilitato per il Centro identità IAM nella console Amazon Redshift. Per assistenza nella configurazione delle connessioni a IAM Identity Center, consulta [Connessione di Redshift al Centro identità IAM per offrire agli utenti un'esperienza di autenticazione unica](#).

## Utente federato

Con questo metodo, i tag dei principali dell'utente o del ruolo IAM devono fornire i dettagli di connessione. Questi tag vengono configurati nel AWS Identity and Access Management nostro provider di identità (IdP). L'editor di query v2 si basa sui seguenti tag:

- `RedshiftDbUser`: questo tag definisce l'utente del database utilizzato dall'editor di query v2. Questo tag è obbligatorio.
- `RedshiftDbGroups`: questo tag definisce i gruppi di database che vengono uniti durante la connessione all'editor di query v2. Questo tag è facoltativo e il suo valore deve essere un elenco separato da due punti, ad esempio `group1:group2:group3`. I valori vuoti vengono ignorati, ossia, `group1:::group2` è interpretato come `group1:group2`.

Questi tag vengono inoltrati all'API `redshift:GetClusterCredentials` per ottenere le credenziali per il tuo cluster. Per ulteriori informazioni, consulta [Configurazione dei tag principali per la connessione a un cluster o un gruppo di lavoro dall'editor di query v2](#).

### Credenziali temporanee con un nome utente del database

Questa opzione è disponibile solo quando ci si connette a un cluster. Con questo metodo, l'editor di query v2 fornisce un nome utente per il database. L'editor di query v2 genera una password temporanea per la connessione al database con il tuo nome utente del database. Un utente che utilizza questo metodo per connettersi deve avere l'autorizzazione IAM per `redshift:GetClusterCredentials`. Per impedire agli utenti di utilizzare questo metodo, modifica il loro utente o ruolo IAM per negare questa autorizzazione.

### Credenziali temporanee che utilizzano la tua identità IAM

Questa opzione è disponibile solo quando ci si connette a un cluster. Con questo metodo, l'editor di query v2 mappa un nome utente alla tua identità IAM e genera una password temporanea per la connessione al database con la tua identità IAM. Un utente che utilizza questo metodo per connettersi deve avere l'autorizzazione IAM per `redshift:GetClusterCredentialsWithIAM`. Per impedire agli utenti di utilizzare questo metodo, modifica il loro utente o ruolo IAM per negare questa autorizzazione.

### Nome utente e password del database

Con questo metodo, fornire anche un Nome utente e una Password per il database a cui ti stai connettendo. L'editor di query v2 crea un segreto per tuo conto archiviato in AWS Secrets Manager. Questo segreto contiene le credenziali per la connessione al database.

## AWS Secrets Manager

Con questo metodo, anziché un nome di database fornisci un Secret (Segreto) archiviato in Gestione dei segreti che contiene il tuo database e le credenziali di accesso. Per informazioni sulla creazione di un segreto, [Creazione di un segreto per le credenziali di connessione al database](#) consulta.

Quando selezioni un cluster o un gruppo di lavoro con l'editor di query v2, a seconda del contesto, puoi creare, modificare ed eliminare connessioni utilizzando il menu contestuale (clic con il pulsante destro del mouse). È possibile visualizzare attributi come l'ARN di connessione della connessione scegliendo Dettagli connessione. È anche possibile modificare i tag collegati alla connessione.

## Navigazione in un database Amazon Redshift

All'interno di un database è possibile gestire schemi, tabelle, viste, funzioni e procedure archiviate nel pannello di visualizzazione ad albero. Ad ogni oggetto nella visualizzazione vengono associate operazioni in un menu contestuale (clic con il pulsante destro del mouse).

Il pannello gerarchico con visualizzazione ad albero mostra gli oggetti del database. Per aggiornare il pannello della visualizzazione ad albero per visualizzare gli oggetti del database che potrebbero essere stati creati dopo l'ultima visualizzazione della visualizzazione ad albero, scegli l'icona



Aprire il menu contestuale (clic con il pulsante destro del mouse) di un oggetto per vedere quali operazioni è possibile eseguire.

- ▼  **redshift-cluster-tickit**
  - ▼  dev
    - ▼  public
      - ▼  Tables 11
        -  accommodations
        -  category
        -  customer\_activity
        -  date
        -  event
        -  listing
        -  sales
        -  sales2
        -  users
        -  venue
        -  zipcode
      - ▼  Views 1
        -  myevent
      - ▼  Functions 2
        - fx* f\_py\_greater(float8,float8)
        - fx* f\_sql\_greater(float8,float8)
      - ▼  Stored procedures 1
        - fx* test\_sp1(int4,varchar)
      - >  testschema
      - >  testschema2
    - ▼  sample\_data\_dev
      - ▼  tickit 
        - >  Tables 7
        - >  Views 0
        - >  Functions 0
        - >  Stored procedures 0
- >  tpcds 
- >  testdb

Dopo aver scelto una tabella, puoi procedere come segue:

- Per avviare una query nell'editor con un'istruzione SELECT che esegue query su tutte le colonne della tabella, utilizzare Seleziona tabella.
- Per visualizzare gli attributi o una tabella, utilizzare Visualizza definizione della tabella. Utilizzare questa opzione per visualizzare i nomi delle colonne, i tipi di colonna, la codifica, le chiavi di distribuzione, le chiavi di ordinamento e se una colonna può contenere valori nulli. Per ulteriori informazioni sugli attributi della tabella, consultare [CREA TABELLA](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Per eliminare una tabella, utilizzare Elimina. È possibile utilizzare Troncare tabella per eliminare tutte le righe dalla tabella o Elimina tabella per rimuovere la tabella dal database. Per ulteriori informazioni, consultare [TRONCARE](#) e [ELIMINA TABELLA](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Scegliere uno schema per Aggiorna o Elimina schema.

Scegliere una vista per Mostra la definizione della vista o Elimina vista.

Scegliere una funzione per Mostra definizione della funzione o Elimina funzione.

Scegli una procedura archiviata per Mostra definizione della procedura o Elimina procedura.

## Creazione di oggetti di database

È possibile creare oggetti di database, inclusi database, schemi, tabelle e funzioni definite dall'utente (FDU). Per creare oggetti di database, è necessaria la connessione a un cluster o a un gruppo di lavoro e a un database.

### Creazione di database

Puoi usare l'editor di query v2 per creare database nel tuo cluster o gruppo di lavoro.

Per creare un database:

Per informazioni sui database [CREA DATABASE](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## 1. Scegliere



Crea,

quindi scegliere Database.

## 2. Inserire un Nome database.

## 3. (Facoltativo) Seleziona Utenti e gruppi e scegli un Utente del database.

## 4. (Facoltativo) È possibile creare il database da una unità di condivisione dati o da AWS Glue Data Catalog. Per ulteriori informazioni su AWS Glue, vedi [Cos'è AWS Glue?](#) nella Guida per gli AWS Glue sviluppatori.

- (Facoltativo) Seleziona Crea utilizzando una unità di condivisione dati e scegli Seleziona una unità di condivisione dati. L'elenco include le unità di condivisione dati che possono essere utilizzate per creare un'unità di condivisione dati consumer nel cluster o nel gruppo di lavoro corrente.
- (Facoltativo) Selezionate Crea utilizzando AWS Glue Data Catalog e scegliete un database Choose an AWS Glue. In Schema del catalogo dati, inserisci il nome che verrà utilizzato per lo schema quando si fa riferimento ai dati in un nome composto da tre parti (database.schema.table).

## 5. Scegliere Crea database.

Il nuovo database viene visualizzato nel pannello con visualizzazione ad albero.

Quando scegli la procedura facoltativa per eseguire una query su un database creato da una unità di condivisione dati, connessi a un database Amazon Redshift nel cluster o nel gruppo di lavoro (ad esempio, il database predefinito dev) e usa una notazione in tre parti (database.schema.table) che fa riferimento al nome del database che hai creato quando hai selezionato Crea utilizzando un'unità di condivisione dati. Il database di unità di condivisione dati è elencato nella scheda editor dell'editor di query v2, ma non è abilitato per la connessione diretta.

Quando scegli il passaggio opzionale per interrogare un database creato da un AWS Glue Data Catalog, connessi al tuo database Amazon Redshift nel cluster o nel gruppo di lavoro (ad esempio, il database predefinito **dev**) e usa una notazione in tre parti (database.schema.table) che fa riferimento al nome del database creato quando hai selezionato Crea utilizzando AWS Glue Data Catalog, allo schema che hai nominato nello schema del catalogo dati e alla tabella in. AWS Glue Data Catalog Simile a:

```
SELECT * FROM glue-database.glue-schema.glue-table
```

### Note

Conferma di essere connesso al database predefinito utilizzando il metodo di connessione Credenziali temporanee che utilizzano la tua identità IAM e che alle tue credenziali IAM sia stato concesso il privilegio di utilizzo per il AWS Glue database.

```
GRANT USAGE ON DATABASE glue-database to "IAM:MyIAMUser"
```

Il AWS Glue database è elencato nella scheda dell'editor di query v2, ma non è abilitato per la connessione diretta.

Per ulteriori informazioni sull'interrogazione di un AWS Glue Data Catalog, consulta [Lavorare con le condivisioni di dati gestite da Lake Formation come consumatore](#) e [Lavorare con le condivisioni di dati gestite da Lake Formation come produttore nella Amazon Redshift Database Developer Guide](#).

## Esempio di creazione di un database come utente di unità di condivisione dati

L'esempio seguente descrive uno scenario specifico utilizzato per creare un database da un'unità di condivisione dati utilizzando l'editor di query v2. Esamina questo scenario per scoprire come creare un database da un'unità di condivisione dati nel tuo ambiente. Questo scenario utilizza due cluster, `cluster-base` (il cluster produttori) e `cluster-view` (il cluster di consumatori).

1. Usa la console Amazon Redshift per creare una condivisione di dati per la tabella `category2` nel cluster `cluster-base`. L'unità di condivisione dati del produttore è denominata `datashare_base`.

Per ulteriori informazioni sulla creazione di unità di condivisione dati, consultare [Condivisione dei dati tra cluster in Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

2. Usa la console Amazon Redshift per creare un'unità di condivisione dati `datashare_base` come consumatore per la tabella `category2` nel cluster `cluster-view`.

3. Visualizza il pannello di visualizzazione ad albero nell'editor di query v2 che mostra la gerarchia di `cluster-base` come:
  - Cluster: `cluster-base`
    - Database: `dev`
      - Schema: `public`
        - Tabelle: `category2`

4. Scegliere



Crea,

quindi scegliere Database.

5. Per Nome database, immettere `see_datashare_base`.
6. Seleziona Crea utilizzando una unità di condivisione dati e scegli Seleziona una unità di condivisione dati. Scegli `datashare_base` da utilizzare come origine del database che stai creando.

Il pannello di visualizzazione ad albero nell'editor di query v2 mostra la gerarchia di `cluster-view` come:

- Cluster: `cluster-view`
    - Database: `see_datashare_base`
      - Schema: `public`
        - Tabelle: `category2`
7. Quando esegui una query sui dati, connessi al database predefinito del cluster `cluster-view` (tipicamente denominato `dev`), ma fai riferimento al database di unità di condivisione dati `see_datashare_base` nel tuo SQL.

#### Note

Nella vista dell'editor di query v2, il cluster selezionato è `cluster-view`. Il database selezionato è `dev`. Il database `see_datashare_base` è elencato ma non è abilitato per la connessione diretta. Tu scegli il database `dev` e i riferimenti `see_datashare_base` nel codice SQL che esegui.

```
SELECT * FROM "see_datashare_base"."public"."category2";
```

La query recupera i dati dall'unità di condivisione dati `datashare_base` nel cluster `cluster_base`.

## Esempio di creazione di un database da un AWS Glue Data Catalog

L'esempio seguente descrive uno scenario specifico utilizzato per creare un database da un editor di query AWS Glue Data Catalog using v2. Esamina questo scenario per scoprire come creare un database da un ambiente AWS Glue Data Catalog in uso. Questo scenario utilizza un cluster, `cluster-view` per contenere il database che crei.

1. Scegliere



quindi scegliere Database.

Crea,

2. Per Nome database, immettere `data_catalog_database`.
3. Seleziona Crea usando un AWS Glue Data Catalog e scegli Scegli un AWS Glue database. Scegli `glue_db` da utilizzare come origine del database che stai creando.

Scegli Schema del catalogo dati e inserisci `myschema` come nome dello schema da utilizzare nella notazione in tre parti.

Il pannello di visualizzazione ad albero nell'editor di query v2 mostra la gerarchia di `cluster-view` come:

- Cluster: `cluster-view`
    - Database: `data_catalog_database`
      - Schema: `myschema`
        - Tabelle: `category3`
4. Quando esegui una query sui dati, connettiti al database predefinito del cluster `cluster-view` (tipicamente denominato `dev`), ma fai riferimento al database `data_catalog_database` nel tuo SQL.

**Note**

Nella vista dell'editor di query v2, il cluster selezionato è `cluster-view`. Il database selezionato è `dev`. Il database `data_catalog_database` è elencato ma non è abilitato per la connessione diretta. Tu scegli il database `dev` e i riferimenti `data_catalog_database` nel codice SQL che esegui.

```
SELECT * FROM "data_catalog_database"."myschema"."category3";
```

L'interrogazione recupera i dati catalogati da AWS Glue Data Catalog.

## Creazione di schemi

Puoi usare l'editor di query v2 per creare schemi nel tuo cluster o gruppo di lavoro.

Per creare uno schema

Per informazioni sugli schemi, consultare [Schemi](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

### 1. Scegliere



quindi scegliere Schema.

### 2. Inserire un Nome schema.

### 3. Scegliere Local (Locale) o External (Esterno) in Schema type (Tipo di schema).

Per ulteriori informazioni sugli schemi locali, consultare [CREATE SCHEMA](#) nella Guida per gli sviluppatori di database di Amazon Redshift. Per ulteriori informazioni sugli schemi esterni, consultare [CREATE EXTERNAL SCHEMA](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

### 4. Se si sceglie External (Esterno), per lo schema esterno sono disponibili le seguenti opzioni.

- Glue Data Catalog (Catalogo dati di Glue): per creare uno schema esterno in Amazon Redshift che faccia riferimento alle tabelle in AWS Glue. Oltre a scegliere il AWS Glue database, scegli il ruolo IAM associato al cluster e il ruolo IAM associato al Data Catalog.

Crea,

- PostgreSQL: per creare uno schema esterno in Amazon Redshift riferito a un database Amazon RDS per PostgreSQL o a un database compatibile con Amazon Aurora PostgreSQL. Specificare inoltre le informazioni sulla connessione al database. Per ulteriori informazioni sulle query federate, consultare [Esecuzione di query su dati con query federate](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- MySQL: per creare uno schema esterno in Amazon Redshift riferito a un database Amazon RDS per MySQL o a un database compatibile con Amazon Aurora MySQL. Specificare inoltre le informazioni sulla connessione al database. Per ulteriori informazioni sulle query federate, consultare [Esecuzione di query su dati con query federate](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## 5. Scegliere Crea schema.

Il nuovo schema viene visualizzato nel pannello con visualizzazione ad albero.

### Creazione di tabelle

Puoi usare l'editor di query v2 per creare tabelle nel tuo cluster o gruppo di lavoro.

#### Per creare una tabella

È possibile creare una tabella basata su un file CSV (valori separati da virgole) in cui è possibile specificare o definire ogni colonna della tabella. Per informazioni sulle tabelle, consultare [Progettazione tabelle](#) e [CREA TABELLA](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Scegliere Apri query nell'editor per visualizzare e modificare l'istruzione CREA TABELLA prima di eseguire la query per creare la tabella.

#### 1. Scegli



(Crea) e quindi Table (Tabella).

#### 2. Scegliere uno schema.

#### 3. Inserire un nome tabella.

#### 4. Scegliere



Aggiungi campo per aggiungere una colonna.

Create

5. Utilizzare un file CSV come modello per la definizione della tabella:

- a. Scegliere Carica da CSV.
- b. Seleziona la posizione del file.

Se si utilizza un file CSV, assicurarsi che la prima riga del file contenga le intestazioni di colonna.

- c. Scegli il file e scegli Apri. Confermare che i nomi delle colonne e i tipi di dati corrispondano a quanto voluto.

6. Per ogni colonna, scegli la colonna e scegli le opzioni desiderate:

- Scegliere un valore per Codifica.
- Scegliere un Valore predefinito.
- Attivare Incremento automatico se si desidera che i valori delle colonne vengano incrementati. Quindi specificare un valore per Auto-incremento del seed e Fase di incremento automatico.
- Attivare Non NULL se la colonna deve sempre contenere un valore.
- Inserire un valore Dimensione per la colonna.
- Attivare Chiave primaria se si desidera che la colonna sia una chiave primaria.
- Attivare Chiave unica se si desidera che la colonna sia una chiave unica.

7. (Facoltativo) Scegliere Dettagli tabella e scegliere una qualsiasi delle seguenti opzioni:

- Colonna e stile della chiave di distribuzione.
- Colonna chiave di ordinamento e tipo di ordinamento.
- Attiva Backup per includere la tabella negli snapshot.
- Attivare Tabella temporanea per creare la tabella come tabella temporanea.

8. Scegliere Apri query nell'editor per continuare a specificare le opzioni per definire la tabella o scegliere Crea tabella per creare la tabella.

## Creazione di funzioni

Puoi usare l'editor di query v2 per creare funzioni nel tuo cluster o gruppo di lavoro.

## Per creare una funzione

1. Scegliere



e scegliere Funzione.

2. Per Tipo, scegliere SQL o Python.
3. Scegliere un valore per Schema.
4. Inserire un valore Nome per la funzione.
5. Inserire un valore Volatilità per la funzione.
6. Scegliere i Parametri in base ai loro tipi di dati nell'ordine dei parametri di input.
7. Per Valori restituiti, scegliere un tipo di dati.
8. Inserisci il codice Programma SQL o Programma Python per la funzione.
9. Scegli Crea.

Crea

Per ulteriori informazioni sulle funzioni definite dall'utente (UDF), consultare [Creazione di funzioni definite dall'utente](#) nella Guida per sviluppatori di database di Amazon Redshift.

## Visualizzazione della cronologia delle query e delle schede

Puoi visualizzare la cronologia delle query con l'editor di query v2. Nella cronologia delle query vengono visualizzate solo le query eseguite utilizzando l'editor di query v2. Vengono visualizzate entrambe le query eseguite utilizzando una scheda Editor o una scheda Notebook. È possibile filtrare l'elenco visualizzato in base a un periodo di tempo, ad esempio `This week`, in cui una settimana è definita come lunedì-domenica. L'elenco delle query recupera contemporaneamente 25 righe di query che corrispondono al filtro in uso. Scegli `Load more` (Carica altro) per vedere il set successivo. Scegli una query e dal menu `Actions` (Operazioni). Le operazioni disponibili dipendono dal fatto se la query selezionata è stata salvata o meno. È possibile effettuare le seguenti operazioni:

- `View query details` (Visualizza dettagli della query): visualizza una pagina dei dettagli della query con ulteriori informazioni sulla query eseguita.
- `Open query in a new tab` (Apri query in una nuova scheda): apre una nuova scheda dell'editor e la prepara con la query scelta. Se ancora connessi, il cluster o il gruppo di lavoro e il database vengono selezionati automaticamente. Per eseguire la query, verifica innanzitutto che siano stati scelti il cluster o il gruppo di lavoro e il database corretti.

- Open source tab (Apri scheda origine): se è ancora aperta, passa alla scheda dell'editor o del notebook che conteneva la query quando è stata eseguita. Il contenuto dell'editor o del notebook potrebbe essere cambiato dopo l'esecuzione della query.
- Open saved query (Apri la query salvata): passa alla scheda dell'editor o del notebook e apre la query.

È inoltre possibile visualizzare la cronologia delle query eseguite in una scheda Editor o la cronologia delle query eseguite in una scheda Notebook. Per visualizzare la cronologia delle query in una scheda, scegliere Tab history (Cronologia scheda). Nella cronologia della scheda, puoi effettuare le operazioni elencate di seguito:

- Copy query (Copia query): copia il contenuto SQL della versione della query negli appunti.
- Open query in a new tab (Apri query in una nuova scheda): apre una nuova scheda dell'editor e la prepara con la query scelta. Per eseguire la query, è necessario scegliere il cluster o il gruppo di lavoro e il database.
- View query details (Visualizza dettagli della query): visualizza una pagina dei dettagli della query con ulteriori informazioni sulla query eseguita.

## Considerazioni sull'utilizzo dell'editor di query v2

Considera quanto segue quando utilizzi l'editor di query v2.

- La dimensione massima del risultato della query è la più piccola di 5 MB o 100.000 righe.
- È possibile eseguire una query contenente fino a 300 mila caratteri.
- È possibile salvare una query contenente fino a 30 mila caratteri.
- Per impostazione predefinita, l'editor di query v2 esegue automaticamente il commit di ogni singolo comando SQL eseguito. Quando viene fornita un'istruzione BEGIN, le istruzioni all'interno del blocco BEGIN-COMMIT o BEGIN-ROLLBACK vengono eseguite come una singola transazione. Per ulteriori informazioni sulle transazioni, consultare [BEGIN](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Il numero massimo di avvisi che l'editor di query v2 visualizza durante l'esecuzione di un'istruzione SQL è 10. Ad esempio, quando viene eseguita una stored procedure, non vengono visualizzate più di 10 istruzioni RAISE.
- L'editor di query v2 non supporta un IAM RoleSessionName che contiene virgole (,). Potresti visualizzare un errore simile al seguente: Messaggio di errore:

«'AROA123456789Example:myText, yourtext' non è un valore valido per TagValue - contiene caratteri non validi» Questo problema si verifica quando si definisce un IAM che include una virgola e quindi si utilizza l'editor di query v2 con quel ruolo IAM. RoleSessionName

[Per ulteriori informazioni su un IAM, consulta l'attributo SAML nella Guida per l'utente di IAM.](#)  
[RoleSessionName RoleSessionName](#)

## Modifica delle impostazioni dell'account

Un utente con le autorizzazioni IAM adeguate può visualizzare e modificare le opzioni selezionate in Account settings (Impostazioni account) per gli altri utenti nello stesso Account AWS.

L'amministratore può visualizzare o impostare quanto segue:

- Il numero massimo di connessioni simultanee al database per utente nell'account. Sono incluse le connessioni per le sessioni isolate. Quando si modifica questo valore, possono essere necessari 10 minuti per rendere effettiva la modifica.
- La possibilità da parte degli utenti nell'account di esportare un intero set di risultati da un comando SQL a un file.
- La possibilità di caricare e visualizzare i database di esempio con alcune query salvate associate.
- Specifica un percorso Amazon S3 utilizzato dagli utenti dell'account per caricare i dati da un file locale.
- La possibilità di visualizzare l'ARN della chiave KMS per crittografare le risorse dell'editor di query v2.

## Interazione con SQL generativo dell'editor di query v2 (anteprima)

Questa è una documentazione di pre-rilascio per SQL generativo dell'editor di query v2, che è in versione di anteprima. La documentazione e la funzionalità sono soggette a modifiche. Consigliamo di utilizzare questa caratteristica solo in ambienti di test e non in ambienti di produzione. Per i termini e le condizioni di anteprima, vedere Partecipazione al servizio beta in [Termini del servizio AWS](#).

### Note

Attualmente, il supporto SQL generativo è disponibile solo nei seguenti casi: Regioni AWS

- Regione Stati Uniti orientali (Virginia settentrionale) (us-east-1)
- Regione Stati Uniti occidentali (Oregon) (us-west-2)
- Regione Europa (Francoforte) (eu-central-1)

Puoi interagire con la funzionalità SQL generativo di Amazon Q nell'Editor di query Amazon Redshift v2. Si tratta di un assistente di codifica che genera istruzioni SQL in base alle istruzioni e allo schema del database, disponibile per la creazione di un notebook nell'editor di query v2.

Quando interagisci con SQL generativo, poni domande specifiche, applica l'iterazione in caso di richieste complesse e verifica l'accuratezza delle risposte.

Quando fornisci richieste di analisi in linguaggio naturale, sii il più specifico possibile per aiutare l'assistente di codifica a capire esattamente di cosa hai bisogno. Invece di chiedere "trova le sedi principali che hanno venduto il maggior numero di biglietti", fornisci maggiori dettagli, ad esempio "trova i nomi/gli ID delle tre sedi che hanno venduto il maggior numero di biglietti nel 2008". Utilizza nomi coerenti per gli oggetti nel database, ad esempio i nomi di schema, tabella e colonna definiti nel database, invece di fare riferimento allo stesso oggetto in modi diversi, che può confondere l'assistente.

Suddividi le richieste complesse in più istruzioni semplici che sono più facili da interpretare per l'assistente. Poni domande di follow-up in modo iterativo per ottenere un'analisi più dettagliata dall'assistente. Ad esempio, per prima cosa chiedi in quale stato ci sono più sedi. Quindi, in base alla risposta, chiedi qual è la sede più popolare di questo stato.

Esamina l'SQL generato prima di eseguirlo per verificarne l'accuratezza. Se la query SQL generata contiene errori o non corrisponde al tuo intento, fornisci all'assistente le istruzioni per correggerla invece di riformulare l'intera richiesta. Ad esempio, se nella query manca una clausola di predicato relativa all'anno, chiedi di fornire le sedi a partire dal 2008.

## Considerazioni sull'interazione con SQL generativo

Considera le seguenti indicazioni quando utilizzi il pannello di chat.

- L'amministratore dell'editor di query v2 del tuo account deve aver attivato la funzionalità di chat nella pagina Impostazioni di SQL generativo.
- Per utilizzare l'SQL generativo di query editor v2, è necessaria l'autorizzazione `sqlworkbench:GetQSqlRecommendations` nella policy IAM, oltre alle altre autorizzazioni

specificate nella policy AWS gestita per l'editor di query v2. Per ulteriori informazioni sulle politiche AWS gestite, consulta [Accesso all'editor di query v2](#)

- Le domande devono essere scritte in inglese.
- Le domande devono fare riferimento al database connesso nel cluster o nel gruppo di lavoro. Per evitare errori di stato vuoto, nel database devono essere presenti almeno una tabella e alcuni dati.
- Le domande devono riferirsi ai dati archiviati nel database connesso. Non è possibile fare riferimento a uno schema esterno. Per ulteriori informazioni sugli schemi supportati, consulta [Create schema](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Qualsiasi domanda che restituisca un codice SQL che modifichi il database connesso può generare un avviso.
- La tecnologia di IA generativa è nuova e nelle risposte possono esserci errori, a volte chiamati allucinazioni. Testa e rivedi tutto il codice per individuare errori e vulnerabilità prima di utilizzarlo nell'ambiente o nel carico di lavoro.
- Puoi migliorare i suggerimenti condividendo nel tuo account le query SQL eseguite da altri utenti. L'amministratore dell'account può eseguire i seguenti comandi SQL per consentire l'accesso alla cronologia delle query dell'account.

```
GRANT ROLE SYS:MONITOR to "IAMR:role-name";  
GRANT ROLE SYS:MONITOR to "IAM:user-name";  
GRANT ROLE SYS:MONITOR to "database-username";
```

Per ulteriori informazioni su SYS:MONITOR, consulta [Ruoli definiti dal sistema di Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- I tuoi dati sono sicuri e privati. I tuoi dati non vengono condivisi tra account. Le query, i dati e gli schemi di database non vengono utilizzati per addestrare un modello di fondazione (FM) di IA generativa. L'input viene utilizzato come prompt contestuale nel modello di fondazione solo per rispondere alle tue query.

## Utilizzo di SQL generativo

Dopo aver configurato le autorizzazioni corrette, quando si lavora con un notebook nell'editor di query v2, è possibile scegliere un'icona per iniziare una conversazione.

Per interagire con la chat di SQL generativo dell'editor di query v2 per generare istruzioni SQL

1. Apri un notebook nella scheda Editor dell'editor di query v2.

## 2. Scegli l'icona SQL generativo



quindi segui le istruzioni per porre le tue domande di SQL generativo dell'Editor di query Amazon Redshift v2 nel pannello di chat.

Inserisci le domande in un campo di prompt e l'editor di query v2 risponde con l'istruzione SQL suggerita. Eventuali errori riscontrati vengono restituiti nel pannello di chat.

## 3. Scegli Aggiungi al notebook per aggiungere una cella markdown con il prompt e una cella SQL con l'istruzione SQL suggerita al notebook.

## 4. (Facoltativo) Scegli Rigenera SQL per generare un'altra risposta per lo stesso prompt. È possibile scegliere Rigenera SQL una sola volta per il prompt corrente.

## 5. (Facoltativo) Nel pannello di chat di SQL generativo, scegli l'icona Altro



quindi seleziona Aggiorna database per aggiornare i metadati che descrivono il database connesso. Questi metadati includono le definizioni di schemi, tabelle e colonne del database.

## Aggiornamento delle impostazioni di SQL generativo come amministratore

Un utente con le autorizzazioni IAM adeguate può visualizzare e modificare le impostazioni di SQL generativo per gli altri utenti nello stesso Account AWS. Questo amministratore deve disporre dell'autorizzazione `sqlworkbench:UpdateAccountQSQLSettings` nella propria politica IAM, oltre alle altre autorizzazioni specificate nella policy AWS gestita per l'editor di query v2. Per ulteriori informazioni sulle policy gestite, consulta [Autorizzazioni necessarie per utilizzare l'editor della query v2](#).

Per consentire a un amministratore di attivare la chat SQL generativo per tutti gli utenti dell'account

## 1. Scegli l'icona Impostazioni



per visualizzare un menu per accedere alle diverse schermate delle impostazioni.

## 2. Quindi scegli l'icona Impostazioni SQL generativo



per visualizzare la pagina Impostazioni SQL generativo.

## 3. Seleziona SQL generativo per attivare la funzionalità SQL generativo per gli utenti dell'account.

## Esempio di utilizzo della funzionalità SQL generativo di Amazon Q con i dati TICKIT

Per creare prompt efficienti che generano istruzioni SQL, devi conoscere lo schema del database e i tuoi dati. I dati TICKIT sono composti da sette tabelle: due tabelle di fatti e cinque di dimensioni. I dati di esempio contengono i record sulle vendite ai partecipanti di eventi di intrattenimento che si sono svolti nel 2008. Per ulteriori informazioni sullo schema di dati TICKIT, consulta [Database di esempio](#) nella Guida per gli sviluppatori di database di Amazon Redshift. Puoi caricare i dati TICKIT in un database tramite vari metodi sia nella console Amazon Redshift che nell'editor di query v2. L'editor di query v2 fornisce un metodo per caricare i dati TICKIT nel database `sample_data_dev`. Per informazioni, consulta [Caricamento di dati di esempio](#). L'editor di query v2 fornisce anche prompt di esempio per i dati TICKIT. Lo scenario seguente descrive una conversazione con SQL generativo per generare istruzioni SQL sui dati di esempio TICKIT. In questo scenario, i dati di esempio TICKIT sono già creati in un database dev di un cluster Amazon Redshift.

### Note

L'esempio illustra una conversazione. Le risposte di SQL generativo potrebbero non corrispondere ai tuoi risultati utilizzando gli stessi prompt.

## Esempio di conversazione con SQL generativo dell'editor di query v2

1. Nell'editor connettiti a un cluster o gruppo di lavoro che contiene i dati di esempio TICKIT.
2. Crea un notebook vuoto e scegli l'icona SQL generativo  per aprire il pannello di chat.
3. Inserisci il seguente prompt per generare un'istruzione SQL per verificare il numero di record nella tabella VENUE:

```
How many venues are there?
```

```
SELECT
  COUNT(*) AS num_venues
FROM
  tickit.venue
```

Scegli Aggiungi al notebook per aggiungere due celle al notebook aperto. Una cella markdown "How many venues are there?" e una contenente l'istruzione SQL generata.

Nella cella SQL, scegli Esegui per ottenere il risultato:

```
count
-----
202
```

4. Per richiedere un'altra versione di SQL, scegli Rigenera SQL e ottieni la seguente risposta:

```
SELECT
  venuestate,
  COUNT(*) AS num_venues
FROM
  tickit.venue
GROUP BY
  venuestate
```

Scegli Aggiungi al notebook per aggiungere altre due celle al notebook aperto. Una cella markdown "How many venues are there?" e una contenente l'istruzione SQL generata.

Nella cella SQL, scegli Esegui per ottenere il risultato che elenca lo stato dei locali per numero:

```
venuestate num_venues
-----
MA          4
OH          8
MI          5
...
```

5. L'assistente SQL generativo può formulare ipotesi su ciò che stai chiedendo. Sebbene non ci siano widget nel database, puoi comunque chiederli. In questo caso, ti restituisce un messaggio indicante che non è stato in grado di generare un'istruzione SQL.

How many widgets are there?

```
I was not able to generate any SQL
```

6. Man mano che acquisisci ulteriori informazioni sul tuo database, puoi porre domande più specifiche per generare le istruzioni SQL. Ad esempio, sai che il database contiene i dati sulle vendite relativi a diversi mesi del 2008. Inserisci il seguente prompt per generare un'istruzione SQL per trovare il numero di vendite nel novembre 2008:

```
How many sales were there in November 2008?
```

```
SELECT
  COUNT(*) AS num_sales
FROM
  tickit.sales s
  JOIN tickit.date d ON s.dateid = d.dateid
WHERE
  d.month = 'November'
  AND d.year = 2008
```

Scegli **Aggiungi al notebook** per aggiungere due celle al notebook aperto. Una cella markdown "How many sales were there in November 2008?" e una contenente l'istruzione SQL generata.

Nella cella SQL, scegli **Esegui** per ottenere il risultato:

```
num_sales
-----
0
```

Tuttavia questo non è il risultato che ti aspettavi.

7. Noti che il predicato `date.month='November'` prevede che il mese nella tabella DATE sia rappresentato da un'abbreviazione del nome del mese. Modifichi il predicato in `d.month='NOV'` ed esegui nuovamente l'istruzione SQL.

```
SELECT
  COUNT(*)
FROM
  sales
  JOIN date ON sales.dateid = date.dateid
WHERE
  date.month = 'NOV'
```

```
AND date.year = 2008
```

Nella cella SQL, scegli Esegui per ottenere nuovi risultati.

```
count
-----
14261
```

8. Se fai una domanda che tenta di modificare il database connesso, viene visualizzato un messaggio di avviso insieme alle istruzioni SQL suggerite. Immetti il seguente prompt per generare un'istruzione SQL per inserire i dati in una tabella:

```
Insert 1 into the venue table.
```

```
INSERT
,
UPDATE
  OR delete data
FROM
  the database AS that could potentially change the data.Please provide a query
  that ONLY selects data
```

```
I was not able to generate the correct SQL code. I generated SQL, but you'll have
to edit it to work with your database.
```

Se scegli Aggiungi al notebook per aggiungere due celle al notebook aperto ed esegui l'istruzione SQL, viene restituito l'esito negativo dell'istruzione SQL.

```
ERROR: syntax error at or near "," Position: 132 [ErrorId:
1-6546764a-011df2691778846219ce6ec2]
```

Questo scenario ha illustrato solo alcuni modi di base per interagire con SQL generativo dell'editor di query v2. Puoi continuare a sperimentare questa tecnologia di IA generativa per iniziare a creare istruzioni SQL per eseguire le query sul tuo database.

## Caricamento dei dati in un database

Puoi utilizzare l'editor di query v2 per caricare i dati in un database in un cluster o un gruppo di lavoro di Amazon Redshift.

### Caricamento di dati di esempio

L'editor di query v2 viene fornito con dati e notebook di esempio che possono essere caricati in un database di esempio e nello schema corrispondente.

Per caricare i dati di esempio, scegliere l'icona



associata ai dati di esempio che si desidera caricare. L'editor di query v2 carica quindi i dati in uno schema nel database `sample_data_dev` e crea una cartella di notebook salvati nella cartella Notebook.

Sono disponibili i seguenti set di dati di esempio.

#### tickit

Nella maggior parte degli esempi della documentazione di Amazon Redshift viene utilizzato un set di dati di esempio denominato `tickit`. Questi dati sono composti da sette tabelle: due tabelle di fatti e cinque di dimensioni. Quando si caricano questi dati, lo schema `tickit` viene aggiornato con i dati di esempio. Per informazioni sui dati `tickit`, consultare [Database di esempio](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

#### tpch

Questi dati vengono utilizzati per un benchmark di supporto decisionale. Quando si caricano questi dati, lo schema `tpch` viene aggiornato con i dati di esempio. Per ulteriori informazioni sui dati `tpch`, consulta [TPC-H](#).

#### tpcds

Questi dati vengono utilizzati per un benchmark di supporto decisionale. Quando si caricano questi dati, lo schema `tpcds` viene aggiornato con i dati di esempio. Per ulteriori informazioni sui dati `tpcds`, consulta [TPC-DS](#).

## Caricamento di dati da Amazon S3

È possibile caricare dati Amazon S3 in una tabella esistente o in una nuova tabella.

## Per caricare i dati in una tabella esistente

Il comando COPIA viene utilizzato dall'editor di query v2 per caricare i dati da Amazon S3. Il comando COPY generato e utilizzato nell'editor di query v2 della procedura guidata Carica dati supporta molti dei parametri disponibili per la sintassi del comando COPY per caricare i dati da Amazon S3. Per informazioni sul comando COPIA e sulle opzioni utilizzate per copiare il caricamento da Amazon S3, consultare [COPIA da Amazon Simple Storage Service](#) nella Guida per sviluppatori di database Amazon Redshift.

1. Confermare che la tabella sia già stata creata nel database in cui si desidera caricare i dati.
2. Prima di continuare, verifica la connessione al database di destinazione nel pannello della visualizzazione ad albero dell'editor di query v2. È possibile creare una connessione utilizzando il menu contestuale (clic con il pulsante destro del mouse) al cluster o al gruppo di lavoro in cui verranno caricati i dati.

Scegliere



Carica

dati.

3. Per Origine dati, scegli Carica dal bucket S3.
4. In URI S3, scegliere Cerca S3 per cercare il bucket Amazon S3 che contiene i dati da caricare.
5. Se il bucket Amazon S3 specificato non si trova nella Regione AWS stessa tabella di destinazione, scegli la posizione del file S3 Regione AWS in cui si trovano i dati.
6. Scegliere Questo file è un file manifesto se il file Amazon S3 è in realtà un manifesto contenente più URI bucket Amazon S3.
7. Scegliere il Formato del file per il file da caricare. I formati dati supportati sono CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. A seconda del formato di file specificato, è possibile scegliere le rispettive Opzioni file. È possibile anche selezionare I dati sono crittografati se i dati sono crittografati e inserire l'Amazon Resource Name (ARN) della chiave KMS utilizzata per crittografare i dati.

Se si sceglie CSV o DELIMITER, è anche possibile scegliere il Carattere delimitatore ed eventualmente l'opzione Ignora righe di intestazione se il numero di righe specificato rappresenta effettivamente nomi di colonna e non dati da caricare.

8. Scegliere un metodo di compressione per comprimere il file. L'impostazione predefinita è nessuna compressione.

9. (Facoltativo) Le Impostazioni avanzate supportano vari Parametri di conversione dei dati e Operazioni di caricamento. Inserisci queste informazioni secondo necessità per il tuo file.

Per ulteriori informazioni sulla conversione dei dati e sui parametri di caricamento dei dati, consultare [Parametri di conversione dei dati](#) e [Operazioni di caricamento dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift

10. Seleziona Successivo.
11. Scegli Carica tabella esistente.
12. Conferma o scegli la posizione Target table (Tabella di destinazione) inclusi Cluster or workgroup (Cluster o gruppo di lavoro), Database, Schema e nome Table (Tabella) in cui vengono caricati i dati.
13. Scegliere un ruolo IAM che dispone delle autorizzazioni necessarie per caricare i dati da Amazon S3.
14. (Facoltativo) Scegli i nomi delle colonne per inserirli in Column mapping (Mappatura colonne) per mappare le colonne nell'ordine del file dei dati di input.
15. Scegliere Caricare dati per avviare il caricamento dei dati.

Al termine del caricamento, l'editor di query viene visualizzato con il comando COPIA generato e utilizzato per caricare i dati. Viene mostrato il Risultato di COPIA. In caso di esito positivo, è ora possibile utilizzare SQL per selezionare i dati dalla tabella caricata. Quando si verifica un errore, eseguire una query sulla visualizzazione di sistema STL\_LOAD\_ERRORS per ottenere ulteriori dettagli. Per informazioni sugli errori del comando COPIA, consultare [STL\\_LOAD\\_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Quando si caricano i dati in una nuova tabella, l'editor di query v2 crea prima la tabella nel database, quindi carica i dati come operazioni separate nello stesso flusso di lavoro.

### Caricamento di dati in una nuova tabella

Il comando COPIA viene utilizzato dall'editor di query v2 per caricare i dati da Amazon S3. Il comando COPY generato e utilizzato nell'editor di query v2 della procedura guidata Carica dati supporta molti dei parametri disponibili per la sintassi del comando COPY per caricare i dati da Amazon S3. Per informazioni sul comando COPIA e sulle opzioni utilizzate per copiare il caricamento da Amazon S3, consultare [COPIA da Amazon Simple Storage Service](#) nella Guida per sviluppatori di database Amazon Redshift.

1. Prima di continuare, verifica la connessione al database di destinazione nel pannello della visualizzazione ad albero dell'editor di query v2. È possibile creare una connessione utilizzando il menu contestuale (clic con il pulsante destro del mouse) al cluster o al gruppo di lavoro in cui verranno caricati i dati.

Scegliere



dati.

Carica

2. Per Origine dati, scegli Carica dal bucket S3.
3. In URI S3, scegliere Cerca S3 per cercare il bucket Amazon S3 che contiene i dati da caricare.
4. Se il bucket Amazon S3 specificato non si trova nella Regione AWS stessa tabella di destinazione, scegli la posizione del file S3 Regione AWS in cui si trovano i dati.
5. Scegliere Questo file è un file manifesto se il file Amazon S3 è in realtà un manifesto contenente più URI bucket Amazon S3.
6. Scegliere il Formato del file per il file da caricare. I formati dati supportati sono CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. A seconda del formato di file specificato, è possibile scegliere le rispettive Opzioni file. È possibile anche selezionare I dati sono crittografati se i dati sono crittografati e inserire l'Amazon Resource Name (ARN) della chiave KMS utilizzata per crittografare i dati.

Se si sceglie CSV o DELIMITER, è anche possibile scegliere il Carattere delimitatore ed eventualmente l'opzione Ignora righe di intestazione se il numero di righe specificato rappresenta effettivamente nomi di colonna e non dati da caricare.

7. Scegliere un metodo di compressione per comprimere il file. L'impostazione predefinita è nessuna compressione.
8. (Facoltativo) Le Impostazioni avanzate supportano vari Parametri di conversione dei dati e Operazioni di caricamento. Inserisci queste informazioni secondo necessità per il tuo file.

Per ulteriori informazioni sulla conversione dei dati e sui parametri di caricamento dei dati, consultare [Parametri di conversione dei dati](#) e [Operazioni di caricamento dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift

9. Seleziona Successivo.
10. Scegli Carica nuova tabella.

Le colonne della tabella sono dedotte dai dati di input. È possibile modificare la definizione dello schema della tabella aggiungendo colonne e dettagli della tabella. Per tornare allo schema della tabella dedotta dall'editor di query v2, scegli Ripristina i valori predefiniti.

11. Conferma o scegli la posizione della Tabella di destinazione inclusi Cluster o gruppo di lavoro, Database e Schema in cui vengono caricati i dati. Inserisci un nome per la tabella da creare.
12. Scegliere un ruolo IAM che dispone delle autorizzazioni necessarie per caricare i dati da Amazon S3.
13. Scegli Crea tabella per creare la tabella utilizzando la definizione mostrata.

Viene visualizzato un riepilogo della definizione della tabella. La tabella viene creata nel database. Per eliminare la tabella in un secondo momento, esegui un comando SQL DROP TABLE. Per ulteriori informazioni, consulta [DROP TABLE](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

14. Scegliere Caricare dati per avviare il caricamento dei dati.

Al termine del caricamento, l'editor di query viene visualizzato con il comando COPIA generato e utilizzato per caricare i dati. Viene mostrato il Risultato di COPIA. In caso di esito positivo, è ora possibile utilizzare SQL per selezionare i dati dalla tabella caricata. Quando si verifica un errore, eseguire una query sulla visualizzazione di sistema STL\_LOAD\_ERRORS per ottenere ulteriori dettagli. Per informazioni sugli errori del comando COPIA, consultare [STL\\_LOAD\\_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Caricamento di dati da una configurazione di file e da un flusso di lavoro locali

È possibile caricare dati da un file locale in una tabella nuova o esistente.

### Configurazione dell'amministratore per caricare dati da un file locale

L'amministratore dell'editor di query v2 deve specificare il bucket Amazon S3 comune nella finestra Account settings (Impostazioni account). Gli utenti dell'account devono essere configurati con le autorizzazioni appropriate.

- Autorizzazioni IAM richieste: gli utenti che caricano dal file locale devono disporre delle autorizzazioni `s3:ListBucket`, `s3:GetBucketLocation`, `s3:putObject`, `s3:getObject` e `s3:deleteObject`. È possibile specificare *optional-prefix* per limitare l'uso correlato dell'editor di query v2 di questo bucket agli oggetti con questo prefisso. Puoi utilizzare questa opzione quando utilizzi lo stesso bucket Amazon S3 per usi diversi dall'editor di query v2.

Per ulteriori informazioni su bucket e prefissi, consulta [Gestione dell'accesso utente a cartelle specifiche](#) nella Guida per l'utente di Amazon Simple Storage Service. Per garantire che l'accesso ai dati tra utenti non sia consentito, consigliamo all'amministratore dell'editor di query v2 di utilizzare una policy dei bucket Amazon S3 per limitare l'accesso agli oggetti in base all'`aws:user-id`. L'esempio seguente consente autorizzazioni di Amazon S3 a un `<staging-bucket-name>` con accesso in lettura/scrittura solo agli oggetti Amazon S3 con `aws:user-id` come prefisso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket-name>"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
        ${aws:user-id}/*"
      ]
    }
  ]
}
```

- Separazione dei dati: consigliamo agli utenti di non avere accesso ai dati degli altri utenti (anche solo per breve tempo). Il caricamento da un file locale utilizza il bucket temporaneo di Amazon S3 configurato dall'amministratore dell'editor di query v2. Configura la policy dei bucket per il bucket temporaneo per fornire la separazione dei dati tra gli utenti. L'esempio seguente mostra una policy del bucket che separa i dati tra gli utenti di `<staging-bucket-name>`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "userIdPolicy",
      "Effect": "Deny",
      "Principal": "*",
      "Action": ["s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"],
      "NotResource": [
        "arn:aws:s3:::<staging-bucket-name>[/<optional-prefix>]/
        ${aws:userid}/*"
      ]
    }
  ]
}
```

## Caricamento di dati da un file locale

### Caricamento di dati di un file locale in una tabella esistente

L'amministratore dell'editor di query v2 deve specificare il bucket Amazon S3 comune nella finestra Impostazioni account. L'editor di query v2 carica automaticamente il file locale in un bucket Amazon S3 comune utilizzato dall'account dell'utente, quindi utilizza il comando COPY per caricare i dati. Il comando COPY generato ed eseguito dalla finestra di caricamento del file locale dell'editor di query v2 supporta molti dei parametri disponibili per la sintassi del comando COPY da copiare da Amazon S3. Per informazioni sul comando COPY e sulle opzioni utilizzate per caricare i dati da Amazon S3, consulta [COPY da Amazon S3](#) nella Guida per sviluppatori di database Amazon Redshift.

1. Confermare che la tabella sia già stata creata nel database in cui si desidera caricare i dati.
2. Verifica che si attiva la connessione al database di destinazione nel pannello della visualizzazione ad albero dell'editor di query v2. È possibile creare una connessione utilizzando il menu contestuale (clic con il pulsante destro del mouse) al cluster o al gruppo di lavoro in cui verranno caricati i dati.
3. Scegliere
  -  dati.

Carica

4. Per Data source (Origine dati), scegli Load from local file (Carica da file locale).
5. Scegli Sfoglia per trovare il file che contiene i dati per Carica file. Per impostazione predefinita vengono visualizzati i file con estensione .csv, .avro, .parquet e .orc, ma è possibile scegliere altri tipi di file. Il file può avere una dimensione massima di 100 MB.
6. Scegliere il Formato del file per il file da caricare. I formati dati supportati sono CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. A seconda del formato di file specificato, è possibile scegliere le rispettive Opzioni file. È possibile anche selezionare I dati sono crittografati se i dati sono crittografati e inserire l'Amazon Resource Name (ARN) della chiave KMS utilizzata per crittografare i dati.

Se si sceglie CSV o DELIMITER, è anche possibile scegliere il Carattere delimitatore ed eventualmente l'opzione Ignora righe di intestazione se il numero di righe specificato rappresenta effettivamente nomi di colonna e non dati da caricare.

7. (Facoltativo) Le Impostazioni avanzate supportano vari Parametri di conversione dei dati e Operazioni di caricamento. Inserisci queste informazioni secondo necessità per il tuo file.

Per ulteriori informazioni sulla conversione dei dati e sui parametri di caricamento dei dati, consultare [Parametri di conversione dei dati](#) e [Operazioni di caricamento dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift

8. Seleziona Successivo.
9. Scegli Carica tabella esistente.
10. Conferma o scegli la posizione Target table (Tabella di destinazione) inclusi Cluster or workgroup (Cluster o gruppo di lavoro), Database, Schema e nome Table (Tabella) in cui vengono caricati i dati.
11. (Facoltativo) Puoi scegliere i nomi delle colonne per inserirli in Column mapping (Mappatura colonne) per mappare le colonne nell'ordine del file dei dati di input.
12. Scegliere Caricare dati per avviare il caricamento dei dati.

Al termine del caricamento, viene visualizzato un messaggio che indica se il caricamento è andato a buon fine o meno. In caso di esito positivo, è ora possibile utilizzare SQL per selezionare i dati dalla tabella caricata. Quando si verifica un errore, eseguire una query sulla visualizzazione di sistema STL\_LOAD\_ERRORS per ottenere ulteriori dettagli. Per informazioni sugli errori del comando COPIA, consultare [STL\\_LOAD\\_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Il modello del comando COPY utilizzato per caricare i dati viene visualizzato in Query history (Cronologia query). Questo modello di comando COPY mostra alcuni dei parametri utilizzati, ma non può essere eseguito direttamente in una scheda dell'editor. Per ulteriori informazioni sulla cronologia delle query, consulta [Visualizzazione della cronologia delle query e delle schede](#).

Quando si caricano i dati in una nuova tabella, l'editor di query v2 crea prima la tabella nel database, quindi carica i dati come operazioni separate nello stesso flusso di lavoro.

### Caricamento di dati di un file locale in una nuova tabella

L'amministratore dell'editor di query v2 deve specificare il bucket Amazon S3 comune nella finestra Account settings (Impostazioni account). Il file locale viene caricato automaticamente in un bucket Amazon S3 comune utilizzato dal tuo account, quindi l'editor di query v2 utilizza il comando COPY per caricare i dati. Il comando COPY generato ed eseguito dalla finestra di caricamento del file locale dell'editor di query v2 supporta molti dei parametri disponibili per la sintassi del comando COPY da copiare da Amazon S3. Per informazioni sul comando COPY e sulle opzioni utilizzate per caricare i dati da Amazon S3, consulta [COPY da Amazon S3](#) nella Guida per sviluppatori di database Amazon Redshift.

1. Verifica che si attiva la connessione al database di destinazione nel pannello della visualizzazione ad albero dell'editor di query v2. È possibile creare una connessione utilizzando il menu contestuale (clic con il pulsante destro del mouse) al cluster o al gruppo di lavoro in cui verranno caricati i dati.
2. Scegliere  Carica dati.
3. Per Data source (Origine dati), scegli Load from local file (Carica da file locale).
4. Scegli Sfoglia per trovare il file che contiene i dati per Carica file. Per impostazione predefinita vengono visualizzati i file con estensione .csv, .avro, .parquet e .orc, ma è possibile scegliere altri tipi di file. Il file può avere una dimensione massima di 100 MB.
5. Scegliere il Formato del file per il file da caricare. I formati dati supportati sono CSV, JSON, DELIMITER, FIXEDWIDTH, SHAPEFILE, AVRO, PARQUET e ORC. A seconda del formato di file specificato, è possibile scegliere le rispettive Opzioni file. È possibile anche selezionare I dati sono crittografati se i dati sono crittografati e inserire l'Amazon Resource Name (ARN) della chiave KMS utilizzata per crittografare i dati.

Carica

Se si sceglie CSV o DELIMITER, è anche possibile scegliere il Carattere delimitatore ed eventualmente l'opzione Ignora righe di intestazione se il numero di righe specificato rappresenta effettivamente nomi di colonna e non dati da caricare.

6. (Facoltativo) Le Impostazioni avanzate supportano vari Parametri di conversione dei dati e Operazioni di caricamento. Inserisci queste informazioni secondo necessità per il tuo file.

Per ulteriori informazioni sulla conversione dei dati e sui parametri di caricamento dei dati, consultare [Parametri di conversione dei dati](#) e [Operazioni di caricamento dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift

7. Seleziona Successivo.
8. Scegli Carica nuova tabella.
9. Conferma o scegli la posizione della Tabella di destinazione inclusi Cluster o gruppo di lavoro, Database e Schema in cui vengono caricati i dati. Inserisci un nome per la tabella da creare.
10. Scegli Crea tabella per creare la tabella utilizzando la definizione mostrata.

Viene visualizzato un riepilogo della definizione della tabella. La tabella viene creata nel database. Per eliminare la tabella in un secondo momento, esegui un comando SQL DROP TABLE. Per ulteriori informazioni, consulta [DROP TABLE](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

11. Scegliere Caricare dati per avviare il caricamento dei dati.

Al termine del caricamento, viene visualizzato un messaggio che indica se il caricamento è andato a buon fine o meno. In caso di esito positivo, è ora possibile utilizzare SQL per selezionare i dati dalla tabella caricata. Quando si verifica un errore, eseguire una query sulla visualizzazione di sistema STL\_LOAD\_ERRORS per ottenere ulteriori dettagli. Per informazioni sugli errori del comando COPIA, consultare [STL\\_LOAD\\_ERRORS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Il modello del comando COPY utilizzato per caricare i dati viene visualizzato in Query history (Cronologia query). Questo modello di comando COPY mostra alcuni dei parametri utilizzati, ma non può essere eseguito direttamente in una scheda dell'editor. Per ulteriori informazioni sulla cronologia delle query, consulta [Visualizzazione della cronologia delle query e delle schede](#).

## Autorizzazione e esecuzione di query

È possibile inserire una query nell'editor o selezionare una query salvata dall'elenco Query e scegliere Esegui.

Per impostazione predefinita, Limite 100 è impostato per limitare i risultati a 100 righe. È possibile disattivare questa opzione per restituire un set di risultati più ampio. Se si disattiva questa opzione, è possibile includere l'opzione LIMITE nell'istruzione SQL se si desidera evitare set di risultati molto grande. Per ulteriori informazioni, consultare [Clausola ORDINA PER](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Per visualizzare un piano di query nell'area dei risultati, attivare Spiega. Attiva Explain graph (Grafico Explain) affinché nei risultati venga visualizzata anche una rappresentazione grafica del piano Explain.

Per salvare una query nella cartella Query, scegliere Salva.

Per una query riuscita, viene visualizzato un messaggio di successo. Se la query restituisce informazioni, i risultati vengono visualizzati nella sezione Risultati. Se il numero di risultati supera l'area di visualizzazione, i numeri vengono visualizzati nella parte superiore dell'area dei risultati. È possibile scegliere i numeri per visualizzare le pagine successive dei risultati.

È possibile filtrare e ordinare Risultato per ogni colonna. Per inserire i criteri di filtro nell'intestazione della colonna dei risultati, passa il mouse sopra la colonna per visualizzare un menu



dove è possibile inserire i criteri per filtrare la colonna.

Se la query contiene un errore, l'editor di query v2 visualizza un messaggio di errore nell'area dei risultati. Il messaggio fornisce informazioni su come correggere la query.

È possibile esportare o copiare i risultati della query utilizzando il menu contestuale (pulsante destro del mouse) nell'area dei risultati come indicato di seguito:

- Scegli Export result set (Esporta set di risultati) e JSON o CSV per scaricare l'intero set di risultati di riga in un file. Il numero di righe nel set di risultati potrebbe essere limitato dall'opzione Limite o dalla clausola SQL `limit` nella query. La dimensione massima del set di risultati scaricato è 5 MB.
- Se non è selezionata alcuna riga, scegli Export current page (Esporta la pagina corrente) e JSON o CSV per scaricare le righe dalla pagina corrente in un file.

- Se ci sono righe selezionate, scegli Export selected rows (Esporta righe selezionate) e JSON o CSV per scaricare le righe selezionate in un file.
- Se ci sono righe selezionate, scegli Copy rows (Copia righe) per copiare le righe selezionate negli appunti.
- Se ci sono righe selezionate, scegli Copy rows with headers (Copia righe con intestazioni) per copiare le righe selezionate con intestazioni di colonna negli appunti.

È inoltre possibile utilizzare i tasti di scelta rapida Ctrl+C su Windows o Cmd+C su macOS per copiare i dati dalla pagina dei risultati corrente negli appunti. Se ci sono righe selezionate, la cella con lo stato attivo viene copiata negli appunti. Se ci sono righe selezionate, queste ultime vengono copiate negli appunti.

Per aggiungere una nuova scheda della query, selezionare l'icona



quindi Editor, che appare nella riga con le schede della query. È possibile che la scheda della query utilizzi `Isolated session`. Con una sessione isolata, i risultati di un comando SQL in una scheda dell'editor, ad esempio la creazione di una tabella temporanea, non sono visibili in un'altra scheda dell'editor. Quando si apre una scheda nell'editor di query v2, per impostazione predefinita viene usata una sessione isolata.

Per eseguire una query

1. Nell'area della query effettuare una delle seguenti operazioni:
  - Inserisci una query.
  - Incolla una query copiata.
  - Selezionare la cartella Query, aprire dal menu contestuale (tasto destro del mouse) una query salvata e scegliere Aprire una query.
2. Conferma di aver scelto il valore corretto di Cluster o Workgroup (Gruppo di lavoro) e Database per l'SQL che intendi eseguire.

Inizialmente, puoi scegliere Cluster o Workgroup (Gruppo di lavoro) nella struttura ad albero. Nella stessa struttura, scegli anche Database.

È possibile modificare i valori nei campi Cluster o Workgroup (Gruppo di lavoro) e Database all'interno di ogni scheda dell'editor mediante il controllo a discesa accanto all'intestazione `Isolated session` (Sessione isolata).

Per ogni scheda dell'editor, è possibile scegliere se eseguire il codice SQL in una sessione isolata. Una sessione isolata dispone di una propria connessione a un database. È possibile utilizzarla per eseguire comandi SQL isolati rispetto alle altre sessioni dell'editor di query. Per ulteriori informazioni sulle connessioni, consulta [Apertura editor di query v2](#).

### 3. Seleziona Esegui.

L'area Risultati si apre e visualizza i risultati della query.

Per visualizzare il piano di spiegazione per una query

1. Seleziona la query.
2. Attivare Spiega.

Per impostazione predefinita, anche Spiega il grafico è attivato.

### 3. Seleziona Esegui.

La query viene eseguita e il piano di spiegazione viene visualizzato nell'area Risultato della query.

L'editor di query v2 supporta le seguenti funzionalità:

- È possibile autorizzare query con più istruzioni SQL in un'unica scheda di query. Le query vengono eseguite in serie e vengono aperte più schede dei risultati per ogni query.
- È possibile autorizzare query con variabili di sessione e tabelle temporanee.
- È possibile autorizzare query con parametri sostituibili designati da  $\${parameter}$ . È possibile autorizzare la query SQL con più parametri sostituibili e utilizzare lo stesso parametro in più posizioni nell'istruzione SQL.

Quando la query viene eseguita, viene visualizzata una finestra per inserire il valore del parametro. Ogni volta che si esegue la query, viene visualizzata la finestra per immettere i valori dei parametri.

Per vedere un esempio, consulta [Esempio: vendite superiori a un parametro specifico](#).

- Viene eseguito automaticamente un controllo delle versioni delle query. È possibile scegliere una versione precedente di una query da eseguire.
- Non è necessario attendere il completamento di una query prima di continuare con il flusso di lavoro. Le query continuano ad essere eseguite anche se si chiude l'editor di query.

- Quando si creano query, è supportato il completamento automatico dei nomi di schema, tabella e colonna.

L'editor SQL supporta le seguenti caratteristiche:

- Le parentesi iniziali e finali utilizzate in SQL hanno colori corrispondenti. Le linee verticali sono mostrate nell'editor per aiutare ad abbinare le parentesi.
- Puoi comprimere ed espandere sezioni dell'SQL.
- Puoi ricercare e sostituire il testo nell'SQL.
- È possibile utilizzare i tasti di scelta rapida per diverse attività comuni di modifica.
- Gli errori SQL sono evidenziati nell'editor per facilitare l'individuazione delle aree problematiche.

Per una demo sulle caratteristiche di modifica, guarda questo video: [New and Enhanced Editing Experience in Amazon Redshift query editor v2](#).

## Esempi di query

Di seguito vengono fornite le descrizioni dei vari tipi di query che è possibile eseguire.

I dati utilizzati in molte di queste query provengono dallo schema di esempio `tickit`. Per ulteriori informazioni sul caricamento dei dati di esempio in `tickit`, consulta [Caricamento di dati di esempio](#). Per informazioni sui dati di esempio `tickit`, consulta [Database di esempio](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Quando si eseguono queste query di esempio, confermare di aver scelto il database corretto nell'editor, ad esempio `sample_data_dev`.

### Argomenti

- [Esempio: impostazione delle variabili di sessione](#)
- [Esempio: migliore evento per vendite totali](#)
- [Esempio: vendite superiori a un parametro specifico](#)
- [Esempio: Creazione di una tabella temporanea](#)
- [Esempio: selezione da una tabella temporanea](#)

## Esempio: impostazione delle variabili di sessione

Il comando seguente imposta il parametro di configurazione del server `search_path` pubblico per la sessione. Per ulteriori informazioni, consultare [IMPOSTA](#) e [search\\_path](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

```
set search_path to public;
```

## Esempio: migliore evento per vendite totali

La seguente query trova l'evento con il maggior numero di vendite.

```
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname
order by 3;
```

Di seguito è riportato un elenco parziale dei risultati.

eventname	totalorders	totalsales
White Christmas	20	9352
Joshua Radin	38	23469
Beach Boys	58	30383
Linda Ronstadt	56	35043
Rascal Flatts	76	38214
Billy Idol	67	40101
Stephenie Meyer	72	41509
Indigo Girls	57	45399
...		

## Esempio: vendite superiori a un parametro specifico

La seguente query rileva le vendite in cui la quantità venduta è superiore al parametro specificato da `${numberoforders}`. Quando il valore del parametro è 7, il risultato è di 60 righe. Quando si esegue la query, l'editor di query v2 visualizza la finestra Modulo di esecuzione della query per raccogliere il valore dei parametri nell'istruzione SQL.

```
select salesid, qtysold
from sales
where qtysold > ${numberoforders}
```

```
order by 2;
```

Di seguito è riportato un elenco parziale dei risultati.

```
salesid qty sold
20005 8
21279 8
130232 8
42737 8
74681 8
67103 8
105533 8
91620 8
121552 8
...
```

Esempio: Creazione di una tabella temporanea

La seguente istruzione crea la tabella temporanea `eventsalestemp` selezionando le informazioni dalle tabelle vendite e evento.

```
create temporary table eventsalestemp as
select eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid
group by eventname;
```

Esempio: selezione da una tabella temporanea

La seguente istruzione seleziona eventi, ordini totali e vendite totali dalla tabella temporanea `eventsalestemp`, ordinato per ordini totali.

```
select eventname, totalorders, totalsales
from eventsalestemp
order by 2;
```

Di seguito è riportato un elenco parziale dei risultati.

eventname	totalorders	totalsales
White Christmas	20	9352
Joshua Radin	38	23469

Martina McBride	50	52932
Linda Ronstadt	56	35043
Indigo Girls	57	45399
Beach Boys	58	30383
...		

## Autorizzazione ed esecuzione di notebook

È possibile utilizzare i notebook per organizzare, annotare e condividere più query SQL in un singolo documento. È possibile aggiungere più query SQL e celle Markdown a un notebook. I notebook offrono un modo per raggruppare query e spiegazioni associate a un'analisi dei dati in un singolo documento utilizzando più query e celle Markdown. È possibile aggiungere testo e formattare l'aspetto utilizzando la sintassi Markdown per fornire contesto e informazioni aggiuntive per le attività di analisi dei dati. È possibile condividere i notebook con i membri del team.

Per utilizzare i notebook, è necessario aggiungere l'autorizzazione per i notebook al principale IAM (un utente IAM o un ruolo IAM). Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#). È possibile aggiungere l'autorizzazione a una delle policy gestite dell'editor di query v2. Per ulteriori informazioni, consulta [Accesso all'editor di query v2](#).

È possibile selezionare l'opzione Run all (Esegui tutte) per eseguire tutte le celle di un notebook in sequenza. La cella di query SQL di un notebook include la maggior parte delle funzionalità di una scheda dell'editor di query. Per ulteriori informazioni, consulta [Autorizzazione e esecuzione di query](#). Di seguito sono elencate le differenze tra una scheda dell'editor di query e una cella SQL in un notebook.

- In un notebook non esiste un controllo per eseguire Explain su un'istruzione SQL.
- È possibile creare un solo grafico per cella SQL in un notebook.

È possibile esportare e importare notebook in file creati con l'editor di query v2. L'estensione dei file è .ipynb e la dimensione massima dei file è 5 MB. Le celle SQL e Markdown vengono archiviate nei file. Un cluster o un gruppo di lavoro e un database non vengono archiviati nel notebook esportato. Quando si apre un notebook importato, occorre scegliere il cluster o il gruppo di lavoro e il database in cui eseguirlo. Dopo aver eseguito le celle SQL, è possibile scegliere nella scheda dei risultati se visualizzare la pagina corrente dei risultati come grafico. Il set di risultati di una query non è archiviato nel notebook.

Quando esegui un notebook con **Esegui tutto** o **Esegui**, diventa disponibile il pannello Stato dell'esecuzione. Scegli l'icona



per aprire il pannello. Questo pannello contiene un riepilogo dello stato delle operazioni **Esegui tutto** o **Esegui** più recenti delle celle SQL del notebook. Se esegui più celle SQL, puoi vedere immediatamente lo stato, il tempo trascorso e alcuni dettagli sull'esecuzione. Puoi filtrare le celle visualizzate in base allo stato: **All**, **Succeeded**, **Error**, **In progress** o **Canceled**. Inoltre, puoi utilizzare questo pannello per accedere a una cella SQL nell'editor.

### Creazione di un notebook

1. Dal menu del navigatore, scegli



Editor.

2. Scegli



e quindi scegli **Notebook**.

Per impostazione predefinita, nel notebook viene visualizzata una cella di query SQL.

3. Nella cella della query SQL effettuare una delle seguenti operazioni:

- Inserisci una query.
- Incolla una query copiata.

4. (Facoltativo) Seleziona l'icona



quindi scegli **Markdown** per aggiungere una cella Markdown in cui includere testo descrittivo o esplicativo utilizzando la sintassi standard Markdown.

5. (Facoltativo) Seleziona l'icona



quindi scegli **SQL** per inserire una cella SQL.

È possibile rinominare i notebook utilizzando l'icona



(matita).

Dal menu



(altro), è inoltre possibile eseguire le seguenti operazioni su un notebook:



Share with my team (Condividi con il mio team): consente di condividere il notebook con il team come definito dai tag. Per ulteriori informazioni, consultare [Condivisione di una query](#)



Export (Esporta): consente di esportare il notebook in un file locale con estensione `.ipynb`.



Save version (Salva versione): consente di creare una versione del notebook. Per visualizzare le versioni di un notebook, accedi ai notebook salvati e apri Version history (Cronologia delle versioni).



Duplicate (Duplica): consente di creare una copia del notebook e aprirlo in una nuova scheda del notebook.



Shortcuts (Scorciatoie): consente di visualizzare le scorciatoie disponibili durante la creazione di un notebook.

Come aprire un notebook salvato

1. Dal menu del navigatore, seleziona



Notebook. Vengono visualizzati i notebook e le cartelle dei notebook salvati.

2. Scegli il notebook da aprire e fai doppio clic su di esso.

Nella scheda dei notebook puoi mostrare My notebooks (I miei notebook), i notebook Shared by me (Condivisi da me) e i notebook Shared to my team (Condivisi con il mio team).

Per importare un notebook da un file locale in My notebooks (I miei notebook), scegli



Import (Importa), quindi vai al file `.ipynb` contenente il notebook. Il notebook viene importato nella cartella del notebook attualmente aperta. È possibile aprire il notebook nell'editor del notebook.

Dal menu contestuale (tasto destro del mouse) di un notebook è possibile eseguire queste operazioni:

- Open notebook (Apri notebook): consente di aprire il notebook nell'editor.
- Save version (Salva versione): consente di salvare una versione del notebook.
- Version history (Cronologia delle versioni): consente di visualizzare le versioni di un notebook. Dalla finestra Version history (Cronologia delle versioni) è possibile eliminare e ripristinare versioni. È anche possibile creare un notebook dalla versione attualmente selezionata.
- Edit tags (Modifica tag): consente di creare e modificare tag su un notebook.
- Share with my team (Condividi con il mio team): consente di condividere un notebook con il team.

Per condividere una query con il team, assicurati di disporre del tag principale `sqlworkbench-team` impostato sullo stesso valore del resto dei membri del team nel tuo account. Ad esempio, un amministratore potrebbe impostare il valore su `accounting-team` per tutti nel reparto contabilità. Per vedere un esempio, consulta [Autorizzazioni necessarie per utilizzare l'editor della query v2](#).

- Export (Esporta): consente di esportare un notebook in un file locale.
- Rename (Rinomina): consente di rinominare un notebook.
- Duplicate (Duplica): consente di creare una copia di un notebook.
- Delete (Elimina): consente di eliminare un notebook.

Per una demo dei notebook, guarda il seguente video: [SQL Notebooks in Amazon Redshift Query Editor V2](#).

## Interrogare il AWS Glue Data Catalog

Puoi utilizzare l'editor di query v2 per eseguire query sui dati catalogati in AWS Glue Data Catalog. Per impostazione predefinita, AWS Glue Data Catalog è elencato come database dell'editor di query v2 denominato `awsdatacatalog`. L'interrogazione di non AWS Glue Data Catalog è disponibile

in tutti gli Amazon Regioni AWS Redshift. Utilizza il comando SHOW per determinare se questa funzionalità è disponibile. Per ulteriori informazioni su AWS Glue, consulta [What is? AWS Glue](#) nella Guida per gli AWS Glue sviluppatori.

### Note

L'interrogazione AWS Glue Data Catalog è supportata solo nei cluster di tipo nodo Amazon Redshift RA3 e Amazon Redshift Serverless.

Puoi configurare il tuo data warehouse e visualizzare gli oggetti del AWS Glue database catalogati utilizzando i seguenti comandi SQL:

- **SHOW:** per visualizzare se `awsdatacatalog` è montato per il data warehouse attualmente connesso. Ad esempio, per mostrare il valore del parametro `data_catalog_auto_mount`, esegui:

```
SHOW data_catalog_auto_mount;
```

Per ulteriori informazioni, consulta [SHOW](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- **ALTER SYSTEM:** per modificare la configurazione a livello di sistema di `data_catalog_auto_mount`. Ad esempio, per modificare il valore del parametro `data_catalog_auto_mount` a on, esegui:

```
ALTER SYSTEM SET data_catalog_auto_mount = on;
```

La modifica ha effetto quando un cluster fornito viene riavviato o un gruppo di lavoro serverless viene automaticamente messo in pausa e ripreso. Per ulteriori informazioni, consulta [ALTER SYSTEM](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- **SHOW SCHEMAS:** mostra un elenco di schemi. Gli schemi del database denominato `awsdatacatalog` rappresentano i AWS Glue database catalogati in AWS Glue Data Catalog. Ad esempio, per mostrare questi schemi, esegui:

```
SHOW SCHEMAS FROM DATABASE awsdatacatalog;
```

Per ulteriori informazioni, consulta [SHOW SCHEMAS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- **SHOW TABLES:** mostra un elenco di tabelle in uno schema. Ad esempio, per mostrare le tabelle del AWS Glue Data Catalog database denominate `awsdatacatalog` presenti nello `schemamyglue`, esegui:

```
SHOW TABLES FROM SCHEMA awsdatacatalog.myschema;
```

Per ulteriori informazioni, consulta [SHOW TABLES](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- **SHOW COLUMNS:** mostra un elenco di colonne in una tabella. Ad esempio, per mostrare le colonne del AWS Glue Data Catalog database denominate `awsdatacatalog` che si trovano nello schema `myglue` e nella tabella `mytable` esegui:

```
SHOW COLUMNS FROM TABLE awsdatacatalog.myglue.mytable;
```

Per ulteriori informazioni, consulta [SHOW COLUMNS](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Per concedere al tuo utente o ruolo IAM l'autorizzazione a interrogare il AWS Glue Data Catalog, segui questi passaggi

1. Nel riquadro della visualizzazione ad albero, connettiti al database iniziale nel cluster o nel gruppo di lavoro serverless utilizzando il metodo di autenticazione Nome utente e password del database. Ad esempio, connettiti al database dev utilizzando l'utente e la password dell'amministratore che hai usato quando hai creato il cluster o il gruppo di lavoro.
2. In una scheda dell'editor, esegui l'istruzione SQL seguente per concedere a un utente IAM l'accesso a AWS Glue Data Catalog.

```
GRANT USAGE ON DATABASE awsdatacatalog to "IAM:myIAMUser"
```

Dove *IAM:myIAMUser* è un utente IAM a cui desideri concedere il privilegio di utilizzo di AWS Glue Data Catalog. In alternativa, puoi concedere il privilegio di utilizzo a *IAMR:myIAMRole* per un ruolo IAM.

3. Nel riquadro della visualizzazione ad albero, modifica o elimina la connessione al cluster o al gruppo di lavoro che hai creato in precedenza. Collegati al cluster o al gruppo di lavoro in uno dei seguenti modi:
  - Per connetterti al database `awsdatacatalog` da un cluster, devi utilizzare il metodo di autenticazione Credenziali temporanee mediante l'identità IAM. Per ulteriori informazioni su questo metodo di autenticazione, consulta [Connessione a un database Amazon Redshift](#). L'amministratore dell'editor di query v2 potrebbe dover configurare Impostazioni account per l'account per visualizzare questi metodi di autenticazione nella finestra di connessione.
  - Per connetterti al database `awsdatacatalog` da un gruppo di lavoro, devi utilizzare il metodo di autenticazione Utente federato. Per ulteriori informazioni su questo metodo di autenticazione, consulta [Connessione a un database Amazon Redshift](#).
4. Con il privilegio concesso, puoi usare l'identità IAM per eseguire SQL su AWS Glue Data Catalog.

Dopo il collegamento, puoi utilizzare l'editor di query v2 per eseguire query sui dati catalogati in AWS Glue Data Catalog. Nel riquadro della visualizzazione ad albero dell'editor di query v2, scegli il cluster o il gruppo di lavoro e il database `awsdatacatalog`. Nel riquadro dell'editor o del notebook, verifica di aver selezionato il cluster o il gruppo di lavoro corretto. Il database scelto deve essere il database iniziale di Amazon Redshift, ad esempio `dev`. Per informazioni sulla creazione di query, consulta [Autorizzazione e esecuzione di query](#) e [Autorizzazione ed esecuzione di notebook](#). Il database denominato `awsdatacatalog` è riservato per fare riferimento al database del catalogo dati esterno del tuo account. Le query sul database `awsdatacatalog` possono solo essere di sola lettura. Utilizza la notazione in tre parti per fare riferimento alla tabella nell'istruzione `SELECT`. Dove la prima parte è il nome del database, la seconda è il nome del AWS Glue database e la terza è il nome della AWS Glue tabella.

```
SELECT * FROM awsdatacatalog.<aws-glue-db-name>.<aws-glue-table-name>;
```

Puoi eseguire vari scenari che leggono i AWS Glue Data Catalog dati e popolano le tabelle Amazon Redshift.

L'esempio seguente SQL unisce due tabelle definite in AWS Glue

```
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

L'esempio seguente SQL crea una tabella Amazon Redshift e la popola con i dati provenienti da un'unione di due tabelle. AWS Glue

```
CREATE TABLE dev.public.glue AS
SELECT pn.emp_id, alias, role, project_name
FROM "awsdatacatalog"."empl_db"."project_name_table" pn,
"awsdatacatalog"."empl_db"."project_alias_table" pa
WHERE pn.emp_id = pa.emp_id;
```

## Esecuzione di query in un data lake

È possibile eseguire query sui dati in un data lake Amazon S3. Per prima cosa, deve essere creato uno schema esterno che faccia riferimento al database esterno nel [AWS Glue Data Catalog](#). Quindi, sarà possibile eseguire la query sui dati in un data lake Amazon S3.

### Demo: query in un data lake

Per una demo su come eseguire una query in un data lake, guardare il video seguente. [Esecuzione di query in un data lake dall'editor di query Amazon Redshift v2](#).

### Prerequisiti

Prima di lavorare con il data lake nell'editor di query v2, verificare che nell'ambiente Amazon Redshift sia configurato quanto segue:

- Eseguire il crawling dei dati Amazon S3 utilizzando AWS Glue e abilitare il catalogo dati per AWS Lake Formation.
- Creare un ruolo IAM per Amazon Redshift utilizzando il catalogo dati abilitato per AWS Glue per AWS Lake Formation. Per ulteriori dettagli su questa procedura, consulta [Come creare un ruolo IAM per Amazon Redshift utilizzando un AWS Glue Data Catalog abilitato per AWS Lake Formation](#). Per ulteriori informazioni sull'uso di Redshift Spectrum e Lake Formation, consulta [Utilizzo di Redshift Spectrum con AWS Lake Formation](#).
- Concedere le autorizzazioni SELECT sulla tabella per eseguire le query nel database Lake Formation. Per ulteriori informazioni su questa procedura, consulta [Come concedere le autorizzazioni SELECT nella tabella per eseguire le query del database Lake Formation](#).

È possibile verificare nella console di Lake Formation (<https://console.aws.amazon.com/lakeformation/>), sezione Autorizzazioni, pagina delle autorizzazioni del Data lake, che il ruolo IAM, il database AWS Glue e le tabelle dispongano delle autorizzazioni appropriate.

- Verificare che l'utente connesso sia autorizzato a creare schemi nel database Amazon Redshift e ad accedere ai dati nel data lake. Quando ci si connette a un database nell'editor di query v2, scegliere un metodo di autenticazione che includa le credenziali, che possono essere un utente del database o un utente IAM. L'utente connesso deve disporre delle autorizzazioni e dei privilegi del database appropriati, ad esempio come `superuser`. L'utente `admin` di Amazon Redshift che ha creato il cluster o il gruppo di lavoro dispone di privilegi `superuser` e può creare schemi e gestire il database Redshift. Per ulteriori informazioni sulla connessione a un database con l'editor di query v2, consulta [Connessione a un database Amazon Redshift](#).

## Creazione di uno schema esterno

Per eseguire query sui dati in un data lake Amazon S3, viene creato uno schema esterno. Lo schema esterno fa riferimento a un database esterno in [AWS Glue Data Catalog](#).

1. Nella vista Editor dell'editor di query v2, scegliere



Crea,

quindi scegliere Schema.

2. Inserire un nome di schema.
3. Per Tipo di schema, scegliere Esterno.
4. Nei dettagli di Catalogo dati, la regione predefinita è la Regione AWS in cui si trova il database Redshift.
5. Scegliere il Database AWS Glue a cui verrà mappato lo schema esterno e che contiene riferimenti alle tabelle AWS Glue.
6. Scegliere un Ruolo IAM per Amazon Redshift che disponga delle autorizzazioni necessarie per eseguire query sui dati in Amazon S3.
7. Facoltativamente, scegliere un ruolo IAM con autorizzazione per il catalogo dati.
8. Scegliere Crea schema.

Lo schema viene visualizzato sotto il database nel pannello con visualizzazione ad albero.

Durante la creazione dello schema, se si riceve un errore di autorizzazione negata per il database, controllare se l'utente connesso dispone del privilegio di database per creare uno schema.

## Esecuzione di query sui dati nel data lake Amazon S3

Utilizzare lo schema creato nella procedura precedente.

1. Nel pannello con visualizzazione ad albero scegliere lo schema.
2. Per visualizzare una definizione di tabella, scegliere una tabella. Vengono visualizzati le colonne e i tipi di dati della tabella.
3. Per eseguire query in una tabella, selezionare la tabella e nel menu contestuale (pulsante destro del mouse) scegliere **Seleziona tabella** per generare una query.
4. Eseguire la query nell'Editor.

Il seguente esempio SQL è stato generato dall'editor di query v2 per eseguire query su tutte le righe della tabella AWS Glue denominata `flightscsv`. Le colonne e le righe mostrate nell'output vengono troncate per semplicità.

```
SELECT * FROM "dev"."mydatalake_schema"."flightscsv";
```

year	quarter	month	dom	day_of_week	fl_date	unique_carrier	airline_id
2016	4	10	19	3	10/19/16	00	20304
00		N753SK	3086				
2016	4	10	19	3	10/19/16	00	20304
00		N753SK	3086				
2016	4	10	19	3	10/19/16	00	20304
00		N778SK	3087				
2016	4	10	19	3	10/19/16	00	20304
00		N778SK	3087				
...							

## Utilizzo dell'unità di condivisione dati

È possibile creare un'unità di condivisione dati in modo che gli utenti di un altro cluster possano eseguire query sui dati. Il cluster che contiene i dati da condividere è chiamato cluster produttore. Puoi creare un'unità di condivisione dati sul cluster produttore per gli oggetti di database che desideri condividere. Puoi condividere schemi, tabelle, viste e funzioni definite dall'utente (UDF) di SQL. Il cluster con il quale intendi condividere i dati viene chiamato cluster consumatore. Nel cluster consumatore viene creato un database dall'unità di condivisione dati. Quindi, gli utenti del cluster

consumatore possono eseguire query sui dati. Per ulteriori informazioni, consulta [Nozioni di base sulla condivisione dei dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Creazione di unità di condivisione dati

Puoi creare un'unità di condivisione dati sul cluster da utilizzare come cluster produttore. Per ulteriori informazioni sulle considerazioni sull'unità di condivisione dati, consulta [Considerazioni sulla condivisione dei dati in Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

1. Scegli il database nel cluster produttore che desideri utilizzare.
2. Crea l'unità di condivisione dati. Ad esempio:

```
create datashare mysource;
```

3. Imposta le autorizzazioni per l'unità di condivisione dati. Ad esempio:

```
grant alter, share on datashare mysource to admin;
```

4. Imposta le autorizzazioni per gli oggetti del database che desideri condividere. Ad esempio:

```
alter datashare mysource add schema public;
```

```
alter datashare mysource add table public.event;
```

5. Imposta le autorizzazioni sullo spazio dei nomi del cluster consumatore per accedere all'unità di condivisione dati. Ad esempio:

```
grant usage on datashare mysource to namespace '2b12345-1234-5678-9012-  
bb1234567890';
```

## Visualizzazione dell'unità di condivisione dati

Puoi visualizzare le unità di condivisione dati create nel cluster produttore.

1. Scegli il cluster produttore.
2. Visualizza le unità di condivisione dati. Ad esempio:

```
show datashares;
```

```
share_name share_owner source_database consumer_database share_type createdate  
is_publicaccessible share_acl producer_account producer_namespace  
test_datashare 100 db_producer NULL OUTBOUND 2/15/2022 FALSE admin  
123456789012 p1234567-8765-4321-p10987654321
```

## Creazione del database consumatore

Nel cluster consumatore viene creato un database dall'unità di condivisione dati. Questa procedura descrive come condividere dati tra due cluster nello stesso account. Per informazioni sulla condivisione dei dati tra AWS account, consulta [Condivisione dei dati tra AWS account](#) nella Amazon Redshift Database Developer Guide.

Puoi utilizzare i comandi SQL o il pannello con visualizzazione ad albero dell'editor di query v2 per creare il database.

Per utilizzare SQL

1. Crea un database dall'unità di condivisione dati per l'account e lo spazio dei nomi del cluster produttore. Ad esempio:

```
create database share_db from datashare mysource of account '123456789012'  
namespace 'p1234567-8765-4321-p10987654321';
```

2. Imposta le autorizzazioni in modo che gli utenti possano accedere al database e allo schema. Ad esempio:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

Per utilizzare il pannello con visualizzazione ad albero dell'editor di query v2

1. Scegliere



quindi scegliere Database.

2. Inserire un Nome database.
3. (Facoltativo) Seleziona Utenti e gruppi e scegli un Utente del database.
4. Scegli Create using a datashare (Crea utilizzando un'unità di condivisione dati).
5. Scegli l'unità di condivisione dati.
6. Scegliere Crea database.

Il nuovo database



di condivisione di dati viene visualizzato nel pannello con visualizzazione ad albero dell'editor di query v2.

7. Imposta le autorizzazioni in modo che gli utenti possano accedere al database e allo schema. Ad esempio:

```
grant usage on database share_db to usernames;
```

```
grant usage on schema public to usernames;
```

## Esecuzione di query sugli oggetti dell'unità di condivisione dati

Nel cluster consumatore puoi eseguire query sugli oggetti dell'unità di condivisione dati utilizzando nomi oggetto completi espressi con la notazione in tre parti: nome del database, schema e nome dell'oggetto.

1. Nel pannello con visualizzazione ad albero dell'editor di query v2, scegli lo schema.
2. Per visualizzare una definizione di tabella, scegliere una tabella.

Vengono visualizzati le colonne e i tipi di dati della tabella.

3. Per eseguire query in una tabella, selezionare la tabella e utilizzare il menu contestuale (pulsante destro del mouse) per selezionare Select table (Seleziona tabella).

4. Esegui query sulle tabelle utilizzando i comandi SELECT. Ad esempio:

```
select top 10 * from test_db.public.event;
```

## Pianificazione di una query con l'editor di query v2

Puoi creare una pianificazione per eseguire un'istruzione SQL con l'editor di query Amazon Redshift v2. Puoi creare una pianificazione per eseguire l'istruzione SQL in base agli intervalli di tempo che corrispondono alle esigenze aziendali. Al momento dell'esecuzione della query pianificata, la query viene avviata da Amazon EventBridge e utilizza l'API Amazon Redshift Data.

Come creare una pianificazione per eseguire un'istruzione SQL

1. Nella



vista

creare una pianificazione per eseguire un'istruzione SQL.

2. Quando definisci la pianificazione, è necessario fornire le informazioni riportate di seguito.

- Il ruolo IAM che assume le autorizzazioni necessarie per eseguire la query. Questo ruolo IAM è anche associato al tuo cluster o gruppo di lavoro.
- I valori di autenticazione per una delle due credenziali AWS Secrets Manager o temporanee per autorizzare l'accesso al cluster o al gruppo di lavoro. Questi metodi di autenticazione sono supportati dall'API Data. Per ulteriori informazioni, consulta [Autenticazione di una query pianificata](#).
- Il cluster o il gruppo di lavoro in cui risiede il database.
- Il nome della tabella del database che contiene i dati su cui eseguire la query.
- Il nome della query pianificata e la relativa descrizione. L'editor di query v2 aggiunge un prefisso "QS2-" al nome delle query pianificate. L'editor di query v1 aggiunge un prefisso "QS" al nome delle query pianificate.
- L'istruzione SQL da eseguire sulla pianificazione.
- La frequenza di pianificazione e le opzioni di ripetizione o un valore formattato cron che definisce la pianificazione. Per ulteriori informazioni, consulta [Cron Expressions](#) nella Amazon CloudWatch Events User Guide.

- Facoltativamente, è possibile abilitare le notifiche standard di Amazon SNS per monitorare la query pianificata. Potrebbe essere necessario confermare l'indirizzo e-mail fornito alla notifica Amazon SNS. Controlla la tua e-mail per trovare un collegamento per confermare l'indirizzo e-mail per la notifica Amazon SNS. Per ulteriori informazioni, consulta [Notifiche e-mail](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service. Se la tua query è in esecuzione ma non vedi i messaggi pubblicati nel tuo argomento SNS, consulta [La mia regola viene eseguita, ma non vedo alcun messaggio pubblicato nel mio argomento Amazon SNS nella Amazon User Guide EventBridge](#).
3. Scegli Pianifica query per salvare e attivare la pianificazione e aggiungere la pianificazione all'elenco delle query nella vista Query pianificate.

La

vista 

pianificate elenca tutte le query pianificate per i cluster e i gruppi di lavoro. Con questa vista, è possibile visualizzare i dettagli delle query pianificate, attivare o disattivare la pianificazione, modificarla ed eliminare la query pianificata. Quando si visualizzano i dettagli della query, è anche possibile visualizzare la cronologia dell'esecuzione della query con la pianificazione.

#### Note

L'esecuzione di una query di pianificazione è disponibile solo nell'elenco Cronologia della pianificazione per 24 ore. Le query eseguite in base a una pianificazione non vengono visualizzate nella vista Cronologia delle query dell'editor di query v2

## Impostazione delle autorizzazioni per pianificare una query

Per pianificare le query, l'utente AWS Identity and Access Management (IAM) che definisce la pianificazione e il ruolo IAM associato alla pianificazione deve essere configurato con le autorizzazioni IAM per utilizzare Amazon EventBridge e Amazon Redshift Data API. Per ricevere e-mail da query pianificate, è necessario configurare anche la notifica Amazon SNS che viene specificata facoltativamente.

Di seguito vengono descritte le attività necessarie per utilizzare le policy AWS gestite per fornire le autorizzazioni, ma a seconda dell'ambiente in uso, potresti voler definire le autorizzazioni consentite.

Per l'utente IAM che ha effettuato l'accesso all'editor di query v2, modifica l'utente IAM utilizzando la console IAM (<https://console.aws.amazon.com/iam/>).

- Oltre alle autorizzazioni per eseguire le operazioni di Amazon Redshift e Query Editor v2, collega le policy AmazonRedshiftDataFullAccess AWS e AmazonEventBridgeFullAccess le policy gestite a un utente IAM.
- In alternativa, assegna le autorizzazioni a un ruolo e assegna il ruolo all'utente.

Collega una policy che conceda l'autorizzazione `sts:AssumeRole` all'ARN della risorsa del ruolo IAM specificato al momento della definizione della query pianificata. Per ulteriori informazioni sull'assunzione dei ruoli, consulta [Concessione di autorizzazioni utente per cambiare ruoli](#) nella Guida per l'utente IAM.

L'esempio seguente mostra una policy di autorizzazione che assume il ruolo IAM `myRedshiftRole` nell'account `123456789012`. Questo è anche il ruolo IAM `myRedshiftRole` collegato al cluster o al gruppo di lavoro quando viene eseguita la query pianificata.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": [
        "arn:aws:iam::123456789012:role/myRedshiftRole"
      ]
    }
  ]
}
```

Aggiorna la politica di affidabilità del ruolo IAM utilizzata per pianificare la query per consentire all'utente IAM di assumerla.

```
{
  "Sid": "AssumeRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::123456789012:user/myIAMUsername"
  }
}
```

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

Per il ruolo IAM specificato per consentire l'esecuzione della query pianificata, modifica il ruolo IAM utilizzando la console IAM (<https://console.aws.amazon.com/iam/>).

- Collega le policy `AmazonRedshiftDataFullAccess` e le policy `AmazonEventBridgeFullAccess` AWS gestite al ruolo IAM. La politica gestita `AmazonRedshiftDataFullAccess` consente solo l'autorizzazione `redshift-serverless:GetCredentials` per i gruppi di lavoro Redshift Serverless contrassegnati con la chiave `RedshiftDataFullAccess`.

## Autenticazione di una query pianificata

Quando si pianifica una query, è possibile utilizzare uno dei seguenti metodi di autenticazione durante l'esecuzione di SQL. Ogni metodo richiede una diversa combinazione di input nell'editor di query v2. Questi metodi di autenticazione sono supportati dall'API dei dati utilizzata per eseguire le istruzioni SQL.

L'utente o il ruolo del database utilizzato per eseguire la query deve disporre dei privilegi di database necessari. Ad esempio, per concedere a `IAMR:MyRedshiftQEv2Scheduler` i privilegi alla tabella `mytable`, esegui il seguente comando SQL.

```
GRANT all ON TABLE mytable TO "IAMR:MyRedshiftQEv2Scheduler";
```

Per visualizzare l'elenco degli utenti del database nel cluster o nel gruppo di lavoro, interroga la vista del sistema `PG_USER_INFO`.

### Note

Qualsiasi gruppo di lavoro Redshift Serverless per il quale si pianificano le interrogazioni deve essere contrassegnato con la chiave `RedshiftDataFullAccess`. Per ulteriori informazioni, consulta [Autorizzazione di accesso all'API dati di Amazon Redshift](#).

In alternativa all'etichettatura del gruppo di lavoro, puoi aggiungere una policy in linea al ruolo IAM (specificata nella pianificazione) che consenta `redshift-serverless:GetCredentials`. Per esempio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllServerlessWorkgroups",
      "Effect": "Allow",
      "Action": "redshift-serverless:GetCredentials",
      "Resource": [
        "arn:aws:redshift-serverless:*:*:workgroup/*"
      ]
    }
  ]
}
```

## AWS Secrets Manager

Con questo metodo, fornire il valore del segreto per `secret-arn` archiviato in AWS Secrets Manager. Questo segreto contiene le credenziali per la connessione al database. Potresti aver creato un segreto con le credenziali corrette quando hai creato il cluster o il gruppo di lavoro. Il segreto deve essere taggato con la chiave `RedshiftDataFullAccess`. Se la chiave del tag non è già presente, usa la AWS Secrets Manager console per aggiungerla. Per informazioni sulla creazione di un segreto, consulta [Creazione di un segreto per le credenziali di connessione al database](#).

Per ulteriori informazioni sulle autorizzazioni minime, consultare [Creazione e gestione di segreti con AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager .

## Credenziali temporanee

Quando ti connetti a un database in un cluster con questo metodo, fornisci i valori per Nome del database e Utente del database. Quando ti connetti a un database in un gruppo di lavoro, fornisci solo il Nome del database.

Quando ci si connette a un cluster, la policy `AmazonRedshiftDataFullAccess` consente all'utente del database denominato `oredshift_data_api_user` l'autorizzazione

per `redshift:GetClusterCredentials`. Se desideri utilizzare un diverso utente di database per eseguire l'istruzione SQL, aggiungi una policy al ruolo IAM collegato al cluster per consentire `redshift:GetClusterCredentials`. La seguente policy di esempio consente gli utenti del database `awsuser` e `myuser`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}
```

## Impostazione delle autorizzazioni per vedere la cronologia delle pianificazioni delle query

Per consentire agli utenti di visualizzare la cronologia delle pianificazioni, modifica il ruolo IAM (specificato con la pianificazione) Relazioni di trust per aggiungere le autorizzazioni.

Quello che segue è un esempio di una policy di attendibilità in un ruolo IAM che consente all'utente IAM *myIAMusername* di visualizzare la cronologia della pianificazione delle query. Invece di consentire a un utente IAM l'autorizzazione `sts:AssumeRole`, puoi scegliere per concedere questa autorizzazione a un ruolo IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.amazonaws.com",

```

```

        "redshift-serverless.amazonaws.com"
    ],
    },
    "Action": "sts:AssumeRole"
},
{
    "Effect": "Allow",
    "Principal": {
        "Service": "events.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
},
{
    "Sid": "AssumeRole",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/myIAMUsername"
    },
    "Action": "sts:AssumeRole"
}
]
}

```

## Monitoraggio della query pianificata

Per l'argomento Amazon SNS che specifichi per l'invio di notifiche e-mail, crea l'argomento Amazon SNS utilizzando l'editor di query v2 accedendo alla sezione Notifiche SNS, Attiva il monitoraggio e crea l'argomento con Crea argomento SNS. L'editor di query v2 crea l'argomento Amazon SNS e aggiunge un service principal alla policy di accesso per Amazon. EventBridge Di seguito è riportato un esempiodi Policy di accesso creata nell'argomento Amazon SNS. Nell'esempio, vengono utilizzati l'argomento Regione AWS *us-west-2*, Account AWS *123456789012* e Amazon SNS. *select-version-pdx-testunload*

```

{
  "Version": "2008-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "Allow_Publish_Events",
      "Effect": "Allow",
      "Principal": {
        "Service": "events.amazonaws.com"
      }
    }
  ]
}

```

```

    },
    "Action": "sns:Publish",
    "Resource": "arn:aws:sns:us-west-2:123456789012:select-version-pdx-testunload"
  }
]
}

```

Quando viene eseguita la query pianificata, Amazon SNS invia e-mail di AWS notifica. *L'esempio seguente mostra un'e-mail inviata a myemail@example.com per la query pianificata QS2-may25a eseguita su Regione AWS eu-north-1 in Account AWS 123456789012 utilizzando l'argomento di notifica di Amazon SNS May25a-SNS.*

```

{"version":"0","id":"8e4323ec-5258-7138-181b-91290e30ff9b","detail-type":"Scheduled
Event","source":"aws.events","account":"123456789012","time":"2023-05-25T15:22:00Z",
  "region":"eu-north-1","resources":["arn:aws:events:eu-
north-1:123456789012:rule/QS2-may25a"],"detail":{}}

```

```

--
If you wish to stop receiving notifications from this topic, please click or visit the
link below to unsubscribe:
https://sns.eu-north-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:eu-
north-1:123456789012:may25a-SNS:0c1a3d05-39c2-4507-
bc3d-47250513d7b0&Endpoint=myemail@example.com

```

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

## Risoluzione dei problemi relativi alla configurazione della pianificazione di una query

Considera quanto segue se hai problemi con la pianificazione di una query.

### Query non in esecuzione

Verifica se il ruolo IAM utilizzato nella pianificazione è autorizzato a ottenere le credenziali temporanee del cluster. L'autorizzazione per i cluster forniti è `redshift:GetClusterCredentialsWithIAM`. L'autorizzazione per i gruppi di lavoro Redshift Serverless è `redshift-serverless:GetCredentials`.

### La cronologia pianificata non viene visualizzata

L'utente IAM o il ruolo IAM utilizzato per accedere alla AWS console non è stato aggiunto alla policy di attendibilità del ruolo IAM utilizzato per pianificare la query.

Quando si utilizza AWS Secrets Manager per la connessione della query pianificata, conferma che il segreto sia contrassegnato con la chiave `RedshiftDataFullAccess`.

Se la query pianificata utilizza una AWS Secrets Manager connessione, al ruolo IAM utilizzato per pianificare la query deve essere `SecretsManagerReadWrite` associata l'equivalente di una policy gestita al ruolo.

Lo stato della cronologia delle query è **Failed**

Visualizza la vista del sistema `SYS_QUERY_HISTORY` per i dettagli sul motivo per cui la query non è riuscita. Un problema comune è che l'utente o il ruolo del database utilizzato per eseguire la query potrebbe non disporre dei privilegi necessari per eseguire l'SQL. Per ulteriori informazioni, consulta [Autenticazione di una query pianificata](#).

Il seguente codice SQL interroga la vista `SYS_QUERY_HISTORY` per restituire query non riuscite.

```
SELECT user_id, query_id, transaction_id, session_id, database_name, query_type,
       status, error_message, query_text
FROM sys_query_history
WHERE status = 'failed';
```

Per scoprire i dettagli di una specifica interrogazione pianificata con esito negativo, vedere [Ricerca di dettagli sulle query pianificate con AWS CloudShell](#).

## Ricerca di dettagli sulle query pianificate con AWS CloudShell

Puoi utilizzarlo AWS CloudShell per scoprire i dettagli di una richiesta pianificata. È necessario disporre delle autorizzazioni appropriate per eseguire i AWS CLI comandi illustrati nella procedura seguente.

Per visualizzare i risultati di una query pianificata

1. Sulla AWS console, aprire il prompt dei AWS CloudShell comandi. Per ulteriori informazioni AWS CloudShell, consulta [Cosa c'è AWS CloudShell](#) nella Guida per l'AWS CloudShell utente.
2. Assumi il ruolo IAM della query pianificata. Per assumere il ruolo, trova il ruolo IAM associato alla query pianificata nell'editor di query v2 e utilizzalo nel AWS CLI comando in AWS CloudShell. Ad esempio, per il ruolo `scheduler` inserisci un AWS STS comando per assumere il ruolo utilizzato dalla query pianificata.

```
aws sts assume-role --role-arn "arn:aws:iam::123456789012:role/scheduler" --role-session-name "scheduler-test"
```

Le credenziali restituite sono simili alle seguenti.

```
"Credentials": {
  "AccessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "SecretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY",
  "SessionToken": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...",
  "Expiration": "2023-08-18T18:19:44+00:00"
},
"AssumedRoleUser": {
  "AssumedRoleId": "AROA35B2NH6WBTP70NL4E:scheduler-test",
  "Arn": "arn:aws:sts::123456789012:assumed-role/scheduler/scheduler-test"
}
}
```

3. Crea variabili ambientali AWS CLI utilizzando le credenziali visualizzate assumendo il ruolo IAM. È necessario utilizzare questi token prima della loro scadenza. Ad esempio, inserisci quanto segue in AWS CloudShell

```
export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY
export AWS_SESSION_TOKEN=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY...
```

4. Per visualizzare l'errore di una query non riuscita, eseguite il AWS CLI comando per descrivere un'istruzione. L'id dell'istruzione SQL proviene dall'ID mostrato nella sezione Cronologia della pianificazione di una query pianificata nell'editor di query v2.

```
aws redshift-data describe-statement --id 130d2620-05d2-439c-b7cf-815d9767f513
```

In questo esempio, l'SQL pianificato `select * from users limit 100` genera un errore SQL che la tabella `users` non esiste.

```
{
  "CreatedAt": "2023-08-18T17:39:15.563000+00:00",
  "Duration": -1,
  "Error": "ERROR: relation \"users\" does not exist",
  "HasResultSet": false,
}
```

```
"Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"QueryString": "select * from users limit 100\n-RequestID=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222; TraceID=1-633c5642-4039308d03f3a0ba53dbdf6f",
"RedshiftPid": 1073766651,
"RedshiftQueryId": 0,
"ResultRows": -1,
"ResultSize": -1,
"Status": "FAILED",
"UpdatedAt": "2023-08-18T17:39:16.116000+00:00",
"WorkgroupName": "default"
}
```

## Demo della pianificazione di una query

Per una demo della pianificazione di una query, guarda il video seguente: [Video demo of scheduling a query](#).

## Visualizzazione dei risultati delle query

Dopo aver eseguito una query e aver visualizzato i risultati, è possibile abilitare l'opzione Chart (Grafico) per ottenere una visualizzazione grafica della pagina dei risultati attuale. Per definire il contenuto, la struttura e l'aspetto del grafico è possibile utilizzare i seguenti controlli:



### Traccia

Rappresenta un insieme di indicatori grafici correlati in un grafico. In un grafico è possibile definire più tracce.

### Type

È possibile definire il tipo di traccia per rappresentare i dati come uno dei seguenti:

- Grafico a dispersione per un grafico a dispersione o un grafico a bolle.
- Grafico a barre per rappresentare categorie di dati con barre verticali o orizzontali.
- Grafico ad aree per definire le aree riempite.
- Istogramma che utilizza le barre per rappresentare la distribuzione della frequenza.
- Grafico a torta per una rappresentazione circolare di dati in cui ogni sezione rappresenta una percentuale dell'intero.

- Grafico a imbuto o ad area di imbuto per rappresentare i dati attraverso varie fasi di un processo.
- Grafico OHLC (open-high-low-close) spesso utilizzato per i dati finanziari per rappresentare valori aperti, elevati, bassi e chiusi lungo l'asse x, che di solito rappresenta intervalli di tempo.
- Grafico a candela per rappresentare un intervallo di valori per una categoria su una linea temporale.
- Grafico a cascata per rappresentare il modo in cui un valore iniziale aumenta o diminuisce attraverso una serie di valori intermedi. I valori possono rappresentare intervalli di tempo o categorie.
- Grafico a linee per rappresentare le variazioni di valore nel tempo.

### Asse X

Specificare una colonna di tabella che contiene valori da tracciare lungo l'asse X. Le colonne che contengono valori descrittivi rappresentano solitamente dati dimensionali. Le colonne che contengono valori quantitativi di solito rappresentano dati di fatto.

### Asse Y

Specificare una colonna di tabella che contiene valori da tracciare lungo l'asse Y. Le colonne che contengono valori descrittivi rappresentano solitamente dati dimensionali. Le colonne che contengono valori quantitativi di solito rappresentano dati di fatto.

### Grafici secondari

È possibile definire presentazioni aggiuntive dei dati del grafico.

### Trasformazioni

È possibile definire le trasformazioni per filtrare i dati di traccia. Utilizzare una trasformazione di suddivisione per visualizzare più tracce da una singola traccia sorgente. Utilizzare una trasformazione aggregata per presentare una traccia come media o minima. Utilizzare una trasformazione di ordinamento per ordinare una traccia.

### Aspetto generale

È possibile impostare i valori di default per il colore di sfondo, il colore dei margini, le scale di colore per progettare tavolozze, stile e dimensioni del testo, stile e dimensione del titolo e barra delle modalità. È possibile definire interazioni per trascinarsi, clic e passaggio del mouse. È possibile definire il metatesto. È possibile definire gli aspetti di default per tracce, assi, legende e annotazioni.

Scegliere Tracce per visualizzare i risultati come grafico. Per Tipo, scegliere lo stile del grafico come Barra, Linea e così via. Per Orientamento, è possibile scegliere Verticale o Orizzontale. Per X, scegliere la colonna della tabella che si desidera utilizzare per l'asse orizzontale. Per Y, scegliere la colonna della tabella che si desidera utilizzare per l'asse verticale.

Per aggiornare la visualizzazione del grafico, scegliere Aggiorna. Scegliere schermo intero per espandere la visualizzazione del grafico.

Per creare un grafico

1. Esegui una query e ottieni risultati.
2. Attivare Grafici.
3. Scegliere Traccia e iniziare a visualizzare i dati.
4. Scegliere uno stile di grafico tra i seguenti:
  - Dispersione
  - Barra
  - Area
  - Istogramma
  - Torta
  - Imbutto
  - Area imbuto
  - OHLC (aperto, alto, basso, chiuso)
  - Candelabro
  - Cascata
  - Line (Linea)
5. Scegliere Stile per personalizzare l'aspetto, inclusi i colori, gli assi, la legenda e le annotazioni. È possibile aggiungere testo, forme e immagini.
6. Scegliere Annotazioni per aggiungere testo, forme e immagini.

Per salvare un grafico

1. Scegliere Salva chart.
2. Inserire un nome per il grafico.
3. Selezionare Salva.

## Per esportare un grafico

1. Scegli Export (Esporta).
2. Scegliere PNG o JPEG.
3. Impostare la larghezza e l'altezza del grafico.
4. Scegli Export (Esporta).
5. Scegliere di aprire il file nell'applicazione grafica predefinita oppure salvare il file con il nome predefinito.

## Per cercare e aprire un grafico salvato

1. Selezionare la scheda Grafici.
2. Apri il grafico che desideri.

## Per organizzare i grafici in cartelle

1. Scegli Grafici dal pannello di navigazione.
2. Scegliere Nuova cartella e dare un nome alla cartella.
3. Scegliere Crea per creare la cartella nella scheda Grafici.

Puoi spostare i grafici dentro e fuori dalla cartella utilizzando drag-and-drop.

## Esempio: crea un grafico a torta per visualizzare i risultati delle query

L'esempio seguente utilizza la tabella Vendite dal database di esempio. Per ulteriori informazioni, consultare [Database di esempio](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Di seguito è riportata la query eseguita per fornire i dati per il grafico a torta.

```
select top 5 eventname, count(salesid) totalorders, sum(pricepaid) totalsales
from sales, event
where sales.eventid=event.eventid group by eventname
order by 3;
```

## Per creare un grafico a torta per l'evento principale in base alle vendite totali

1. Eseguire la query.

2. Nell'area dei risultati della query, attivare Grafico.
3. Scegli Traccia.
4. Per Tipo, scegli Torta.
5. Per Valori, scegli venditetotali.
6. Per Etichette, scegli nomeevento.
7. Scegliere Stile e poi Generale.
8. In Scalecolori, scegliere Categorici e poi Pastello2.



## Esempio: creazione di un grafico combinato per il confronto di entrate e vendite

Esegui la procedura descritta in questo esempio per creare un grafico che combina un grafico a barre per i dati delle entrate e un grafico a linee per i dati di vendita. Nell'esempio seguente viene utilizzata la tabella Sales (Vendite) del database di esempio tickit. Per ulteriori informazioni, consultare [Database di esempio](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Di seguito è riportata la query eseguita per fornire i dati per il grafico.

```
select eventname, total_price, total_qty_sold
from (select eventid, total_price, total_qty_sold, ntile(1000) over(order by
total_price desc) as percentile
      from (select eventid, sum(pricepaid) total_price, sum(qtysold) total_qty_sold
            from tickit.sales
            group by eventid)) Q, tickit.event E
where Q.eventid = E.eventid
and percentile = 1
order by total_price desc;
```

## Creazione di un grafico combinato per il confronto di entrate e vendite

1. Eseguire la query.
2. Nell'area dei risultati della query, attivare Grafico.
3. In trace o, per Type (Tipo), scegli Bar (A barre).
4. Per X, scegli eventname.
5. Per Y, scegli total\_price.

Il grafico a barre viene visualizzato con i nomi degli eventi lungo l'asse X.

6. In Style (Stile), scegli Traces (Tracce).
7. Per Name (Nome), inserisci Revenue (Fatturato).
8. In Style (Stile), scegliere Axes (Assi).
9. Per Titles (Titoli), scegli Y e inserisci Revenue (Fatturato).

L'etichetta Revenue (Fatturato) viene visualizzata sull'asse Y sinistro.

10. In Structure (Struttura), scegli Traces (Tracce).
11. Scegliere



Traccia.

Vengono visualizzate le opzioni di traccia 1.

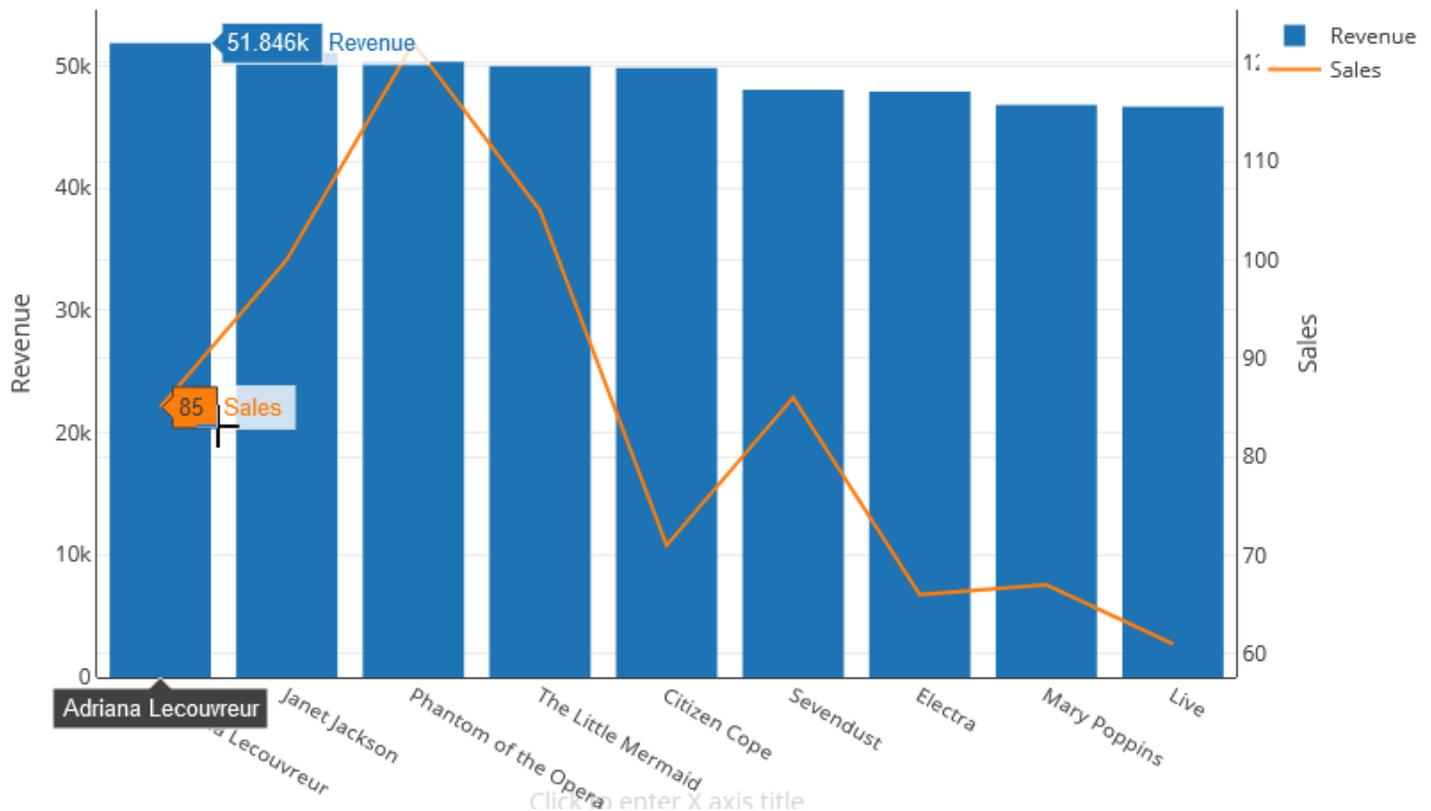
12. Per Type (Tipo), scegliere Line (A linee).
13. Per X, scegli eventname.
14. Per Y, scegli total\_qty\_sold.
15. In Axes To Use (Asse da utilizzare), per Y Axis (Asse Y) scegli



Y Axis (Asse Y) visualizza Y2.

16. In Style (Stile), scegliere Axes (Assi).
17. In Titles (Titoli), scegli Y2.
18. Per Name (Nome), immettere Sales (Vendite).
19. In Lines (Linee), scegli Y:Sales.
20. In Axis Line (Linea asse), scegli Show (Mostra) e per Position (Posizione), scegli Right (Destra).

## Revenue and Sales



## Demo: creazione di visualizzazioni con l'editor di query Amazon Redshift v2

Per una dimostrazione di come creare le visualizzazioni, guardare il video seguente. [Creazione di visualizzazioni con l'editor di query Amazon Redshift v2.](#)

## Collaborazione e condivisione come team

Puoi condividere query con il team.

Per un insieme di utenti che collaborano e condividono risorse dell'editor di query v2 viene definito un team. Un amministratore può creare un team aggiungendo un tag a un ruolo IAM. Per ulteriori informazioni, consulta [Autorizzazioni necessarie per utilizzare l'editor della query v2.](#)

## Salvataggio, ricerca ed eliminazione di query

Prima di poter condividere la query con il tuo team, salvala. È possibile visualizzare ed eliminare le query salvate.

## Per salvare una query

1. Preparare la query e scegliere Salva.
2. Inserisci un titolo per la query.
3. Selezionare Salva.

## Per cercare le query salvate

1. Scegliere Query dal pannello di navigazione.
2. È possibile visualizzare le query che sono Le mie query, Condivise da me oppure Condivise con il mio team. Queste query possono essere visualizzate come singole query o all'interno di cartelle create.

## Per eliminare una query salvata

1. Aprire il menu contestuale (tasto destro del mouse) per una query salvata.
2. Scegliere Elimina e confermare l'operazione.

## Per organizzare le query salvate in cartelle

1. Scegliere Query dal pannello di navigazione.
2. Scegliere Nuova cartella e dare un nome alla cartella.
3. Scegliere Crea per creare la cartella nella scheda Query.

È ora possibile spostare le interrogazioni dentro e fuori dalla cartella utilizzando drag-and-drop.

## Condivisione di una query

Puoi condividere query con il team. È inoltre possibile visualizzare la cronologia delle query salvate e gestire le versioni delle query.

Per condividere una query con il team, assicurati di disporre del tag principale `sqlworkbench-team` imposta lo stesso valore del resto dei membri del tuo team nel tuo account. Ad esempio, un amministratore potrebbe impostare il valore su `accounting-team` per tutti nel reparto contabilità. Per vedere un esempio, consulta [Autorizzazioni necessarie per utilizzare l'editor della query v2](#).

## Per condividere una query con un team

1. Scegliere Query dal pannello di navigazione.
2. Aprire il menu contestuale (clic con il pulsante destro del mouse) della query che si desidera condividere e scegliere Condividi con il mio team.
3. Scegliere il team o i team con cui si desidera condividere la query, quindi scegliere Opzioni di condivisione del salvataggio.

Ogni volta che si salva una query SQL, l'editor di query v2 la salva come nuova versione. È possibile cercare le versioni precedenti di query, salvare una copia di una query o ripristinare una query.

## Per gestire le versioni delle query

1. Scegliere Query dal pannello di navigazione.
2. Aprire il menu contestuale (tasto destro del mouse) per la query con cui si desidera lavorare.
3. Scegliere Cronologia delle versioni per aprire un elenco di versioni della query.
4. Nella pagina Cronologia delle versioni, puoi eseguire queste operazioni:
  - Ripristina versione selezionata — Torna alla versione selezionata e continua il tuo lavoro con questa versione.
  - Salva selezionato come — Crea una nuova query nell'editor.

## Esecuzione di query in un database con l'editor della query

L'uso dell'editor di query è la soluzione più semplice per eseguire query sui database ospitati dal cluster Amazon Redshift. Dopo aver creato il cluster, è possibile eseguire immediatamente le query con l'editor della query nella console Amazon Redshift.

### Note

Non puoi eseguire query sui dati in Amazon Redshift Serverless utilizzando questo editor di query originale. Utilizza invece l'editor di query v2 di Amazon Redshift.

Nel febbraio 2021 è stato implementato un editor di query aggiornato e i permessi di autorizzazione per utilizzare l'editor di query sono stati modificati. Il nuovo editor di query utilizza l'API dati di

Amazon Redshift Data per eseguire le query. La `AmazonRedshiftQueryEditor` policy, che è una policy AWS gestita AWS Identity and Access Management (IAM), è stata aggiornata per includere le autorizzazioni necessarie. Se si dispone di una policy IAM personalizzata, assicurarsi di aggiornarla. Utilizzare `AmazonRedshiftQueryEditor` come guida. Queste modifiche a `AmazonRedshiftQueryEditor` includono:

- L'autorizzazione per gestire i risultati delle istruzioni dell'editor di query richiede l'utente proprietario dell'istruzione.
- È stata aggiunta l'autorizzazione per utilizzare Secrets Manager per la connessione a un database.

Per ulteriori informazioni, consultare [Autorizzazioni richieste per utilizzare l'editor di query della console Amazon Redshift](#).

Quando ci si connette al cluster dal nuovo editor di query, è possibile utilizzare uno dei due metodi di autenticazione, come descritto in [Connessione con l'editor di query](#).

Con l'editor della query puoi:

- Eseguire query singole su istruzioni SQL.
- Scaricare set di risultati fino a 100 MB in un file CSV.
- Salvare le query per riutilizzarle. Non è possibile salvare le query nelle regioni Europa (Parigi), Asia Pacifico (Osaka), Asia Pacifico (Hong Kong) o Medio Oriente (Bahrein).
- Visualizzare i dettagli di runtime delle query per le tabelle definite dall'utente.
- Pianificare le query da eseguire in un secondo momento.
- Visualizzare una cronologia delle query create nell'editor di query.
- Eseguire le query sui cluster utilizzando il routing VPC avanzato.

## Considerazioni sull'editor della query

Se si utilizza l'editor di query, tenere in considerazione quanto riportato di seguito:

- La durata massima di una query è 24 ore.
- La dimensione massima dei risultati della query è 100 MB. Se la chiamata restituisce più di 100 MB di dati di risposta, verrà terminata.
- Il tempo massimo di conservazione dei risultati delle query è 24 ore.
- La dimensione massima dell'istruzione della query è 100 KB.

- Il cluster deve trovarsi in un Virtual Private Cloud (VPC) basato sul servizio Amazon VPC.
- Nell'editor della query non puoi utilizzare le transazioni. Per ulteriori informazioni sulle transazioni, consultare [BEGIN](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- È possibile salvare una query contenente fino a 3.000 caratteri.

## Abilitazione dell'accesso all'editor della query

Per accedere all'editor della query, sono necessarie le opportune autorizzazioni. Per abilitare l'accesso, ti consigliamo di collegare le policy `AmazonRedshiftQueryEditor` e le policy `AmazonRedshiftReadOnlyAccess` AWS gestite per le autorizzazioni IAM al ruolo IAM che utilizzi per accedere al tuo cluster. Quindi assegna il ruolo a un utente. Per collegare le policy IAM è possibile utilizzare la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>. Per ulteriori informazioni, consulta [Utilizzo di policy basate su identità \(policy IAM\) per Amazon Redshift](#).

Se hai già creato un utente per accedere ad Amazon Redshift, puoi allegare `AmazonRedshiftQueryEditor` le policy `AmazonRedshiftReadOnlyAccess` AWS gestite a quell'utente tramite un ruolo assegnato. Se ancora non hai creato un utente, creane uno e collega la policy al ruolo IAM, quindi assegna il ruolo all'utente.

La policy AWS gestita `AmazonRedshiftQueryEditor` consente l'azione `redshift:GetClusterCredentials`, che per impostazione predefinita consente ai superutenti di accedere al database. Per limitare l'accesso, è possibile procedere in uno dei seguenti modi:

- Creare una policy personalizzata che consente di chiamare `redshift:GetClusterCredentials` e limita la risorsa a un determinato valore per `DbUser`.
- Aggiungi una policy che rifiuta l'autorizzazione a `redshift:GetClusterCredentials`. Qualsiasi utente a cui è stato assegnato un ruolo con questa autorizzazione collegata, deve accedere all'editor di query con le credenziali temporanee. Questa policy di rifiuto illustra un esempio.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "*"
  }
}
```

```
}
```

Per ulteriori informazioni sulla creazione di un ruolo con le autorizzazioni richieste, consulta [Crea un ruolo IAM con le autorizzazioni per la chiamata GetClusterCredentials](#).

Qualsiasi utente a cui è stato concesso l'accesso all'editor di query di Amazon Redshift tramite la policy AWS gestita `AmazonRedshiftQueryEditor` può elencare tutti i segreti. Tuttavia, questa policy consente la creazione e il recupero solo dei segreti con il tag della chiave `RedshiftQueryOwner` e il valore `${aws:userid}`. Se la chiave viene creata con l'Editor di query Amazon Redshift, il tag viene applicato automaticamente. Per utilizzare un segreto che non è stato creato con l'editor di query di Amazon Redshift, verificare che il segreto sia taggato con la chiave `RedshiftQueryOwner` e un valore dell'identificatore utente IAM univoco, ad esempio `AIDACKCEVSQ6C2EXAMPLE`.

Le autorizzazioni richieste per utilizzare l'editor `AmazonRedshiftQueryEditor` di query di Amazon Redshift sono `AmazonRedshiftReadOnlyAccess`

Per fornire l'accesso, aggiungi autorizzazioni ai tuoi utenti, gruppi o ruoli:

- Utenti e gruppi in: AWS IAM Identity Center

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center .

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creating a role for a third-party identity provider \(federation\)](#) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina [Creating a role for an IAM user](#) (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente di IAM.

## Connessione con l'editor di query

Quando ci si connette a un cluster con l'editor di query, utilizzare uno dei seguenti metodi di autenticazione. Ogni metodo richiede una combinazione diversa di input dalla console Amazon Redshift.

### AWS Secrets Manager

Con questo metodo, fornire il valore del segreto per secret-arn archiviato in AWS Secrets Manager. Questo segreto contiene le credenziali per la connessione al database.

### Credenziali temporanee

Con questo metodo, vengono forniti i propri valori database e db-user.

## Memorizzazione delle credenziali del database in AWS Secrets Manager

Quando si chiama l'editor di query, è possibile passare credenziali per il cluster utilizzando un segreto in AWS Secrets Manager. Per utilizzare questo metodo per passare le credenziali, specificare il nome del segreto o l'Amazon Resource Name (ARN) del segreto.

Per ulteriori informazioni sulle autorizzazioni minime, consultare [Creazione e gestione di segreti con AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager .

Come archiviare le credenziali in un segreto per un cluster Amazon Redshift

1. Consente AWS Secrets Manager di creare un segreto che contenga le credenziali per il cluster. Quando si sceglie Archivia un nuovo segreto, selezionare Credenziali per il cluster Redshift. Archiviare un valore per Nome utente (utente del database), Password e Cluster database (identificatore del cluster) nel segreto.

Per le istruzioni, consultare [Creazione di un segreto di base](#) nella Guida per l'utente di AWS Secrets Manager .

2. Usa la AWS Secrets Manager console per visualizzare i dettagli del segreto che hai creato o esegui il `aws secretsmanager describe-secret` AWS CLI comando.

Se hai scelto di utilizzare le credenziali di amministratore del cluster AWS Secrets Manager, puoi connetterti al database utilizzando le credenziali di amministratore archiviate da Secrets Manager.

## Utilizzo dell'editor della query

Nell'esempio seguente utilizzi l'editor della query per le seguenti attività:

- Eseguire comandi SQL.
- Visualizzare i dettagli di esecuzione delle query.
- Salvare una query.
- Scaricare un set di risultati di una query.

Per completare l'esempio seguente è necessario un cluster Amazon Redshift esistente. Se non disponi di un cluster, creane uno seguendo la procedura descritta in [Creazione di un cluster](#).

Come utilizzare l'editor di query nella console Amazon Redshift

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Query editor (Editor di query), quindi collegarsi a un database nel cluster.
3. In Schema, scegli public (pubblico) per creare una nuova tabella in base allo schema.
4. Immetti quanto segue nella finestra dell'editor della query, e scegli Run (Esegui) per creare una nuova tabella.

```
create table shoes(  
    shoetype varchar (10),  
    color varchar(10));
```

5. Scegli Clear (Cancella).
6. Immetti il comando seguente nella finestra dell'editor della query, quindi scegli Run query (Esegui query) per aggiungere righe alla tabella.

```
insert into shoes values  
( 'loafers', 'brown'),  
( 'sandals', 'black');
```

7. Scegli Clear (Cancella).
8. Immetti il comando seguente nella finestra dell'editor della query e scegli Run (Esegui) per eseguire una query sulla nuova tabella.

```
select * from shoes;
```

La voce Query results (Risultati della query) visualizza i risultati.

Tipo di calzatura	Colore
sandali	nero
mocassini	marrone

9. Scegli Execution (Esecuzione) per visualizzare i dettagli di esecuzione.
10. Scegli Data (Dati), quindi Export (Esporta) per scaricare i risultati della query sotto forma di file.

## Pianificazione di una query

### Important

L'editor di query Amazon Redshift v2 ora supporta la pianificazione di una query. Consigliamo di utilizzare l'editor di query v2. Per ulteriori informazioni, consulta [Pianificazione di una query con l'editor di query v2](#).

Per creare una pianificazione per l'esecuzione di un'istruzione SQL, è possibile utilizzare l'editor di query nella console Amazon Redshift. È possibile creare una pianificazione per eseguire l'istruzione SQL in base agli intervalli di tempo che corrispondono alle esigenze aziendali. Al momento dell'esecuzione della query pianificata, Amazon EventBridge avvia la query.

Come creare una pianificazione per eseguire un'istruzione SQL

1. Aprire la console e l'editor di query come descritto in [Utilizzo dell'editor della query](#). È possibile utilizzare questo editor di query solo con i cluster con provisioning.
2. Scegliere Pianificazione per creare una pianificazione per eseguire un'istruzione SQL.

Quando si definisce la pianificazione, è necessario fornire le informazioni riportate di seguito:

- Un ruolo IAM utilizzato per assumere le autorizzazioni necessarie per eseguire la query. Per ulteriori informazioni, consulta [Impostazione delle autorizzazioni per pianificare una query](#).

- I valori di autenticazione per una delle due credenziali AWS Secrets Manager o temporanee per autorizzare l'accesso al cluster. Per ulteriori informazioni, consulta [Autenticazione di una query pianificata](#).
- Il nome della query pianificata e una singola istruzione SQL da eseguire.
- La frequenza di pianificazione e le opzioni di ripetizione o un valore formattato cron.
- Facoltativamente, è possibile abilitare le notifiche Amazon SNS per monitorare la query pianificata. Se la tua query è in esecuzione ma non vedi messaggi pubblicati nel tuo argomento SNS, consulta [La mia regola viene attivata ma non vedo alcun messaggio pubblicato nel mio argomento Amazon SNS nella Amazon User Guide](#). EventBridge

È possibile gestire e aggiornare le query pianificate anche utilizzando la console Amazon Redshift. A seconda della versione della console, è possibile che le query pianificate siano elencate nelle seguenti posizioni:

- Nella scheda Pianificazioni della pagina dei dettagli del cluster.
- Nella scheda Query pianificate dell'editor di query.

Se si sceglie Nome della pianificazione da una di queste posizioni, sarà possibile visualizzare e modificare la definizione della query pianificata.

## Impostazione delle autorizzazioni per pianificare una query sulla console Amazon Redshift

Per pianificare le query, l'utente AWS Identity and Access Management (IAM) che definisce la pianificazione e il ruolo IAM associato alla pianificazione deve essere configurato come segue.

Per l'utente IAM connesso alla console Amazon Redshift, completare la seguente procedura:

- AmazonEventBridgeFullAccess AWS Associa la policy gestita a un ruolo IAM.
- Collegare una policy con l'autorizzazione `sts:AssumeRole` del ruolo IAM specificato al momento della definizione dell'istruzione SQL pianificata.

L'esempio seguente mostra una policy che assume un ruolo IAM specificato.

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

```

    {
      "Sid": "AssumeIAMRole",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::account-id:role/sql-statement-iam-role"
    }
  ]
}

```

Per il ruolo IAM specificato per consentire al pianificatore di eseguire una query, completare la seguente procedura:

- Assicurati che questo ruolo IAM specifichi il EventBridge service principal (`events.amazonaws.com`). Di seguito è riportato un esempio di relazione di attendibilità.

```

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

```

Per ulteriori informazioni su come creare un ruolo IAM per EventBridge gli eventi, consulta [Autorizzazioni necessarie per utilizzare lo scheduler di Amazon EventBridge](#).

- Allega la policy `AmazonRedshiftDataFullAccess` AWS gestita al ruolo IAM.
- Per consentire agli utenti di visualizzare la cronologia delle pianificazioni, modifica il ruolo IAM per aggiungere l'autorizzazione `sts:AssumeRole`.

Di seguito è riportato un esempio di policy di attendibilità in un ruolo IAM.

```

{

```

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

## Autenticazione di una query pianificata

Quando si pianifica una query, è possibile utilizzare uno dei seguenti metodi di autenticazione durante l'esecuzione della query SQL. Ogni metodo richiede una combinazione diversa di input dalla console Amazon Redshift.

### AWS Secrets Manager

Con questo metodo, fornire il valore del segreto per `secret-arn` archiviato in AWS Secrets Manager. Questo segreto contiene le credenziali per la connessione al database. Il segreto deve essere taggato con la chiave `RedshiftDataFullAccess`.

Per ulteriori informazioni sulle autorizzazioni minime, consultare [Creazione e gestione di segreti con AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager .

### Credenziali temporanee

Con questo metodo, vengono forniti i propri valori database e `db-user`.

La policy `AmazonRedshiftDataFullAccess` consente all'utente del database denominato `redshift_data_api_user` l'autorizzazione per `redshift:GetClusterCredentials`. Se si desidera utilizzare un utente di database diverso per eseguire l'istruzione SQL, aggiungere una policy al ruolo IAM per consentire `redshift:GetClusterCredentials`. La seguente policy di esempio consente gli utenti del database `awsuser` e `myuser`.

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

```

    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}

```

## Crea una EventBridge regola Amazon da eseguire al termine di una query

È possibile creare una regola evento per inviare una notifica al termine di una query. Per la procedura di utilizzo della EventBridge console Amazon, consulta la sezione [Creazione di EventBridge regole Amazon che reagiscono agli eventi](#) nella Amazon EventBridge User Guide. Per ulteriori informazioni sui modelli di eventi, consulta i [modelli di EventBridge eventi](#) di Amazon nella Amazon EventBridge User Guide.

Ad esempio, il seguente evento di esempio viene inviato quando una query è FINISHED.

```

{
  "version": "0",
  "id": "6a7e8feb-b491-4cf7-a9f1-bf3703467718",
  "detail-type": "Redshift Data Statement Status Change",
  "source": "aws.redshift-data",
  "account": "123456789012",
  "time": "2020-12-22T17:00:00Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:redshift:us-east-2:123456789:cluster:t1"
  ],
  "detail": {
    "statementId": "01bdaca2-8967-4e34-ae3f-41d9728d5644",
    "clusterId": "test-dataapi",
    "statementName": "awesome query",
    "state": "FINISHED",
    "pages": 5,
    "expireAt": "2020-12-22T18:43:48Z",
    "principal": "arn:aws:sts::123456789012:assumed-role/any",
    "queryId": 123456
  }
}

```

```
}  
}
```

È possibile creare una regola di pattern di eventi per filtrare l'evento.

```
{  
  "source": [  
    "aws.redshift-data"  
  ],  
  "detail-type": [  
    "Redshift Data Statement Status Change"  
  ],  
  "detail": {  
    "state": [  
      "FINISHED"  
    ]  
  }  
}
```

## Connessione a un data warehouse Amazon Redshift tramite strumenti client SQL

Puoi connetterti ai data warehouse Amazon Redshift dagli strumenti client SQL tramite connessioni Java Database Connectivity (JDBC), Python e Open Database Connectivity (ODBC). Amazon Redshift non fornisce né installa alcuna libreria o strumento client SQL. Per utilizzare questi strumenti o librerie per lavorare con i dati nei tuoi data warehouse, installali sul tuo computer client o sull'istanza Amazon EC2. Puoi usare la maggior parte degli strumenti del client SQL che supportano i driver JDBC, Python o ODBC.

Utilizza l'elenco delle sezioni alla fine di questo argomento per aiutarti a seguire il processo di configurazione del computer client o dell'istanza Amazon EC2 per l'utilizzo di una connessione JDBC, Python o ODBC. Gli argomenti illustrano anche le opzioni di sicurezza correlate per la connessione del client al server. In più, sono fornite informazioni sulla configurazione e la connessione da strumenti client SQL, come SQL Workbench/J, uno strumento di terze parti e [Amazon Redshift RSQL](#). Puoi provare questi strumenti se non disponi ancora di uno strumento di business intelligence da utilizzare. Puoi anche utilizzare questa sezione per scoprire come connetterti al tuo data warehouse in modo programmatico. Infine, se riscontri problemi durante il tentativo di connessione al tuo data warehouse, puoi consultare le informazioni sulla risoluzione dei problemi per identificare le soluzioni.

## Consigli per la connessione con gli strumenti client

Se ti connetti al tuo cluster Redshift utilizzando un indirizzo IP, possono verificarsi ulteriori tempi di inattività in caso di interruzione o perdita della connessione e il cluster viene portato online in una nuova zona di disponibilità (AZ). Tuttavia, se desideri comunque che la tua applicazione si connetta a Redshift utilizzando un indirizzo IP, usa l'indirizzo IP privato collegato all'endpoint del cluster ( virtual-private-cloud VPC). Puoi trovarlo nei dettagli del cluster in Rete e sicurezza, nella scheda Proprietà.

### Note

Se l'applicazione utilizza l'indirizzo IP del nodo leader per accedere al cluster Redshift, la best practice consigliata è cambiarlo per utilizzare l'URL dell'endpoint del cluster. Per ulteriori informazioni, consulta [Configurazione delle connessioni in Amazon Redshift](#).

### Argomenti

- [Configurazione delle connessioni in Amazon Redshift](#)
- [Configurazione delle opzioni di sicurezza per le connessioni](#)
- [Connessione da codice e strumenti client](#)
- [Connessione con SQL Workbench/J](#)
- [Connect al tuo data warehouse in modo programmatico](#)
- [Connettersi ad Amazon Redshift con un profilo di autenticazione.](#)
- [Risoluzione dei problemi di connessione in Amazon Redshift](#)

## Configurazione delle connessioni in Amazon Redshift

Nella sezione seguente scopri come configurare le connessioni JDBC, Python e ODBC per connetterti al cluster dagli strumenti client SQL. In questa sezione viene descritto come impostare le connessioni JDBC, Python e ODBC. Viene inoltre descritto come utilizzare i certificati SSL (Secure Sockets Layer) e server per crittografare le comunicazioni tra client e server.

### Driver JDBC, Python e ODBC per Amazon Redshift

Per utilizzare i dati nel cluster, sono richiesti i driver JDBC, Python o ODBC per stabilire la connettività dal computer client o dall'istanza. Codifica le tue applicazioni affinché usino operazioni

API di accesso ai dati JDBC, Python o ODBC e utilizza gli strumenti del client SQL che supportano JDBC, Python o ODBC.

Amazon Redshift permette di scaricare i driver JDBC, Python e ODBC. Questi driver sono supportati da AWS Support. I driver PostgreSQL non sono testati e non sono supportati dal team Amazon Redshift. Utilizza i driver specifici di Amazon Redshift quando ti connetti a un cluster Amazon Redshift. I driver Amazon Redshift presentano i seguenti vantaggi:

- Support per IAM, SSO e autenticazione federata.
- Support per i nuovi tipi di dati Amazon Redshift.
- Support per i profili di autenticazione.
- Prestazioni migliorate in combinazione con i miglioramenti di Amazon Redshift.

Per ulteriori informazioni su come scaricare i driver JDBC e ODBC e configurare le connessioni al cluster, consultare [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#), [Configurazione del connettore Python di Amazon Redshift](#) e [Configurazione di una connessione ODBC](#).

Per ulteriori informazioni sulla gestione delle identità IAM, comprese le best practice per i ruoli IAM, consulta [Identity and Access Management in Amazon Redshift](#).

### Ricerca della stringa di connessione al cluster

Per connetterti al cluster con il tuo strumento client SQL è richiesta la stringa di connessione al cluster. Tale stringa di connessione al cluster è presente nella console di Amazon Redshift, nella pagina dei dettagli del cluster.

Per trovare la stringa di connessione di un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli.
3. Sono disponibili le stringhe di connessione URL JDBC e URL ODBC, insieme a dettagli aggiuntivi, nella sezione Informazioni generali. Ogni stringa si basa sulla AWS regione in cui viene eseguito il cluster. Fai clic sull'icona accanto alla stringa di connessione corretta per copiarla.

Per connetterti a un endpoint del cluster, puoi utilizzare l'URL dell'endpoint del cluster da una richiesta [DescribeClusters API](#). Di seguito è riportato un esempio di URL dell'endpoint del cluster.

```
mycluster.cmeaswqeuae.us-east-2.redshift.amazonaws.com
```

Se hai impostato un nome di dominio personalizzato per il tuo cluster, puoi utilizzarlo anche per connetterti al tuo cluster. Per ulteriori informazioni sulla creazione di un nome di dominio personalizzato, consulta [Configurazione di un nome di dominio personalizzato](#).

#### Note

Quando ti connetti, non utilizzare l'indirizzo IP di un nodo del cluster o l'indirizzo IP dell'endpoint VPC. Usa sempre l'endpoint Redshift per evitare interruzioni non necessarie. L'unica eccezione all'utilizzo dell'URL dell'endpoint è quando utilizzi un nome di dominio personalizzato. Per ulteriori informazioni, consulta [Utilizzo di un nome di dominio personalizzato per le connessioni client](#).

## Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift

Per connettersi al cluster Amazon Redshift da numerosi strumenti client SQL di terze parti è possibile utilizzare una connessione al driver JDBC versione 2.1. Il connettore Amazon Redshift JDBC fornisce una soluzione open source. Puoi sfogliare il codice sorgente, richiedere miglioramenti, segnalare problemi e fornire contributi.

Per utilizzare una connessione JDBC, consultare le sezioni seguenti.

### Argomenti

- [Scarica il driver JDBC Amazon Redshift, versione 2.1](#)
- [Installazione del driver JDBC di Amazon Redshift, versione 2.1](#)
- [Ottenimento dell'URL JDBC](#)
- [Creazione dell'URL di connessione](#)
- [Configurazione dei keepalive TCP per la connessione JDBC](#)
- [Configurazione della connessione JDBC con Apache Maven](#)
- [Configurazione dell'autenticazione e di SSL](#)

- [Configurazione della registrazione](#)
- [Conversione dei tipi di dati](#)
- [Utilizzo del supporto per le istruzioni preparate](#)
- [Differenze tra le versioni 2.1 e 1.x del driver JDBC](#)
- [Creazione di file di inizializzazione \(.ini\) per il driver JDBC versione 2.1](#)
- [Opzioni per la configurazione del driver JDBC versione 2.1](#)
- [Versioni precedenti del driver JDBC versione 2.1](#)

Scarica il driver JDBC Amazon Redshift, versione 2.1

Amazon Redshift offre driver per strumenti compatibili con l'API JDBC 4.2. Il nome della classe per questo driver è `com.amazon.redshift.Driver`.

Per informazioni dettagliate su come installare il driver JDBC, fare riferimento alle librerie del driver JDBC e registrare la classe driver, consultare i seguenti argomenti.

Per ogni computer su cui viene utilizzato il driver JDBC versione 2.1 di Amazon Redshift, assicurarsi che sia installato Java Runtime Environment (JRE) 8.0.

Se si utilizza il driver JDBC di Amazon Redshift per l'autenticazione del database, assicurarsi di disporre di AWS SDK for Java 1.11.118 o versione successiva nella classpath Java. Se non lo avete AWS SDK for Java installato, scaricate il file ZIP con driver compatibili con JDBC 4.2 e librerie dipendenti dai driver per l'SDK: AWS

- [Driver compatibile con JDBC 4.2 versione 2.1 e librerie dipendenti dai driver AWS SDK driver compatibili con JDBC 4.2 e librerie dipendenti dai driver SDK AWS](#)

Questo file ZIP contiene la versione 2.1 del driver compatibile con JDBC 4.2 e i file di libreria dipendenti dal driver SDK for AWS Java 1.x. Decomprimere i file jar dipendenti nella stessa posizione del driver JDBC. Solo il driver JDBC deve trovarsi nella variabile CLASSPATH.

Questo file ZIP non include l' AWS SDK completo per Java 1.x. Tuttavia, include le librerie AWS SDK for Java 1.x dipendenti dai driver necessarie AWS Identity and Access Management per l'autenticazione del database (IAM).

Utilizza questo driver JDBC Amazon Redshift con l' AWS SDK necessario per l'autenticazione del database IAM.

Per installare l' AWS SDK completo per Java 1.x, [AWS consulta SDK for Java 1.x](#) nella Developer Guide.AWS SDK for Java

- [Driver compatibile con JDBC 4.2 versione 2.1 \(senza AWS SDK\) Nella regione Cina \(Pechino\)](#)

Esaminare la licenza software del driver JDBC versione 2.1 e il file di log delle modifiche:

- [Licenza del driver JDBC versione 2.1](#)
- [Log delle modifiche del driver JDBC versione 2.1](#)

I driver JDBC versione 1.2.27.1051 e successive supportano le procedure archiviate di Amazon Redshift. Per ulteriori informazioni, consulta [Creazione di procedure archiviate in Amazon Redshift](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Installazione del driver JDBC di Amazon Redshift, versione 2.1

Per installare la versione 2.1 del driver compatibile con Amazon Redshift JDBC 4.2 e le librerie dipendenti dai driver per AWS SDK, estrai i file dall'archivio ZIP nella directory di tua scelta.

Per installare la versione 2.1 del driver compatibile con Amazon Redshift JDBC 4.2 (senza AWS SDK), copia il file JAR nella directory che preferisci.

Per accedere a un archivio dati Amazon Redshift utilizzando il driver JDBC di Amazon Redshift, occorre eseguire la configurazione come descritto di seguito.

Argomenti

- [Riferimento alle librerie del driver JDBC](#)
- [Registrazione della classe del driver](#)

Riferimento alle librerie del driver JDBC

L'applicazione JDBC o il codice Java utilizzati per connettersi ai dati devono accedere ai file JAR del driver. Nell'applicazione o nel codice, specificare tutti i file JAR che sono stati estratti dall'archivio ZIP.

Utilizzo del driver in un'applicazione JDBC

Le applicazioni JDBC in genere forniscono una serie di opzioni di configurazione per l'aggiunta di un elenco di file di libreria del driver. Utilizzare le opzioni fornite per includere tutti i file JAR dall'archivio

ZIP nell'ambito della configurazione del driver nell'applicazione. Per ulteriori informazioni, consultare la documentazione relativa all'applicazione JDBC.

### Utilizzo del driver nel codice Java

È necessario includere tutti i file della libreria del driver nella variabile classpath. Questo è il percorso in cui Java Runtime Environment cerca le classi e gli altri file delle risorse. Per ulteriori informazioni, consultare la documentazione di Java SE appropriata per impostare la variabile classpath per il sistema operativo in uso.

- Windows: <https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html>
- Linux e Solaris: <https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html>
- macOS: il percorso di classe macOS predefinito è la directory in cui è installato il driver JDBC.

### Registrazione della classe del driver

Assicurarsi di registrare la classe corretta per l'applicazione. Utilizzare le seguenti classi per connettere il driver JDBC Amazon Redshift agli archivi dati Amazon Redshift:

- Le classi `Driver` estendono `java.sql.Driver`.
- Le classi `DataSource` estendono `javax.sql.DataSource` e `javax.sql.ConnectionPoolDataSource`.

Il driver supporta i seguenti nomi di classe completi indipendenti dalla versione JDBC:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

L'esempio seguente mostra come utilizzare la `DriverManager` classe per stabilire una connessione per JDBC 4.2.

```
private static Connection connectViaDM() throws Exception
{
    Connection connection = null;
    connection = DriverManager.getConnection(CONNECTION_URL);
    return connection;
}
```

Nell'esempio seguente viene illustrato come utilizzare la classe `DataSource` per stabilire una connessione.

```
private static Connection connectViaDS() throws Exception
{
    Connection connection = null;
    //
    Amazon Redshift JDBC Driver Installation and Configuration Guide
    DataSource ds = new com.amazon.redshift.jdbc.DataSource
    ();
    ds.setURL(CONNECTION_URL);
    connection = ds.getConnection();
    return connection;
}
```

## Ottenimento dell'URL JDBC

Prima di potersi connettere al cluster Amazon Redshift da uno strumento del client SQL, è necessario conoscere l'URL JDBC del cluster. L'URL JDBC ha il formato seguente: `jdbc:redshift://endpoint:port/database`.

I campi del formato mostrato in precedenza hanno i seguenti valori.

Campo	Valore
<code>jdbc</code>	Protocollo per la connessione.
<code>redshift</code>	Il protocollo secondario che specifica di utilizzare il driver Amazon Redshift per connettersi al database.
<code><i>endpoint</i></code>	L'endpoint del cluster Amazon Redshift.
<code><i>port</i></code>	Numero di porta specificato all'avvio del cluster. In presenza di un firewall, assicurati che questa porta sia aperta per poterla utilizzare.
<code><i>database</i></code>	Il database che hai creato per il tuo cluster.

Di seguito è riportato un esempio di URL JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Assicurati di inserire i valori dell'URL, ad esempio i SessionToken valori, in formato codificato URL.

Per informazioni su come ottenere la tua connessione JDBC, consulta [Ricerca della stringa di connessione al cluster](#).

Se il computer client non riesce a connettersi al database, puoi provare a risolvere i possibili problemi. Per ulteriori informazioni, consulta [Risoluzione dei problemi di connessione in Amazon Redshift](#).

### Creazione dell'URL di connessione

Utilizza l'URL di connessione per fornire informazioni di connessione all'archivio dati a cui si sta accedendo. Di seguito è riportato il formato dell'URL di connessione per il driver JDBC Amazon Redshift versione 2.1. Qui, [Host] è l'endpoint del server Amazon Redshift e [Port] è il numero della porta TCP utilizzata dal server per ascoltare le richieste dei client.

```
jdbc:redshift://[Host]:[Port]
```

Di seguito è riportato il formato di un URL di connessione che specifica alcune impostazioni facoltative.

```
jdbc:redshift://[Host]:[Port]/[database];[Property1]=[Value];  
[Property2]=[Value];
```

Ad esempio, supponiamo di volersi connettere alla porta 9000 su un cluster Amazon Redshift nella regione Stati Uniti occidentali (California settentrionale) in AWS. Inoltre vuoi accedere al database denominato dev e autenticare la connessione utilizzando un nome utente del database e una password. In tal caso, viene utilizzato l'URL di connessione seguente.

```
jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/  
dev;UID=amazon;PWD=amazon
```

Per separare le opzioni di configurazione dal resto della stringa URL puoi utilizzare i seguenti caratteri:

- ;

- ?

Ad esempio, le seguenti stringhe URL sono equivalenti:

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=false;defaultRowFetchSize=100
```

Per separare le opzioni di configurazione una dall'altra nella stringa URL puoi utilizzare i seguenti caratteri:

- ;
- &

Ad esempio, le seguenti stringhe URL sono equivalenti:

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev;ssl=false&defaultRowFetchSize=100
```

Nell'esempio di URL seguente viene specificato un livello di log pari a 6 e il percorso dei log.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs;
```

Non duplicare le proprietà nell'URL di connessione.

Per un elenco completo delle opzioni di configurazione che è possibile specificare, consultare [Opzioni per la configurazione del driver JDBC versione 2.1](#).

#### Note

Quando ti connetti, non utilizzare l'indirizzo IP di un nodo del cluster o l'indirizzo IP dell'endpoint VPC. Usa sempre l'endpoint Redshift per evitare interruzioni non necessarie. L'unica eccezione all'utilizzo dell'URL dell'endpoint è quando utilizzi un nome di dominio personalizzato. Per ulteriori informazioni, consulta [Utilizzo di un nome di dominio personalizzato per le connessioni client](#).

## Configurazione dei keepalive TCP per la connessione JDBC

Per impostazione predefinita, il driver JDBC di Amazon Redshift è configurato per utilizzare keepalive TCP per impedire il timeout delle connessioni. È possibile specificare quando il driver inizia a inviare pacchetti keepalive o disattivare la funzionalità impostando le proprietà pertinenti nell'URL di connessione. Per ulteriori informazioni sulla sintassi dell'URL di connessione, consultare [Creazione dell'URL di connessione](#).

Proprietà	Descrizione
TCPKeepAlive	Per disattivare i keepalive TCP, impostare questa proprietà su FALSE.

## Configurazione della connessione JDBC con Apache Maven

Apache Maven è uno strumento di comprensione e gestione di progetti software. AWS SDK for Java Supporta i progetti Apache Maven. Per ulteriori informazioni, consultare [Utilizzo di SDK con Apache Maven](#) nella Guida per gli sviluppatori di AWS SDK for Java .

Se si utilizza Apache Maven, è possibile configurare e compilare i progetti in modo da usare un driver JDBC di Amazon Redshift per connettersi al cluster Amazon Redshift. A tale scopo, aggiungi il driver JDBC come una dipendenza nel file `pom.xml` del progetto. Segui la procedura descritta in questa sezione se utilizzi Maven per compilare il progetto e intendi usare una connessione JDBC.

## Configurazione del driver JDBC come una dipendenza Maven

Per configurare il driver JDBC come una dipendenza Maven

1. Aggiungere il repository Amazon o il repository Maven Central alla sezione dei repository del file `pom.xml`.

### Note

L'URL nel codice seguente restituisce un errore se utilizzato in un browser. Utilizzare questo URL solo nel contesto di un progetto Maven.

Per un repository Amazon Maven, utilizzare quanto segue.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
release</url>
  </repository>
</repositories>
```

Per connettersi tramite Secure Sockets Layer (SSL), aggiungere il seguente repository al file `pom.xml`.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
  </repository>
</repositories>
```

Per un repository Maven Central, aggiungere quanto segue al file `pom.xml`.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://repo1.maven.org/maven2</url>
  </repository>
</repositories>
```

2. Dichiarare la versione del driver che si intende utilizzare nella sezione delle dipendenze del file `pom.xml`.

Amazon Redshift offre driver per strumenti compatibili con l'API JDBC 4.2. Per informazioni sulla funzionalità supportata da questi driver, consulta [Scarica il driver JDBC Amazon Redshift, versione 2.1.](#)

Aggiungere una dipendenza per il driver come riportato di seguito.

Sostituire *driver-version* nell'esempio seguente con la versione del driver, ad esempio `2.1.0.1`.

Per un driver compatibile con JDBC 4.2, utilizzare quanto segue.

```
<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42</artifactId>
  <version>driver-version</version>
</dependency>
```

Il nome della classe per questo driver è `com.amazon.redshift.Driver`.

I driver Amazon Redshift Maven richiedono le seguenti dipendenze facoltative quando si utilizza l'autenticazione del database IAM.

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-core</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-redshift</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-sts</artifactId>
  <version>1.12.23</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
```

### Aggiornamento del driver alla versione più recente

Per aggiornare o passare alla versione più recente del driver JDBC di Amazon Redshift, modificare la sezione relativa alla versione della dipendenza indicando l'ultima versione del driver. Quindi ripristina il progetto con il plugin di pulizia Maven, come mostrato di seguito.

```
mvn clean
```

## Configurazione dell'autenticazione e di SSL

Per proteggere i dati da accessi non autorizzati, gli archivi dati di Amazon Redshift richiedono l'autenticazione di tutte le connessioni tramite le credenziali utente. Alcuni archivi dati richiedono inoltre connessioni tramite il protocollo Secure Sockets Layer (SSL), con o senza autenticazione unidirezionale.

Il driver JDBC versione 2.1 di Amazon Redshift fornisce il supporto completo per questi protocolli di autenticazione.

La versione SSL supportata dal driver dipende dalla versione JVM che si sta utilizzando. Per ulteriori informazioni sulle versioni SSL supportate da ogni versione di Java, consultare [Diagnosi di TLS, SSL e HTTPS](#) sul blog di gestione prodotti del gruppo di piattaforme Java.

La versione SSL utilizzata per la connessione è la versione più alta supportata sia dal driver che dal server e viene determinata al momento della connessione.

Configura il driver JDBC versione 2.1 di Amazon Redshift per autenticare la connessione in base ai requisiti di sicurezza del server Redshift a cui stai effettuando la connessione.

Per autenticare la connessione, è sempre necessario specificare il nome utente e la password di Redshift. A seconda che SSL sia abilitato e necessario sul server, potresti dover configurare il driver per la connessione tramite SSL. Oppure potrebbe essere necessario utilizzare l'autenticazione SSL unidirezionale in modo che il client (il driver stesso) verifichi l'identità del server.

Le informazioni di configurazione vengono fornite al driver nell'URL di connessione. Per ulteriori informazioni sulla sintassi dell'URL di connessione, consultare [Creazione dell'URL di connessione](#).

SSL indica TLS/SSL, ovvero sia Transport Layer Security che Secure Sockets Layer. Il driver supporta le versioni standard di settore di TLS/SSL.

### Utilizzo solo del nome utente e della password

Se il server a cui ti connetti non utilizza SSL, per autenticare la connessione è sufficiente fornire il nome utente e la password di Redshift.

Per configurare l'autenticazione utilizzando solo il nome utente e la password di Redshift

1. Imposta la proprietà UID sul nome utente di Redshift per accedere al server Amazon Redshift.
2. Imposta la proprietà PWD sulla password corrispondente al nome utente di Redshift.

## Utilizzo di SSL senza verifica dell'identità

Se il server a cui ci si connette utilizza SSL ma non richiede la verifica dell'identità, è possibile configurare il driver per utilizzare un factory SSL non convalidante.

Come configurare una connessione SSL senza verifica dell'identità

1. Imposta la proprietà UID sul nome utente di Redshift per accedere al server Amazon Redshift.
2. Imposta la proprietà PWD sulla password corrispondente al nome utente di Redshift.
3. Impostare la proprietà SSLFactory su `com.amazon.redshift.ssl.NonValidatingFactory`.

## Utilizzo dell'autenticazione SSL unidirezionale

Se il server a cui ci si connette utilizza SSL e dispone di un certificato, allora è possibile configurare il driver per verificare l'identità del server utilizzando l'autenticazione unidirezionale.

L'autenticazione unidirezionale richiede un certificato SSL firmato e attendibile che verifichi l'identità del server. È possibile configurare il driver per utilizzare un certificato specifico o accedere a un certificato TrustStore contenente il certificato appropriato. Se non si specifica un certificato o TrustStore, il driver utilizza il codice Java predefinito TrustStore (in genere uno `jssecacerts` o `duecacerts`).

Come configurare l'autenticazione SSL unidirezionale

1. Imposta la proprietà UID sul nome utente di Redshift per accedere al server Amazon Redshift.
2. Imposta la proprietà PWD sulla password corrispondente al nome utente di Redshift.
3. Impostare la proprietà SSL su `true`.
4. Imposta la `RootCert` proprietà SSL sulla posizione del certificato CA principale.
5. Se non utilizzi uno dei file Java predefiniti TrustStores, esegui una delle seguenti operazioni:
  - Per specificare un certificato server, imposta la `RootCert` proprietà SSL sul percorso completo del certificato.
  - Per specificare a TrustStore, procedi come segue:
    - a. Utilizzate il programma `keytool` per aggiungere il certificato del server a TrustStore quello che desiderate utilizzare.

- b. Specificate la password TrustStore e da utilizzare all'avvio dell'applicazione Java utilizzando il driver. Per esempio:

```
-Djavax.net.ssl.trustStore=[TrustStoreName]
-Djavax.net.ssl.trustStorePassword=[TrustStorePassword]
-Djavax.net.ssl.trustStoreType=[TrustStoreType]
```

#### 6. modi:

- Per convalidare il certificato, impostare la proprietà SSLMode su verify-ca.
- Per convalidare il certificato e verificare il nome host nel certificato, impostare la proprietà SSLMode su verify-full.

### Configurazione dell'autenticazione IAM

Se ci si connette a un server Amazon Redshift tramite l'autenticazione IAM, impostare le seguenti proprietà come parte della stringa di connessione all'origine dati.

Per ulteriori informazioni sull'autenticazione IAM, consultare [Identity and Access Management in Amazon Redshift](#).

Per utilizzare l'autenticazione IAM, utilizzare uno dei seguenti formati di stringa di connessione:

Stringa di connessione	Descrizione
<code>jdbc:redshift:iam:// [host]:[port]/[db]</code>	Una stringa di connessione normale. Il driver deduce il ClusterID e la regione dall'host.
<code>jdbc:redshift:iam:// [cluster-id]: [region]/[db]</code>	Il driver recupera le informazioni sull'host, dato il ClusterID e la regione.
<code>jdbc:redshift:iam:// [host]/[db]</code>	Il driver utilizza di default la porta 5439 e recupera ClusterID e regione dall'host. A seconda della porta selezionata durante la creazione, la modifica o la migrazione del cluster, consenti l'accesso alla porta selezionata.

## Specifica di profili

Se si utilizza l'autenticazione IAM, è possibile specificare eventuali altre proprietà di connessione obbligatorie o facoltative sotto il nome di un profilo. In questo modo, è possibile evitare di inserire determinate informazioni direttamente nella stringa di connessione. Il nome del profilo viene specificato nella stringa di connessione utilizzando la proprietà Profile.

I profili possono essere aggiunti al file delle AWS credenziali. Il percorso predefinito per questo file è `~/.aws/credentials`.

È possibile modificare il valore predefinito impostando il percorso nella seguente variabile di ambiente: `AWS_CREDENTIAL_PROFILES_FILE`

Per ulteriori informazioni sui profili, consultare [Utilizzo delle credenziali AWS](#) nella AWS SDK for Java.

### Utilizzo delle credenziali del profilo dell'istanza

Se si sta eseguendo un'applicazione su un'istanza Amazon EC2 associata a un ruolo IAM, è possibile connettersi utilizzando le credenziali del profilo dell'istanza.

A tale scopo, utilizzare uno dei formati di stringa di connessione IAM nella tabella precedente e impostare la proprietà `dbuser.connection` sul nome utente Amazon Redshift con cui ci si connette.

Per ulteriori informazioni sui profili dell'istanza, consultare [Gestione degli accessi](#) nella Guida per l'utente di IAM.

### Utilizzo di provider di credenziali

Il driver supporta inoltre i plug-in del provider di credenziali dei seguenti servizi:

- Active Directory Federation Service (ADFS)
- Servizio JSON Web Tokens (JWT)
- Servizio Microsoft Azure Active Directory (AD) e servizio Browser Microsoft Azure Active Directory (AD)
- Servizio Okta
- PingFederate Servizio
- Browser SAML per servizi SAML quali Okta, Ping o ADFS

Se si utilizza uno di questi servizi, l'URL di connessione deve specificare le proprietà seguenti:

- `Plugin_Name`: la variabile classpath completa per la classe di plug-in del provider di credenziali.
- `IdP_Host`: l'host del servizio che si sta utilizzando per autenticarsi in Amazon Redshift.
- `IdP_Port`: la porta su cui l'host del servizio di autenticazione è in ascolto. Non richiesta per Okta.
- `User`: il nome utente per il server `idp_host`.
- `Password`: la password associata al nome utente `idp_host`.
- `DbUser`— Il nome utente Amazon Redshift con cui ti stai connettendo.
- `SSL_Insecure`: indica se il certificato del server IDP deve essere verificato.
- `Client_ID`: l'ID client associato al nome utente nel portale di Azure AD. Utilizzata solo per Azure AD.
- `Client_Secret`: il segreto client associato all'ID client nel portale di Azure AD. Utilizzata solo per Azure AD.
- `IdP_Tenant`: l'ID tenant di Azure AD per l'applicazione Amazon Redshift. Utilizzata solo per Azure AD.
- `App_ID`: l'ID dell'app Okta per l'applicazione Amazon Redshift. Utilizzata solo per Okta.
- `App_Name`: il nome dell'app Okta per l'applicazione Amazon Redshift. Utilizzata solo per Okta.
- `Partner_SPID`: il valore facoltativo dello SPID (Service Provider ID) del partner. Utilizzato solo per PingFederate.

Se si utilizza un plug-in per il browser per uno di questi servizi, l'URL di connessione può includere anche:

- `Login_URL`: l'URL della risorsa sul sito Web del provider di identità quando si usa il linguaggio SAML (Security Assertion Markup Language) o i servizi di Azure AD tramite un plug-in del browser. Questo parametro è obbligatorio se si utilizza un plug-in del browser.
- `Listen_Port`: la porta utilizzata dal driver per ottenere la risposta SAML dal provider di identità quando si usano i servizi SAML o Azure AD tramite un plug-in del browser.
- `IdP_Response_Timeout`: la quantità di tempo, espressa in secondi, per cui il driver attende la risposta SAML dal provider di identità quando si usano i servizi SAML o Azure AD tramite un plug-in del browser.

Per informazioni sulle proprietà aggiuntive della stringa di connessione, consultare [Opzioni per la configurazione del driver JDBC versione 2.1.](#)

## Configurazione della registrazione

È possibile attivare l'accesso al driver per facilitare la diagnosi dei problemi.

È possibile registrare le informazioni sui driver utilizzando i seguenti metodi.

- Per salvare le informazioni registrate nei file di log, consultare [Utilizzo dei file di log](#).
- Per inviare informazioni registrate a LogStream o LogWriter specificate in DriverManager, vedere [Utilizzando o LogStream LogWriter](#).

Le informazioni di configurazione vengono fornite al driver nell'URL di connessione. Per ulteriori informazioni sulla sintassi dell'URL di connessione, consultare [Creazione dell'URL di connessione](#).

### Utilizzo dei file di log

Attivare la registrazione abbastanza a lungo da rilevare un problema. La registrazione riduce le prestazioni e può richiedere una grande quantità di spazio su disco.

Imposta la LogLevel chiave nell'URL di connessione per attivare la registrazione e specifica la quantità di dettagli inclusi nei file di registro. Nella tabella seguente sono riportati i livelli di registrazione forniti dal driver JDBC versione 2.1 di Amazon Redshift, in ordine dal meno dettagliato al più dettagliato.

LogLevel valore	Descrizione
1	Registrazione eventi di errore gravi che comportano o l'interruzione del driver.
2	Registrazione eventi di errore che potrebbero consentire al driver di restare in esecuzione.
3	Registra gli eventi che potrebbero causare un errore se non viene eseguita un'azione. Questo livello di registrazione e i livelli di registrazione superiori a questo livello registrano anche le query dell'utente.
4	Registrazione informazioni generali che descrivono l'avanzamento del driver.

LogLevel valore	Descrizione
5	Registrazione informazioni dettagliate utili per il debug del driver.
6	Registrazione tutte le attività del driver.

Come configurare la registrazione che utilizza i file di log

1. Imposta la LogLevel proprietà sul livello di informazioni desiderato da includere nei file di registro.
2. Imposta la LogPath proprietà sul percorso completo della cartella in cui desideri salvare i file di registro.

Ad esempio, il seguente URL di connessione abilita il livello di registrazione 3 e salva i file di log nella cartella C:\temp: jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp

3. Per assicurarsi che le nuove impostazioni abbiano effetto, riavviare l'applicazione JDBC e riconnettersi al server.

Il driver JDBC di Amazon Redshift produce i seguenti file di log nella posizione specificata nella proprietà: LogPath

- File redshift\_jdbc.log che registra l'attività del driver che non è specifica di una connessione.
- File redshift\_jdbc\_connection\_[numero].log per ogni connessione effettuata al database, dove [numero] è un numero che identifica ogni file di log. Questo file registra l'attività del driver specifica per la connessione.

Se il LogPath valore non è valido, il driver invia le informazioni registrate allo standard output stream () System.out

Utilizzando o LogStream LogWriter

Attivare la registrazione abbastanza a lungo da rilevare un problema. La registrazione riduce le prestazioni e può richiedere una grande quantità di spazio su disco.

Imposta la LogLevel chiave nell'URL di connessione per attivare la registrazione e specifica la quantità di dettagli inviati a LogStream o LogWriter specificata in. DriverManager

Per attivare la registrazione che utilizza o: LogStream LogWriter

1. Per configurare il driver in modo da registrare informazioni generali che descrivono lo stato di avanzamento del driver, impostate la LogLevel proprietà su 1 o INFO.
2. Per assicurarsi che le nuove impostazioni abbiano effetto, riavviare l'applicazione JDBC e riconnettersi al server.

Per disattivare la registrazione che utilizza LogStream o LogWriter:

1. Rimuovi la LogLevel proprietà dall'URL di connessione.
2. Per assicurarsi che le nuove impostazioni abbiano effetto, riavviare l'applicazione JDBC e riconnettersi al server.

### Conversione dei tipi di dati

Il driver JDBC versione 2.1 di Amazon Redshift supporta molti formati di dati comuni, convertendo tra tipologie di dati Amazon Redshift, SQL e Java.

La tabella seguente riporta le mappature dei tipi di dati supportate.

Tipo di Amazon Redshift	Tipo SQL	Tipo di Java
BIGINT	SQL_BIGINT	Long
BOOLEAN	SQL_BIT	Booleano
CHAR	SQL_CHAR	Stringa
DATE	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMERIC	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Doppio
GEOMETRY	SQL_LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Numero intero
OID	SQL_BIGINT	Long

Tipo di Amazon Redshift	Tipo SQL	Tipo di Java
SUPER	SQL_LONGVARCHAR	Stringa
REAL	SQL_REAL	Float
SMALLINT	SQL_SMALLINT	Breve
TEXT	SQL_VARCHAR	Stringa
TIME	SQL_TYPE_TIME	java.sql.Time
TIMETZ	SQL_TYPE_TIME	java.sql.Time
TIMESTAMP	SQL_TYPE_TIMESTAMP	java.sql.Timestamp
TIMESTAMPZ	SQL_TYPE_TIMESTAMP	java.sql.Timestamp
VARCHAR	SQL_VARCHAR	Stringa

## Utilizzo del supporto per le istruzioni preparate

Il driver JDBC di Amazon Redshift supporta le istruzioni preparate. È possibile utilizzare le istruzioni preparate per migliorare le prestazioni delle query con parametri che devono essere eseguite più volte durante la stessa connessione.

Una istruzione preparata è un'istruzione SQL compilata sul lato server ma che non viene eseguita immediatamente. L'istruzione compilata viene archiviata sul server come PreparedStatement oggetto fino alla chiusura dell'oggetto o della connessione. Mentre tale oggetto esiste, è possibile eseguire l'istruzione preparata tutte le volte necessarie utilizzando valori di parametro diversi senza dover compilare nuovamente l'istruzione. Questo sovraccarico ridotto consente di eseguire più rapidamente l'insieme di query.

Per ulteriori informazioni sulle istruzioni preparate, consultare "[Utilizzo delle istruzioni preparate](#)" nel [tutorial Elementi essenziali di JDBC di Oracle](#).

È possibile preparare un'istruzione che contiene più query. Ad esempio, l'istruzione preparata seguente contiene due query INSERT:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO
```

```
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES
(1, 'abc');");
```

Fare attenzione in quanto queste query non dipendono dai risultati di altre query specificate all'interno della stessa istruzione preparata. Poiché le query non vengono eseguite durante la fase di preparazione, i risultati non sono ancora stati restituiti e non sono disponibili per altre query nella stessa istruzione preparata.

Ad esempio, la seguente istruzione preparata, che crea una tabella e quindi inserisce valori nella tabella appena creata, non è consentita:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable
VALUES (1, 'abc');");
```

Se si prova a preparare questa istruzione, il server restituisce un errore che indica che la tabella di destinazione (MyTable) non esiste ancora. La query CREATE deve essere eseguita prima che la query INSERT possa essere preparata.

## Differenze tra le versioni 2.1 e 1.x del driver JDBC

In questa sezione sono descritte le differenze nelle informazioni restituite dalle versioni 2.1 e 1.x del driver JDBC. Il driver JDBC versione 1.x è interrotto.

La tabella seguente elenca le DatabaseMetadata informazioni restituite dalle funzioni `getDatabaseProduct Name ()` e `getDatabaseProduct Version ()` per ogni versione del driver JDBC. Il driver JDBC versione 2.1 ottiene i valori mentre stabilisce la connessione. Il driver JDBC versione 1.x ottiene i valori come risultato di una query.

Versione driver JDBC	<code>get DatabaseProduct Name ()</code> risultato	ottieni il risultato DatabaseP roduct Version ()
2.1	Redshift	8.0.2
1.x	PostgreSQL	08,0002

La tabella seguente elenca le DatabaseMetadata informazioni restituite dalla `getTypeInfo` funzione per ogni versione del driver JDBC.

Versione driver JDBC	getTypeInfo risultato
2.1	Coerente con i tipi di dati Redshift
1.x	Coerente con i tipi di dati PostgreSQL

## Creazione di file di inizializzazione (.ini) per il driver JDBC versione 2.1

Grazie ai file di inizializzazione (.ini) per il driver JDBC versione 2.1 di Amazon Redshift, è possibile specificare i parametri di configurazione a livello di sistema. Ad esempio, i parametri di autenticazione IdP federati possono variare per ogni applicazione. Il file .ini fornisce una posizione comune dove i client SQL possono ottenere i parametri di configurazione richiesti.

È possibile creare un file di inizializzazione (.ini) del driver JDBC versione 2.1 contenente le opzioni di configurazione per i client SQL. Il nome di default del file è `rsjdbc.ini`. Il driver JDBC versione 2.1 controlla il file .ini nelle seguenti posizioni, elencate in ordine di precedenza:

- Parametro `IniFile` nell'URL di connessione o nella finestra di dialogo delle proprietà di connessione del client SQL. Assicurarsi che il parametro `IniFile` contenga il percorso completo del file .ini, incluso il nome del file. Per ulteriori informazioni sul parametro `IniFile`, consultare [IniFile](#). Se il parametro `IniFile` specifica in modo errato la posizione del file ini, viene visualizzato un errore.
- Variabili di ambiente quali `AMAZON_REDSHIFT_JDBC_INI_FILE` con il percorso completo, incluso il nome del file. È possibile utilizzare `rsjdbc.ini` oppure specificare un nome file. Se la variabile di ambiente `AMAZON_REDSHIFT_JDBC_INI_FILE` specifica in modo errato la posizione del file ini, viene visualizzato un errore.
- Directory in cui si trova il file JAR del driver.
- Directory home dell'utente.
- Directory temporanea del sistema.

È possibile organizzare il file .ini in sezioni, ad esempio `[DRIVER]`. Ogni sezione contiene coppie chiave-valore che specificano i vari parametri di connessione. È possibile utilizzare il plug-in `IniSection` per specificare una sezione nel file .ini. Per ulteriori informazioni sul parametro `IniSection`, consultare [IniSection](#).

Di seguito è riportato un esempio del formato di file .ini, con sezioni per [DRIVER], [DEV], [QA] e [PROD]. La sezione [DRIVER] può essere applicata a qualsiasi connessione.

```
[DRIVER]
key1=val1
key2=val2

[DEV]
key1=val1
key2=val2

[QA]
key1=val1
key2=val2

[PROD]
key1=val1
key2=val2
```

Il driver JDBC versione 2.1 carica i parametri di configurazione dalle seguenti posizioni, elencate in ordine di precedenza:

- Parametri di configurazione di default nel codice dell'applicazione.
- Proprietà della sezione [DRIVER] dal file .ini, se incluso.
- Parametri di configurazione della sezione personalizzata, se l'opzione `IniSection` viene fornita nell'URL di connessione o nella finestra di dialogo delle proprietà di connessione del client SQL.
- Proprietà dall'oggetto proprietà di connessione specificato nella chiamata `getConnection`.
- Parametri di configurazione specificati nell'URL di connessione.

### Opzioni per la configurazione del driver JDBC versione 2.1

Di seguito è possibile trovare le descrizioni per le opzioni che è possibile specificare per la versione 2.1 del driver JDBC di Amazon Redshift. Le opzioni di configurazione non fanno distinzione tra maiuscole e minuscole.

È possibile impostare le proprietà di configurazione utilizzando l'URL di connessione. Per ulteriori informazioni, consulta [Creazione dell'URL di connessione](#).

### Argomenti

- [AccessKeyID](#)
- [AllowDB UserOverride](#)
- [App\\_ID](#)
- [App\\_Name](#)
- [ApplicationName](#)
- [AuthProfile](#)
- [AutoCreate](#)
- [Client\\_ID](#)
- [Client\\_Secret](#)
- [ClusterID](#)
- [Compressione](#)
- [connectTimeout](#)
- [connectionTimezone](#)
- [database MetadataCurrent DbOnly](#)
- [DbUser](#)
- [DbGroups](#)
- [DBNAME](#)
- [RowFetchdimensione predefinita](#)
- [DisableIsValidQuery](#)
- [abilita Buffer FetchRing](#)
- [abilitare MultiSql Support](#)
- [dimensione di recupero RingBuffer](#)
- [ForceLowercase](#)
- [groupFederation](#)
- [HOST](#)
- [IAM DisableCache](#)
- [IAMDuration](#)
- [Identity\\_Namespace](#)
- [IdP\\_Host](#)

- [IdP\\_Port](#)
- [idp\\_tenant](#)
- [IdP\\_Response\\_Timeout](#)
- [IniFile](#)
- [IniSection](#)
- [isServerless](#)
- [URL\\_login\\_](#)
- [loginTimeout](#)
- [effettuare il login ToRp](#)
- [LogLevel](#)
- [LogPath](#)
- [OverrideSchemaPatternType](#)
- [Partner\\_SPID](#)
- [Password](#)
- [Plugin\\_Name](#)
- [PORT](#)
- [preferred\\_role](#)
- [Profilo](#)
- [PWD](#)
- [queryGroup](#)
- [readOnly](#)
- [Regione](#)
- [Inseriti rossi WriteBatched](#)
- [re WriteBatched InsertsSize](#)
- [roleArn](#)
- [ruolo SessionName](#)
- [scope](#)
- [SecretAccessChiave](#)
- [SessionToken](#)

- [senza server AcctId](#)
- [senza server WorkGroup](#)
- [socketFactory](#)
- [socketTimeout](#)
- [SSL](#)
- [ssl\\_insecure](#)
- [SSLCert](#)
- [SSLFactory](#)
- [SSLKey](#)
- [SSLMode](#)
- [SSLPassword](#)
- [SSL RootCert](#)
- [StsEndpointUrl](#)
- [tcp KeepAlive](#)
- [token](#)
- [token\\_type](#)
- [UID](#)
- [Utente](#)
- [web IdentityToken](#)

### AccessKeyID

- Valore predefinito: nessuno
- Tipo di dati: stringa

È possibile specificare questo parametro per immettere la chiave di accesso IAM per l'utente o il ruolo. Di solito è possibile individuare la chiave guardando una stringa o un profilo utente esistente. Se si specifica questo parametro, è necessario specificare anche il parametro `SecretAccessKey`. Se passato nell'URL JDBC, l' `AccessKeyID` deve essere codificato come URL.

Questo parametro è facoltativo.

## AllowDB UserOverride

- Valore predefinito: 0
- Tipo di dati: stringa

Questa opzione specifica se il driver utilizza l'opzione `DbUser` dall'asserzione SAML o il valore specificato nella proprietà di connessione `DbUser` nell'URL di connessione.

Questo parametro è facoltativo.

1

Il driver utilizza il valore `DbUser` dall'asserzione SAML.

Se l'asserzione SAML non specifica un valore per `DbUser`, il driver utilizzerà il valore specificato nella proprietà di connessione `DbUser`. Se neanche la proprietà di connessione specifica un valore, il driver utilizzerà il valore specificato nel profilo di connessione.

0

Il driver utilizza il valore `DbUser` specificato nella proprietà di connessione `DbUser`.

Se la proprietà di connessione `DbUser` non specifica un valore, il driver utilizzerà il valore specificato nel profilo di connessione. Se neanche il profilo di connessione specifica un valore, il driver utilizzerà il valore dall'asserzione SAML.

## App\_ID

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID univoco fornito da Okta associato all'applicazione Amazon Redshift.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Okta.

## App\_Name

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome dell'applicazione Okta utilizzata per autenticare la connessione ad Amazon Redshift.

Questo parametro è facoltativo.

ApplicationName

- Valore predefinito: null
- Tipo di dati: stringa

Il nome dell'applicazione da passare ad Amazon Redshift a scopo di verifica.

Questo parametro è facoltativo.

AuthProfile

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del profilo di autenticazione da utilizzare per la connessione ad Amazon Redshift.

Questo parametro è facoltativo.

AutoCreate

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se il driver determina la creazione di un nuovo utente quando l'utente specificato non esiste.

Questo parametro è facoltativo.

true

Se l'utente specificato da DBUser o ID univoco (UID) non esiste, sarà creato un nuovo utente con tale nome.

false

Il driver non provoca la creazione di nuovi utenti. Se l'utente specificato non esiste, l'autenticazione avrà esito negativo.

## Client\_ID

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID client da usare durante l'autenticazione della connessione tramite il servizio Azure AD.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

## Client\_Secret

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il segreto client da usare durante l'autenticazione della connessione tramite il servizio Azure AD.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

## ClusterID

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del cluster Amazon Redshift a cui connettersi. Il driver prova a rilevare questo parametro dall'host specificato. Se utilizzi un Network Load Balancer (NLB) e una connessione tramite IAM, il driver non riuscirà a rilevarla, quindi puoi impostarla mediante questa opzione di connessione.

Questo parametro è facoltativo.

## Compressione

- Valore predefinito: off
- Tipo di dati: stringa

Il metodo di compressione utilizzato per la comunicazione del protocollo wire tra il server Amazon Redshift e il client o il driver.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

- lz4

Imposta il metodo di compressione utilizzato per la comunicazione del protocollo wire con Amazon Redshift su lz4.

- off

Non utilizza la compressione per la comunicazione del protocollo wire con Amazon Redshift.

`connectTimeout`

- Valore di default: 10
- Tipo di dati: numero intero

Il valore di timeout da utilizzare per le operazioni di connessione socket. Se il tempo necessario per stabilire una connessione Amazon Redshift supera questo valore, la connessione è considerata non disponibile. Il timeout è specificato in secondi. Un valore pari a 0 significa che non viene specificato alcun timeout.

Questo parametro è facoltativo.

`connectionTimezone`

- Valore predefinito: LOCAL
- Tipo di dati: stringa

Il fuso orario a livello di sessione.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

LOCAL

Configura il fuso orario a livello di sessione nel fuso orario LOCAL JVM.

## SERVER

Configura il fuso orario a livello di sessione sul fuso orario impostato per l'utente nel server Amazon Redshift. Puoi configurare i fusi orari a livello di sessione per gli utenti con il seguente comando:

```
ALTER USER  
[...]  
SET TIMEZONE TO [...];
```

### database MetadataCurrent DbOnly

- Valore predefinito: true
- Tipo di dati: booleano

Questa opzione specifica se l'API dei metadati recupera i dati da tutti i database accessibili o solo dal database connesso.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

true

L'applicazione recupera i metadati da un singolo database.

false

L'applicazione recupera i metadati da tutti i database accessibili.

### DbUser

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID utente da utilizzare con il proprio account Amazon Redshift. Puoi usare un ID che attualmente non esiste se hai abilitato la AutoCreate proprietà.

Questo parametro è facoltativo.

## DbGroups

- Valore predefinito: PUBLIC
- Tipo di dati: stringa

Un elenco separato da virgole di nomi di gruppo di database esistenti che DBUser unisce per la sessione corrente.

Questo parametro è facoltativo.

## DBNAME

- Valore predefinito: null
- Tipo di dati: stringa

Il nome del database a cui connettersi. Questa opzione può essere utilizzata per specificare il nome del database nell'URL di connessione JDBC.

Questo parametro è obbligatorio. Il nome del database va specificato nell'URL di connessione o nelle proprietà di connessione dell'applicazione client.

## RowFetchdimensione predefinita

- Valore predefinito: 0
- Tipo di dati: numero intero

Questa opzione specifica un valore predefinito per getFetchSize.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

0

Recupera tutte le righe in un'unica operazione.

Numero intero positivo

Numero di righe da recuperare dal database per ogni iterazione di recupero di. ResultSet

## DisableIsValidQuery

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se il driver invia una nuova query di database quando si utilizza il metodo `Connection.isValid()` per determinare se la connessione al database è attiva.

Questo parametro è facoltativo.

true

Il driver non invia una query quando si utilizza il metodo `Connection.isValid()` per determinare se la connessione al database è attiva. Ciò potrebbe far sì che il driver identifichi erroneamente la connessione al database come attiva se il server di database si è arrestato in modo imprevisto.

false

Il driver invia una query quando si utilizza il metodo `Connection.isValid()` per determinare se la connessione al database è attiva.

## abilita Buffer FetchRing

- Valore predefinito: true
- Tipo di dati: booleano

Questa opzione specifica che il driver recupera le righe utilizzando un buffer ad anello su un thread separato. Il parametro `fetchRingBufferSize` specifica la dimensione del ring buffer.

Se una transazione rileva uno `Statement` contenente più comandi SQL separati da punto e virgola, il `fetch ring buffer` per quella transazione è impostato su `false`. `enableFetchRing` il valore del buffer non cambia.

Questo parametro è facoltativo.

## abilitare MultiSql Support

- Valore predefinito: true
- Tipo di dati: booleano

Questa opzione specifica se elaborare più comandi SQL separati da punti e virgola in un'istruzione.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

true

Il driver elabora più comandi SQL, separati da punti e virgola, in un oggetto Statement.

false

Il driver restituisce un errore per più comandi SQL in una singola istruzione.

dimensione di recupero RingBuffer

- Valore predefinito: 1G
- Tipo di dati: stringa

Questa opzione specifica la dimensione del buffer ad anello utilizzato durante il recupero del set di risultati. È possibile specificare una dimensione in byte, ad esempio 1K per 1 KB, 5000 per 5.000 byte, 1M per 1 MB, 1G per 1 GB e così via. È inoltre possibile specificare una percentuale di memoria heap. Il driver smette di recuperare le righe al raggiungimento del limite. Il recupero riprende quando l'applicazione legge le righe e libera spazio nel buffer ad anello.

Questo parametro è facoltativo.

ForceLowercase

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se il driver mette in minuscolo tutti i gruppi di database (DbGroups) inviati dal provider di identità ad Amazon Redshift quando si utilizza l'autenticazione Single Sign-On.

Questo parametro è facoltativo.

true

Il driver converte in minuscolo i nomi di tutti i gruppi di database inviati dal provider di identità.

## false

Il driver non modifica i gruppi di database.

## groupFederation

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se utilizzare i gruppi IDP di Amazon Redshift. Questa funzionalità è supportata dall'API V2. `GetClusterCredentials`

Questo parametro è facoltativo.

## true

Utilizzare i gruppi di Identity Provider (IDP) di Amazon Redshift.

## false

Utilizza l'API STS e `GetClusterCredentials` per la federazione degli utenti e specifica esplicitamente `DbGroups` la connessione.

## HOST

- Valore predefinito: null
- Tipo di dati: stringa

Il nome host del server Amazon Redshift a cui connettersi. Questa opzione può essere utilizzata per specificare il nome host nell'URL di connessione JDBC.

Questo parametro è obbligatorio. Il nome host va specificato nell'URL di connessione o nelle proprietà di connessione dell'applicazione client.

## IAM DisableCache

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se le credenziali IAM vengono memorizzate nella cache.

Questo parametro è facoltativo.

true

Le credenziali IAM non sono memorizzate nella cache.

false

Le credenziali IAM sono memorizzate nella cache. Ciò migliora le prestazioni quando le richieste ad API Gateway sono limitate, ad esempio.

IAMDuration

- Valore predefinito: 900
- Tipo di dati: numero intero

Il periodo di tempo, in secondi, fino alla scadenza delle credenziali temporanee IAM.

- Valore minimo: 900
- Valore massimo: 3.600

Questo parametro è facoltativo.

Identity\_Namespace

- Valore predefinito: nessuno
- Tipo di dati: stringa

Lo spazio dei nomi di identità da utilizzare durante l'autenticazione tramite IdpTokenAuthPlugin. Consente a Redshift di determinare quale istanza Centro identità IAM utilizzare.

Questo parametro è facoltativo se esiste una sola istanza Centro identità IAM o se è impostato lo spazio dei nomi di identità predefinito. In caso contrario, è obbligatorio.

IdP\_Host

- Valore predefinito: nessuno

- Tipo di dati: stringa

L'host IdP (provider di identità) utilizzato per l'autenticazione in Amazon Redshift. Questo può essere specificato nella stringa di connessione o in un profilo.

Questo parametro è facoltativo.

#### IdP\_Port

- Valore predefinito: nessuno
- Tipo di dati: stringa

La porta utilizzata da un IdP (provider di identità). La porta può essere specificata nella stringa di connessione o in un profilo. La porta predefinita è 5439. A seconda della porta selezionata durante la creazione, la modifica o la migrazione del cluster, consenti l'accesso alla porta selezionata.

Questo parametro è facoltativo.

#### idp\_tenant

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID tenant di Azure AD per l'applicazione Amazon Redshift.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

#### IdP\_Response\_Timeout

- Valore predefinito: 120
- Tipo di dati: numero intero

La quantità di tempo, espressa in secondi, per cui il driver attende la risposta SAML dal provider di identità quando si usano i servizi SAML o Azure AD tramite un plug-in del browser.

Questo parametro è facoltativo.

#### IniFile

- Valore predefinito: nessuno

- Tipo di dati: stringa

Il percorso completo del file .ini, compreso il nome file. Ad esempio:

```
IniFile="C:\tools\rsjdbc.ini"
```

Per ulteriori informazioni sul file .ini, consultare [Creazione di file di inizializzazione \(.ini\) per il driver JDBC versione 2.1.](#)

Questo parametro è facoltativo.

### IniSection

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome di una sezione nel file .ini contenente le opzioni di configurazione. Per ulteriori informazioni sul file .ini, consultare [Creazione di file di inizializzazione \(.ini\) per il driver JDBC versione 2.1.](#)

Nell'esempio seguente viene specificata la sezione [Prod] del file .ini:

```
IniSection="Prod"
```

Questo parametro è facoltativo.

### isServerless

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione specifica se l'host endpoint di Amazon Redshift è un'istanza serverless. Il driver prova a rilevare questo parametro dall'host specificato. Se utilizzi un Network Load Balancer (NLB), il driver non riuscirà a rilevarlo, quindi puoi impostarlo qui.

Questo parametro è facoltativo.

true

L'host endpoint di Amazon Redshift è un'istanza serverless.

false

L'host endpoint di Amazon Redshift è un cluster con provisioning.

URL login\_

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'URL della risorsa sul sito Web del provider di identità quando si usa SAML o i servizi Azure AD tramite un plug-in del browser.

Questo parametro è obbligatorio se si esegue l'autenticazione con SAML o i servizi Azure AD tramite un plug-in del browser.

loginTimeout

- Valore predefinito: 0
- Tipo di dati: numero intero

Il numero di secondi da attendere prima del timeout durante la connessione e l'autenticazione con il server. Se stabilire la connessione richiede più tempo della soglia prevista, l'operazione viene interrotta.

Quando questa proprietà è impostata su 0, non si verifica il timeout delle connessioni.

Questo parametro è facoltativo.

effettuare il login ToRp

- Valore predefinito: urn:amazon:webservices
- Tipo di dati: stringa

La parte attendibile che si desidera utilizzare per il tipo di autenticazione AD FS.

Questo parametro è facoltativo.

LogLevel

- Valore predefinito: 0

- Tipo di dati: numero intero

Utilizzare questa proprietà per attivare o disattivare la registrazione nel driver e per specificare il livello di dettaglio incluso nei file di log.

Abilitare la registrazione abbastanza a lungo da rilevare un problema. La registrazione riduce le prestazioni e può richiedere una grande quantità di spazio su disco.

Questo parametro è facoltativo.

Impostare il parametro su uno dei seguenti valori:

0

Disabilitare la registrazione.

1

Abilitare la registrazione sul livello FATAL, che registra eventi di errore molto gravi che comportano l'interruzione del driver.

2

Abilitare la registrazione sul livello ERROR, che registra eventi di errore che potrebbero consentire al driver di restare in esecuzione.

3

Abilitare la registrazione sul livello WARNING, che registra eventi che potrebbero causare un errore se non viene eseguita un'azione.

4

Abilitare la registrazione sul livello INFO, che registra informazioni generali che descrivono l'avanzamento del driver.

5

Abilitare la registrazione sul livello DEBUG, che registra informazioni dettagliate utili per il debug del driver.

6

Abilitare la registrazione sul livello TRACE, che registra tutte le attività del driver.

Quando la registrazione è abilitata, il driver produce i seguenti file di log nella posizione specificata nella proprietà `LogPath`:

- **`redshift_jdbc.log`**: file che registra l'attività del driver che non è specifica di una connessione.
- **`redshift_jdbc_connection_[Number].log`**: file per ogni connessione effettuata al database, dove `[Number]` è un numero che distingue ogni file di log dagli altri. Questo file registra l'attività del driver specifica per la connessione.

Se il `LogPath` valore non è valido, il driver invia le informazioni registrate allo standard output stream, `System.out`

### `LogPath`

- Valore predefinito: la directory di lavoro corrente.
- Tipo di dati: stringa

Il percorso completo della cartella in cui il driver salva i file di registro quando la `LogLevel` proprietà DSI è abilitata.

Per assicurarsi che l'URL di connessione sia compatibile con tutte le applicazioni JDBC, si consiglia di eseguire l'escape sulle barre rovesciate (`\`) nel percorso del file digitando un'altra barra rovesciata.

Questo parametro è facoltativo.

### `OverrideSchemaPatternType`

- Valore predefinito: null
- Tipo di dati: numero intero

Questa opzione specifica se sovrascrivere il tipo di query utilizzata nelle chiamate `getTables`.

0

Nessuna query a schema universale

1

Query a schema locale

---

## 2

### Query a schema esterno

Questo parametro è facoltativo.

#### Partner\_SPID

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il valore SPID (ID del fornitore di servizi) del partner da utilizzare per l'autenticazione della connessione tramite il servizio. PingFederate

Questo parametro è facoltativo.

#### Password

- Valore predefinito: nessuno
- Tipo di dati: stringa

Quando si esegue la connessione con l'autenticazione IAM tramite un IDP, si tratta della password per il server IDP\_Host. Quando si utilizza l'autenticazione standard, questo può essere utilizzato per la password del database Amazon Redshift anziché per PWD.

Questo parametro è facoltativo.

#### Plugin\_Name

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome completo della classe che implementa un plug-in specifico del provider di credenziali.

Questo parametro è facoltativo.

Sono supportate le seguenti opzioni di provider:

- **AdfsCredentialsProvider**— Servizio Active Directory Federation.

- **AzureCredentialsProvider**— Servizio Microsoft Azure Active Directory (AD).
- **BasicJwtCredentialsProvider**— Servizio JSON Web Tokens (JWT).
- **BasicSamlCredentialsProvider** — Credenziali SAML (Security Assertion Markup Language) che è possibile utilizzare con molti provider di servizi SAML.
- **BrowserAzureCredentialsProvider**— Browser del servizio Microsoft Azure Active Directory (AD).
- **BrowserAzureOAuth2CredentialsProvider**— Browser Microsoft Azure Active Directory (AD) Service per l'autenticazione nativa.
- **BrowserSamlCredentialsProvider**— Browser SAML per servizi SAML come Okta, Ping o ADFS.
- **IdpTokenAuthPlugin**— Un plug-in di autorizzazione che accetta un token IAM Identity Center o token di identità (JWT) basati su JSON OpenID Connect (OIDC) da qualsiasi provider di identità Web collegato a IAM Identity Center.
- **OktaCredentialsProvider**— Servizio Okta.
- **PingCredentialsProvider**— PingFederate Assistenza.

## PORT

- Valore predefinito: null
- Tipo di dati: numero intero

La porta del server Amazon Redshift a cui connettersi. Questa opzione può essere utilizzata per specificare la porta nell'URL di connessione JDBC.

Questo parametro è facoltativo.

## preferred\_role

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il ruolo IAM che si desidera assumere durante la connessione ad Amazon Redshift.

Questo parametro è facoltativo.

## Profilo

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del profilo da utilizzare per l'autenticazione IAM. Questo profilo contiene eventuali proprietà di connessione aggiuntive non specificate nella stringa di connessione.

Questo parametro è facoltativo.

## PWD

- Valore predefinito: nessuno
- Tipo di dati: stringa

La password corrispondente al nome utente Amazon Redshift che fornisce utilizzando l'UID della proprietà.

Questo parametro è facoltativo.

## queryGroup

- Valore predefinito: null
- Tipo di dati: stringa

Questa opzione assegna una query a una coda in fase di runtime assegnando la query al gruppo di query appropriato. Il gruppo di query viene impostato per la sessione. Tutte le query eseguite sulla connessione appartengono a questo gruppo di query.

Questo parametro è facoltativo.

## readOnly

- Valore predefinito: false
- Tipo di dati: booleano

Questa proprietà specifica se il driver è in modalità di sola lettura.

Questo parametro è facoltativo.

true

La connessione è in modalità di sola lettura e non può scrivere nell'archivio dati.

false

La connessione non è in modalità di sola lettura e può scrivere nell'archivio dati.

Regione

- Valore predefinito: null
- Tipo di dati: stringa

Questa opzione specifica la AWS regione in cui si trova il cluster. Se si specifica l' `StsEndPoint` opzione, l'opzione Regione viene ignorata. L'API `GetClusterCredentials` Redshift utilizza anche l'opzione Regione.

Questo parametro è facoltativo.

Inseri rossi `WriteBatched`

- Valore predefinito: false
- Tipo di dati: booleano

Questa opzione abilita l'ottimizzazione per riscrivere e combinare istruzioni INSERT compatibili in batch.

Questo parametro è facoltativo.

re `WriteBatched InsertsSize`

- Valore predefinito: 128
- Tipo di dati: numero intero

Questa opzione abilita l'ottimizzazione per riscrivere e combinare istruzioni INSERT compatibili in batch. Questo valore deve aumentare esponenzialmente con potenza 2.

Questo parametro è facoltativo.

roleArn

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'Amazon Resource Name (ARN) del ruolo. Assicuratevi di specificare questo parametro quando BasicJwtCredentialsProvider specificate l'opzione Plugin\_Name. Specificare l'ARN nel seguente formato:

*arn:partition:service:region:account-id:resource-id*

Questo parametro è obbligatorio se specificate l'opzione BasicJwtCredentialsProvider Plugin\_Name.

ruolo SessionName

- Valore predefinito: jwt\_redshift\_session
- Tipo di dati: stringa

Un identificatore della sessione del ruolo assunto. In genere, si passa il nome o l'identificatore associato all'utente dell'applicazione. Le credenziali di sicurezza temporanee utilizzate dall'applicazione sono associate a tale utente. È possibile specificare questo parametro quando si specifica BasicJwtCredentialsProvider l'opzione Plugin\_Name.

Questo parametro è facoltativo.

scope

- Valore predefinito: nessuno
- Tipo di dati: stringa

Un elenco separato da spazi contenente ambiti ai quali l'utente può acconsentire. È possibile specificare questo parametro in modo che l'applicazione Microsoft Azure possa ottenere il consenso per le API che si desidera chiamare. È possibile specificare questo parametro quando si specifica BrowserAzure OAuth2 CredentialsProvider per l'opzione Plugin\_Name.

Questo parametro è obbligatorio per il plug-in OAuth2. BrowserAzure CredentialsProvider

## SecretAccessChiave

- Valore predefinito: nessuno
- Tipo di dati: stringa

La chiave di accesso IAM per l'utente o il ruolo. Se viene specificato, è necessario specificare anche l'AccessKeyID. Se passato nell'URL JDBC, SecretAccessKey deve essere codificato come URL.

Questo parametro è facoltativo.

## SessionToken

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il token di sessione IAM temporaneo associato al ruolo IAM utilizzato per l'autenticazione. Se passato nell'URL JDBC, il token di sessione IAM temporaneo deve essere con codifica URL.

Questo parametro è facoltativo.

## senza server AcctId

- Valore predefinito: null
- Tipo di dati: stringa

L'ID account di Amazon Redshift Serverless. Il driver prova a rilevare questo parametro dall'host specificato. Se utilizzi un Network Load Balancer (NLB), il driver non riuscirà a rilevarlo, quindi puoi impostarlo qui.

Questo parametro è facoltativo.

## senza server WorkGroup

- Valore predefinito: null
- Tipo di dati: stringa

Il nome del gruppo di lavoro di Amazon Redshift Serverless. Il driver prova a rilevare questo parametro dall'host specificato. Se utilizzi un Network Load Balancer (NLB), il driver non riuscirà a rilevarlo, quindi puoi impostarlo qui.

Questo parametro è facoltativo.

socketFactory

- Valore predefinito: null
- Tipo di dati: stringa

Questa opzione specifica una factory di socket per la creazione di socket.

Questo parametro è facoltativo.

socketTimeout

- Valore predefinito: 0
- Tipo di dati: numero intero

Il numero di secondi da attendere durante le operazioni di lettura del connettore prima del timeout. Se un'operazione richiede più tempo della soglia prevista, la connessione viene chiusa. Quando questa proprietà è impostata su 0, non si verifica il timeout della connessione.

Questo parametro è facoltativo.

SSL

- Valore predefinito: TRUE
- Tipo di dati: stringa

Utilizzare questa proprietà per attivare o disattivare SSL per la connessione.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

TRUE

Il driver si connette al server tramite SSL.

## FALSE

Il driver si connette al server senza utilizzare SSL. Questa opzione non è supportata con l'autenticazione IAM.

In alternativa, è possibile configurare la AuthMech proprietà.

### ssl\_insecure

- Valore predefinito: true
- Tipo di dati: stringa

Questa proprietà indica se il certificato del server host IDP deve essere verificato.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

true

Il driver non controlla l'autenticità del certificato del server IDP.

false

Il driver controlla l'autenticità del certificato del server IDP.

### SSLCert

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il percorso completo di un file .pem o .crt contenente ulteriori certificati emessi da una CA attendibili per verificare l'istanza del server Amazon Redshift quando si utilizza SSL.

Questo parametro è richiesto se è specificato SSLKey.

### SSLFactory

- Valore predefinito: nessuno

- Tipo di dati: stringa

L'SSL factory da utilizzare per la connessione al server tramite TLS/SSL senza utilizzare un certificato server.

### SSLKey

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il percorso completo del file con estensione .der contenente il file di chiave PKCS8 per la verifica dei certificati specificati in SSLCert.

Questo parametro è richiesto se è specificato SSLCert.

### SSLMode

- Valore predefinito: verify-ca
- Tipo di dati: stringa

Utilizzare questa proprietà per specificare il modo in cui il driver convalida i certificati quando TLS/SSL è abilitato.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

#### verify-ca

Il driver verifica che il certificato proviene da una certification authority (CA) attendibile.

#### verify-full

Il driver verifica che il certificato proviene da una CA attendibile e che il nome host nel certificato corrisponde al nome host specificato nell'URL di connessione.

### SSLPassword

- Valore predefinito: 0
- Tipo di dati: stringa

La password per il file della chiave crittografata specificato in SSLKey.

Questo parametro è obbligatorio se viene specificato SSLKey e il file della chiave è crittografato.

### SSL RootCert

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il percorso completo di un file .pem o .crt contenente ulteriori certificati emessi da una CA attendibili per verificare l'istanza del server Amazon Redshift quando si utilizza SSL.

### StsEndpointUrl

- Valore predefinito: null
- Tipo di dati: stringa

È possibile specificare un endpoint AWS Security Token Service (AWS STS). Se si specifica questa opzione, l'opzione Regione viene ignorata. Per questo endpoint è possibile specificare solo un protocollo sicuro (HTTPS).

### tcp KeepAlive

- Valore predefinito: TRUE
- Tipo di dati: stringa

Utilizzare questa proprietà per attivare o disattivare i keepalive TCP.

Questo parametro è facoltativo.

Puoi specificare le seguenti valori:

TRUE

Il driver utilizza i keepalive TCP al fine di impedire il timeout delle connessioni.

FALSE

Il driver non utilizza keepalive TCP.

## token

- Valore predefinito: nessuno
- Tipo di dati: stringa

Un token di accesso fornito da IAM Identity Center o un token Web JSON (JWT) OpenID Connect (OIDC) fornito da un provider di identità Web collegato a IAM Identity Center. L'applicazione deve generare questo token autenticando l'utente dell'applicazione con IAM Identity Center o un provider di identità collegato a IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## token\_type

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il tipo di token che viene utilizzato in. `IdpTokenAuthPlugin`

Puoi specificare le seguenti valori:

### ACCESS\_TOKEN

Inserisci questo valore se utilizzi un token di accesso fornito da IAM Identity Center.

### EXT\_JWT

Inserisci questo valore se utilizzi un JSON Web Token (JWT) OpenID Connect (OIDC) fornito da un provider di identità basato sul Web integrato con IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## UID

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome utente del database utilizzato per accedere al database.

Questo parametro è obbligatorio.

### Utente

- Valore predefinito: nessuno
- Tipo di dati: stringa

Quando ci si connette con l'autenticazione IAM tramite un IDP, questo è il nome utente per il server `idp_host`. Quando si utilizza l'autenticazione standard, può essere usato per il nome utente del database di Amazon Redshift.

Questo parametro è facoltativo.

### web IdentityToken

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il token di accesso OAuth 2.1 o un token ID OpenID Connect fornito dal provider di identità. L'applicazione deve ottenere questo token autenticando l'utente dell'applicazione con un provider di identità Web. Assicuratevi di specificare questo parametro quando `BasicJwtCredentialsProvider` specificate l'opzione `Plugin_Name`.

Questo parametro è obbligatorio se specificate l'opzione `BasicJwtCredentialsProvider Plugin_Name`.

### Versioni precedenti del driver JDBC versione 2.1

Scaricare una versione precedente del driver JDBC versione 2.1 di Amazon Redshift solo se lo strumento richiede una versione specifica del driver.

Questi sono i precedenti driver JDBC versione 2.1 compatibili con JDBC 4.2:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.28/redshift-jdbc42-2.1.0.28.zip>  
link: <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/drivers/jdbc/2.1.0.28/redshift-jdbc42-2.1.0.28.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.26/redshift-jdbc42-2.1.0.26.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.25/redshift-jdbc42-2.1.0.25.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.24/redshift-jdbc42-2.1.0.24.zip>

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.23/redshift-jdbc42-2.1.0.23.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.22/redshift-jdbc42-2.1.0.22.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.21/redshift-jdbc42-2.1.0.21.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.20/redshift-jdbc42-2.1.0.20.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.19/redshift-jdbc42-2.1.0.19.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.18/redshift-jdbc42-2.1.0.18.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.17/redshift-jdbc42-2.1.0.17.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.16/redshift-jdbc42-2.1.0.16.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.15/redshift-jdbc42-2.1.0.15.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.14/redshift-jdbc42-2.1.0.14.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.13/redshift-jdbc42-2.1.0.13.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.12/redshift-jdbc42-2.1.0.12.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.11/redshift-jdbc42-2.1.0.11.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.10/redshift-jdbc42-2.1.0.10.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.9/redshift-jdbc42-2.1.0.9.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.8/redshift-jdbc42-2.1.0.8.zip>
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.1.0.7/redshift-jdbc42-2.1.0.7.zip>

## Configurazione del connettore Python di Amazon Redshift

Utilizzando il connettore Amazon Redshift per Python, puoi integrare il lavoro con l' [AWS SDK for Python \(Boto3\)](#), oltre a [panda e Numerical Python](#) (). NumPy [Per ulteriori informazioni sui panda, consulta il repository pandas. GitHub](#) [Per ulteriori informazioni su NumPy, consulta il repository. NumPy GitHub](#)

Il connettore Amazon Redshift Python fornisce una soluzione open source. Puoi sfogliare il codice sorgente, richiedere miglioramenti, segnalare problemi e fornire contributi.

Per utilizzare il connettore Amazon Redshift Python, assicurati di avere Python versione 3.6 o successiva. Per ulteriori informazioni, consultare il [Contratto di patente di guida Amazon Redshift Python](#).

Il connettore Amazon Redshift Python fornisce quanto segue:

- AWS Identity and Access Management autenticazione (IAM). Per ulteriori informazioni, consulta [Identity and Access Management in Amazon Redshift](#).
- Autenticazione del provider di identità utilizzando l'accesso alle API federate. L'accesso alle API federate è supportato per i provider di identità aziendali, come i seguenti:
  - Azure AD. Per ulteriori informazioni, consulta il post sul blog AWS Big Data [Federate Amazon Redshift access with Microsoft Azure](#) AD Single Sign-on.
  - Active Directory Federation Service. Per ulteriori informazioni, consulta il post sul blog AWS Big Data [Federare l'accesso al cluster Amazon Redshift con Active Directory Federation Services \(AD FS\): Parte 1](#).
  - Okta. Per ulteriori informazioni, consulta il post sul blog AWS Big Data [Federate Amazon Redshift access with Okta come](#) provider di identità.
  - PingFederate. Per ulteriori informazioni, consulta il [PingFederate sito](#).
  - JumpCloud. Per ulteriori informazioni, consulta il [JumpCloud sito](#).
- Tipi di dati di Amazon Redshift.

Il connettore Amazon Redshift Python implementa Python Database API Specification 2.0. Per ulteriori informazioni, consultare [PEP 249—Specifica API del database Python v2.0](#) sul sito Web Python.

## Argomenti

- [Installazione del connettore Amazon Redshift Python](#)
- [Opzioni di configurazione per il connettore Amazon Redshift Python](#)
- [Importazione del connettore Python](#)
- [Integrazione del connettore Python con NumPy](#)
- [Integrazione del connettore Python con panda](#)
- [Utilizzo di plug-in del provider di identità](#)
- [Esempi di utilizzo del connettore Python Amazon Redshift](#)
- [Riferimento API per il connettore Python di Amazon Redshift](#)

## Installazione del connettore Amazon Redshift Python

Per installare il connettore Amazon Redshift Python, puoi utilizzare uno dei seguenti metodi:

- Indice dei pacchetti Python (PyPI)

- Conda
- Clonazione del repository GitHub

## Installazione del connettore Python da PyPI

Per installare il connettore Python da Python Package Index (PyPI), puoi usare pip. Per farlo, esegui il comando seguente.

```
>>> pip install redshift_connector
```

È possibile installare il connettore all'interno di un ambiente virtuale. Per farlo, esegui il comando seguente.

```
>>> pip install redshift_connector
```

Facoltativamente, puoi installare panda e con il connettore. NumPy

```
>>> pip install "redshift_connector[full]"
```

Per ulteriori informazioni su pip, consultare il [sito pip](#).

## Installazione del connettore Python da Conda

È possibile installare il connettore Python da Anaconda.org.

```
>>>conda install -c conda-forge redshift_connector
```

## Installazione del connettore Python clonando il repository da GitHub AWS

Per installare il connettore Python dal sorgente, clona il GitHub repository da AWS. Dopo aver installato Python e virtualenv, configurare l'ambiente e installare le dipendenze richieste eseguendo i seguenti comandi.

```
$ git clone https://github.com/aws/amazon-redshift-python-driver.git
$ cd RedshiftPythonDriver
$ virtualenv venv
$ . venv/bin/activate
$ python -m pip install -r requirements.txt
```

```
$ python -m pip install -e .  
$ python -m pip install redshift_connector
```

## Opzioni di configurazione per il connettore Amazon Redshift Python

Di seguito è possibile trovare le descrizioni per le opzioni che è possibile specificare per il connettore Python di Amazon Redshift.

### id\_chiave\_accesso

- Valore predefinito - nessuno
- Tipo di dati - stringa

La chiave di accesso per il ruolo IAM o l'utente IAM configurato per l'autenticazione database IAM.

Questo parametro è facoltativo.

### allow\_db\_user\_override

- Valore predefinito - falso
- Tipo di dati - booleano

### True

Specifica che il connettore utilizza il valore `DbUser1` dall'asserzione Security Assertion Markup Language (SAML).

### False

Specifica che viene usato il valore nel parametro di connessione `DbUser1`.

Questo parametro è facoltativo.

### Nome\_App

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome dell'applicazione del provider di identità (IdP) utilizzata per l'autenticazione.

Questo parametro è facoltativo.

`auth_profile`

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome di un profilo di autenticazione Amazon Redshift con proprietà di connessione come JSON. Per maggiori informazioni sulla denominazione dei parametri di connessione, vedere la classe `RedshiftProperty`. La classe `RedshiftProperty` memorizza i parametri di connessione forniti dall'utente finale e, se applicabile, generati durante il processo di autenticazione IAM (per esempio, credenziali IAM temporanee). [Per ulteriori informazioni, consultate la classe `RedshiftProperty`](#)

Questo parametro è facoltativo.

`auto_create`

- Valore predefinito - falso
- Tipo di dati - booleano

Un valore che indica se creare l'utente se l'utente non esiste.

Questo parametro è facoltativo.

`client_id`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'ID client da Azure IdP.

Questo parametro è facoltativo.

`client_secret`

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il client segreto da Azure IdP.

Questo parametro è facoltativo.

`cluster_identifier`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'identificatore del cluster del cluster Amazon Redshift.

Questo parametro è facoltativo.

`credentials_provider`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'IdP utilizzato per l'autenticazione con Amazon Redshift. I seguenti valori sono validi:

- `AdfsCredentialsProvider`
- `AzureCredentialsProvider`
- `BrowserAzureCredentialsProvider`
- `BrowserAzureOAuth2CredentialsProvider`
- `BrowserSamlCredentialsProvider`
- `IdpTokenAuthPlugin`— Un plug-in di autorizzazione che accetta un token Identity Center (iDC) o token di identità (JWT) basati su JSON OpenID Connect (OIDC) da qualsiasi provider di identità Web collegato all'iDC.
- `PingCredentialsProvider`
- `OktaCredentialsProvider`

Questo parametro è facoltativo.

`database`

- Valore predefinito - nessuno
- Tipo di dati - stringa

Scegliere il nome del database a cui connettersi.

Questo parametro è obbligatorio.

`database_metadata_current_db_only`

- Valore predefinito - vero
- Tipo di dati - booleano

Un valore che indica se un'applicazione supporta cataloghi multidatabase di condivisione dati. Il valore predefinito di True indica che l'applicazione non supporta i cataloghi multidatabase di condivisione dati per la compatibilità con le versioni precedenti.

Questo parametro è facoltativo.

`db_groups`

- Valore predefinito - nessuno
- Tipo di dati - stringa

Un elenco separato da virgole di nomi di gruppi di database esistenti a cui l'utente ha indicato si unisce alla sessione corrente. DbUser

Questo parametro è facoltativo.

`db_user`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'ID utente da utilizzare con Amazon Redshift.

Questo parametro è facoltativo.

`endpoint_url`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'URL dell'endpoint Amazon Redshift. Questa opzione è solo per uso interno. AWS

Questo parametro è facoltativo.

group\_federation

- Valore predefinito - falso
- Tipo di dati - booleano

Questa opzione specifica se utilizzare i gruppi IDP di Amazon Redshift.

Questo parametro è facoltativo.

true

Utilizzare i gruppi di Identity Provider (IDP) di Amazon Redshift.

false

Usa l'API STS e GetClusterCredentials per la federazione degli utenti e specifica db\_groups per la connessione.

host

- Valore predefinito - nessuno
- Tipo di dati - stringa

Nome host del cluster Amazon Redshift.

Questo parametro è facoltativo.

iam

- Valore predefinito - falso
- Tipo di dati - booleano

L'autenticazione IAM è abilitata.

Questo parametro è obbligatorio.

## iam\_disable\_cache

- Valore predefinito - falso
- Tipo di dati - booleano

Questa opzione specifica se le credenziali IAM vengono memorizzate nella cache. Per impostazione predefinita, le credenziali IAM sono memorizzate nella cache. Questo migliora le prestazioni quando le richieste al gateway API sono strozzate.

Questo parametro è facoltativo.

## identity\_namespace

- Valore predefinito: null
- Tipo di dati - stringa

Lo spazio dei nomi di identità da utilizzare durante l'autenticazione tramite IdpTokenAuthPlugin Aiuta Redshift a decidere quale istanza di Identity Center utilizzare.

Se esiste una sola istanza di Identity Center o se è impostato lo spazio dei nomi di identità predefinito, questo parametro è facoltativo. Altrimenti, è obbligatoria.

## idpPort

- Valore predefinito - 7890
- Tipo di dati - numero intero

La porta di ascolto a cui IdP invia l'asserzione SAML.

Questo parametro è obbligatorio.

## idP\_Response\_Timeout

- Valore predefinito – 120
- Tipo di dati - numero intero

Il timeout per il recupero dell'asserzione SAML da IdP.

Questo parametro è obbligatorio.

## idp\_tenant

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il tenant IdP.

Questo parametro è facoltativo.

## listen\_port

- Valore predefinito - 7890
- Tipo di dati - numero intero

La porta di ascolto a cui IdP invia l'asserzione SAML.

Questo parametro è facoltativo.

## login\_url

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'URL Single Sign-On per l'IdP.

Questo parametro è facoltativo.

## max\_prepared\_statement

- Valore predefinito: 1000
- Tipo di dati - numero intero

Il numero massimo di istruzioni preparate che possono essere aperte contemporaneamente.

Questo parametro è obbligatorio.

## numeric\_to\_float

- Valore predefinito - falso
- Tipo di dati - booleano

Questa opzione specifica se il connettore converte i valori del tipo di dati numerici da decimal.Decimal in float. Per impostazione predefinita, il connettore riceve i valori del tipo di dati numerici come decimal.Decimal e non li converte.

Non è consigliabile abilitare numeric\_to\_float per casi d'uso che richiedono precisione, poiché i risultati potrebbero essere arrotondati.

Per ulteriori informazioni su decimal.Decimal e i compromessi tra esso e float, consulta [decimal — Decimal fixed point and floating point arithmetic](#) (decimal — Decimale a punto fisso e aritmetica a virgola mobile) sul sito Web Python.

Questo parametro è facoltativo.

partner\_sp\_id

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'ID SP partner utilizzato per l'autenticazione con Ping.

Questo parametro è facoltativo.

password

- Valore predefinito - nessuno
- Tipo di dati - stringa

La password da utilizzare per l'autenticazione.

Questo parametro è facoltativo.

port

- Valore di default: 5439
- Tipo di dati - numero intero

Il numero della porta del cluster Amazon Redshift.

Questo parametro è obbligatorio.

## preferred\_role

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il ruolo IAM preferito per la connessione corrente.

Questo parametro è facoltativo.

## principal\_arn

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome della risorsa Amazon (ARN) dell'utente o del ruolo IAM per il quale si genera la policy. Si consiglia di collegare una policy a un ruolo e assegnare il ruolo all'utente per l'accesso.

Questo parametro è facoltativo.

## profilo

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome di un profilo in un file di AWS credenziali che contiene credenziali. AWS

Questo parametro è facoltativo.

## provider\_name

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome del Redshift Native Authentication Provider.

Questo parametro è facoltativo.

## Regione

- Valore predefinito - nessuno

- Tipo di dati - stringa

La posizione Regione AWS in cui si trova il cluster.

Questo parametro è facoltativo.

role\_arn

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'Amazon Resource Name (ARN) del ruolo che il chiamante sta assumendo. Questo parametro viene utilizzato dal provider indicato da `JwtCredentialsProvider`.

Per il provider `JwtCredentialsProvider`, questo parametro è obbligatorio. Questo parametro è facoltativo.

role\_session\_name

- Valore predefinito - sessione\_jwt\_redshift
- Tipo di dati - stringa

Un identificatore della sessione del ruolo assunto. In genere, si passa il nome o l'identificatore associato all'utente che sta utilizzando l'applicazione. Le credenziali di sicurezza temporanee utilizzate dall'applicazione sono associate a tale utente. Questo parametro viene utilizzato dal provider indicato da `JwtCredentialsProvider`.

Questo parametro è facoltativo.

scope

- Valore predefinito - nessuno
- Tipo di dati - stringa

Un elenco separato da spazi contenente ambiti a cui l'utente può acconsentire. È possibile specificare questo parametro in modo che l'applicazione possa ottenere il consenso per le API che si desidera chiamare. È possibile specificare questo parametro quando si specifica `BrowserAzure OAuth2 CredentialsProvider` per l'opzione `credentials_provider`.

Questo parametro è obbligatorio per il plug-in OAuth2. BrowserAzure CredentialsProvider

`secret_access_key_id`

- Valore predefinito - nessuno
- Tipo di dati - stringa

La chiave di accesso segreta per il ruolo IAM o l'utente configurato per l'autenticazione database IAM.

Questo parametro è facoltativo.

`session_token`

- Valore predefinito - nessuno
- Tipo di dati - stringa

La chiave di accesso per il ruolo IAM o l'utente IAM configurato per l'autenticazione database IAM.

Questo parametro è obbligatorio se vengono utilizzate AWS credenziali temporanee.

Questo parametro è facoltativo.

`serverless_acct_id`

- Valore predefinito - nessuno
- Tipo di dati - stringa

L'ID account di Amazon Redshift Serverless.

Questo parametro è facoltativo.

`serverless_work_group`

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome del gruppo di lavoro di Amazon Redshift Serverless.

Questo parametro è facoltativo.

## ssl

- Valore predefinito - vero
- Tipo di dati - booleano

Secure Sockets Layer (SSL) è abilitato.

Questo parametro è obbligatorio.

## ssl\_insecure

- Valore predefinito - vero
- Tipo di dati - booleano

Un valore che specifica se il certificato del server host IdP deve essere verificato.

Questo parametro è facoltativo.

## sslmode

- Valore predefinito - verify-ca
- Tipo di dati - stringa

La sicurezza della connessione ad Amazon Redshift. Puoi specificare uno dei seguenti:

- verify-ca
- verify-full

Questo parametro è obbligatorio.

## timeout

- Valore predefinito - nessuno
- Tipo di dati - numero intero

Il numero di secondi prima del timeout della connessione al server.

Questo parametro è facoltativo.

## token

- Valore predefinito: nessuno
- Tipo di dati: stringa

Un token di accesso fornito da IAM Identity Center o un token Web JSON (JWT) OpenID Connect (OIDC) fornito da un provider di identità Web collegato a IAM Identity Center. L'applicazione deve generare questo token autenticando l'utente dell'applicazione con IAM Identity Center o un provider di identità collegato a IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## token\_type

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il tipo di token che viene utilizzato in. `IdpTokenAuthPlugin`

Puoi specificare le seguenti valori:

### ACCESS\_TOKEN

Inserisci questo valore se utilizzi un token di accesso fornito da IAM Identity Center.

### EXT\_JWT

Inserisci questo valore se utilizzi un JSON Web Token (JWT) OpenID Connect (OIDC) fornito da un provider di identità basato sul Web integrato con IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## Utente

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il nome utente da utilizzare per l'autorizzazione.

Questo parametro è facoltativo.

## web\_identity\_token

- Valore predefinito - nessuno
- Tipo di dati - stringa

Il token di accesso OAuth 2.0 o un token ID OpenID Connect fornito dal provider di identità. Assicurarsi che l'applicazione ottenga questo token autenticando l'utente dell'applicazione con un provider di identità Web. Il provider indicato da `JwtCredentialsProvider` utilizza questo parametro.

Per il provider `JwtCredentialsProvider`, questo parametro è obbligatorio. Questo parametro è facoltativo.

## Importazione del connettore Python

Per importare il connettore Python, esegui il comando seguente.

```
>>> import redshift_connector
```

## Importazione NumPy e connessione ad Amazon Redshift

Per importare il connettore Amazon Redshift Python e Numerical Python (NumPy), esegui i seguenti comandi.

```
import redshift_connector
import numpy
```

Per connetterti a un cluster Amazon Redshift utilizzando AWS le credenziali, esegui il comando seguente.

```
conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)
```

## Integrazione del connettore Python con NumPy

Di seguito è riportato un esempio di integrazione del connettore Python con NumPy

```
>>> import numpy
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)

# Create a Cursor object
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")

result: numpy.ndarray = cursor.fetch_numpy_array()
print(result)
```

Di seguito è riportato il risultato.

```
[['One Hundred Years of Solitude' 'Gabriel García Márquez']
 ['A Brief History of Time' 'Stephen Hawking']]
```

## Integrazione del connettore Python con panda

Di seguito è riportato un esempio di integrazione del connettore Python con panda.

```
>>> import pandas

#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    port=5439,
    database='dev',
    user='awsuser',
    password='my_password'
)

# Create a Cursor object
```

```
>>> cursor = conn.cursor()

# Query and receive result set
cursor.execute("select * from book")
result: pandas.DataFrame = cursor.fetch_dataframe()
print(result)
```

## Utilizzo di plug-in del provider di identità

Per informazioni generali su come utilizzare i plugin del provider di identità, consultare [Opzioni per fornire credenziali IAM](#). Per ulteriori informazioni sulla gestione delle identità IAM, comprese le best practice per i ruoli IAM, consulta [Identity and Access Management in Amazon Redshift](#).

## Autenticazione tramite il plugin del provider di identità ADFS

Di seguito è riportato un esempio di utilizzo del plugin del provider di identità ADFS (Active Directory Federation Service) per autenticare un utente che si connette a un database Amazon Redshift.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AdfsCredentialsProvider',
    user='brooke@myadfshostname.com',
    password='Hunter2',
    idp_host='myadfshostname.com'
)
```

## Autenticazione tramite il plugin del provider di identità Azure

Di seguito è riportato un esempio di autenticazione utilizzando il plugin del provider di identità di Azure. È possibile creare valori per un `client_id` e `client_secret` per un'applicazione Azure Enterprise come illustrato di seguito.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='AzureCredentialsProvider',
    user='brooke@myazure.org',
```

```
password='Hunter2',
idp_tenant='my_idp_tenant',
client_id='my_client_id',
client_secret='my_client_secret',
preferred_role='arn:aws:iam:123:role/DataScientist'
)
```

## Autenticazione tramite il plugin del provider di identità Azure Browser

Di seguito è riportato un esempio di utilizzo del plugin del provider di identità del Browser Azure per autenticare un utente che si connette a un database Amazon Redshift.

L'autenticazione a più fattori avviene nel browser, dove le credenziali di accesso sono fornite dall'utente.

```
>>>con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserAzureCredentialsProvider',
    idp_tenant='my_idp_tenant',
    client_id='my_client_id',
)
```

## Autenticazione tramite il plugin del provider di identità Okta

Di seguito è riportato un esempio di autenticazione utilizzando il plugin del provider di identità di Okta. È possibile ottenere i valori per `idp_host`, `app_id` e `app_name` tramite l'applicazione Okta.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='OktaCredentialsProvider',
    user='brooke@myazure.org',
    password='hunter2',
    idp_host='my_idp_host',
    app_id='my_first_appetizer',
    app_name='dinner_party'
)
```

## Autenticazione tramite un JumpCloud plug-in generico SAML per il provider di identità del browser

Di seguito è riportato un esempio di utilizzo JumpCloud con un plug-in generico SAML per l'autenticazione del browser Identity Provider.

Il parametro password è obbligatorio. Tuttavia, non è necessario immettere questo parametro perché l'autenticazione a più fattori avviene nel browser.

```
>>> con = redshift_connector.connect(
    iam=True,
    database='dev',
    host='my-testing-cluster.abc.us-east-2.redshift.amazonaws.com',
    cluster_identifier='my-testing-cluster',
    credentials_provider='BrowserSamlCredentialsProvider',
    user='brooke@myjumpcloud.org',
    password='',
    login_url='https://sso.jumpcloud.com/saml2/plustwo_melody'
)
```

## Esempi di utilizzo del connettore Python Amazon Redshift

Di seguito sono riportati degli esempi di utilizzo del connettore Python Amazon Redshift. Per eseguirli, è prima necessario installare il connettore Python. Per ulteriori informazioni sull'installazione del connettore Amazon Redshift Python, consulta [Installazione del connettore Amazon Redshift Python](#). Per ulteriori informazioni sulle opzioni di configurazione che è possibile utilizzare con il connettore Python, consulta [Opzioni di configurazione per il connettore Amazon Redshift Python](#).

### Argomenti

- [Connessione e interrogazione di un cluster Amazon Redshift tramite credenziali AWS](#)
- [Abilitazione di autocommit](#)
- [Configurazione del paramstyle del cursore](#)
- [Utilizzo di COPY e UNLOAD rispettivamente per copiare e scrivere dati in un bucket Amazon S3](#)

## Connessione e interrogazione di un cluster Amazon Redshift tramite credenziali AWS

L'esempio seguente ti guida nella connessione a un cluster Amazon Redshift utilizzando AWS le tue credenziali, quindi nell'interrogazione di una tabella e nel recupero dei risultati della query.

```
#Connect to the cluster
```

```
>>> import redshift_connector
>>> conn = redshift_connector.connect(
    host='examplecluster.abc123xyz789.us-west-1.redshift.amazonaws.com',
    database='dev',
    port=5439,
    user='awsuser',
    password='my_password'
)

# Create a Cursor object
>>> cursor = conn.cursor()

# Query a table using the Cursor
>>> cursor.execute("select * from book")

#Retrieve the query result set
>>> result: tuple = cursor.fetchall()
>>> print(result)
>> (['One Hundred Years of Solitude', 'Gabriel García Márquez'], ['A Brief History of Time', 'Stephen Hawking'])
```

## Abilitazione di autocommit

La proprietà `autocommit` è disattivata per impostazione predefinita, seguendo la specifica dell'API del database Python. Per attivare la proprietà `autocommit` della connessione, è possibile utilizzare i comandi riportati di seguito dopo aver eseguito un comando di ripristino dello stato precedente per assicurarsi che non sia in corso una transazione.

```
#Connect to the cluster
>>> import redshift_connector
>>> conn = redshift_connector.connect(...)

# Run a rollback command
>>> conn.rollback()

# Turn on autocommit
>>> conn.autocommit = True
>>> conn.run("VACUUM")

# Turn off autocommit
>>> conn.autocommit = False
```

## Configurazione del paramstyle del cursore

Il paramstyle di un cursore può essere modificato utilizzando `cursor.paramstyle`. Il paramstyle predefinito usato è `format`. I valori validi per il paramstyle sono `qmark`, `numeric`, `named`, `format` e `pyformat`.

Di seguito sono riportati alcuni esempi di utilizzo di vari paramstyle per passare i parametri a un'istruzione SQL di esempio.

```
# qmark
redshift_connector.paramstyle = 'qmark'
sql = 'insert into foo(bar, jar) VALUES(?, ?)'
cursor.execute(sql, (1, "hello world"))

# numeric
redshift_connector.paramstyle = 'numeric'
sql = 'insert into foo(bar, jar) VALUES(:1, :2)'
cursor.execute(sql, (1, "hello world"))

# named
redshift_connector.paramstyle = 'named'
sql = 'insert into foo(bar, jar) VALUES(:p1, :p2)'
cursor.execute(sql, {"p1":1, "p2":"hello world"})

# format
redshift_connector.paramstyle = 'format'
sql = 'insert into foo(bar, jar) VALUES(%s, %s)'
cursor.execute(sql, (1, "hello world"))

# pyformat
redshift_connector.paramstyle = 'pyformat'
sql = 'insert into foo(bar, jar) VALUES(%(bar)s, %(jar)s)'
cursor.execute(sql, {"bar": 1, "jar": "hello world"})
```

Utilizzo di COPY e UNLOAD rispettivamente per copiare e scrivere dati in un bucket Amazon S3

L'esempio seguente mostra come copiare i dati da un bucket Amazon S3 in una tabella e quindi scaricarli da tale tabella nel bucket.

Un file di testo denominato `category_csv.txt` contenente i seguenti dati viene caricato in un bucket Amazon S3.

```
12,Shows,Musicals,Musical theatre
```

```
13,Shows,Plays,"All ""non-musical"" theatre"
14,Shows,Opera,"All opera, light, and ""rock"" opera"
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

Di seguito è riportato un esempio del codice Python, che per primo si connette al database Amazon Redshift. Quindi crea una tabella chiamata `category` e copia i dati CSV dal bucket S3 nella tabella.

```
#Connect to the cluster and create a Cursor
>>> import redshift_connector
>>> with redshift_connector.connect(...) as conn:
>>> with conn.cursor() as cursor:

#Create an empty table
>>> cursor.execute("create table category (catid int, cargroup varchar, catname
  varchar, catdesc varchar)")

#Use COPY to copy the contents of the S3 bucket into the empty table
>>> cursor.execute("copy category from 's3://testing/category_csv.txt' iam_role
  'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the table
>>> cursor.execute("select * from category")
>>> print(cursor.fetchall())

#Use UNLOAD to copy the contents of the table into the S3 bucket
>>> cursor.execute("unload ('select * from category') to 's3://testing/
  unloaded_category_csv.txt' iam_role 'arn:aws:iam::123:role/RedshiftCopyUnload' csv;")

#Retrieve the contents of the bucket
>>> print(cursor.fetchall())
>> ([12, 'Shows', 'Musicals', 'Musical theatre'], [13, 'Shows', 'Plays', 'All "non-
  musical" theatre'], [14, 'Shows', 'Opera', 'All opera, light, and "rock" opera'], [15,
  'Concerts', 'Classical', 'All symphony, concerto, and choir concerts'])
```

Se `autocommit` non è impostato su `True`, esegui il `commit()` dopo aver eseguito le istruzioni `execute()`.

I dati vengono scaricati nel file `unloaded_category_csv.text0000_part00` nel bucket S3 contenente quanto segue:

```
12,Shows,Musicals,Musical theatre
13,Shows,Plays,"All ""non-musical"" theatre"
```

```
14,Shows,Opera,"All opera, light, and ""rock"" opera"  
15,Concerts,Classical,"All symphony, concerto, and choir concerts"
```

## Riferimento API per il connettore Python di Amazon Redshift

Di seguito, puoi trovare una descrizione delle operazioni API del connettore Python di Amazon Redshift.

### `redshift_connector`

Di seguito è riportata una descrizione dell'operazione API `redshift_connector`.

```
connect(user, database, password[, port, ...])
```

Stabilisce una connessione a un cluster Amazon Redshift. Questa funzione convalida l'input dell'utente, facoltativamente si autentica utilizzando un plugin del provider di identità e quindi crea un oggetto di connessione.

### `apilevel`

Il livello DBAPI supportato, attualmente "2.0".

```
paramstyle, str(object='') -> str str(bytes_or_buffer[, encoding[, errors]])  
-> str
```

Lo stile dei parametri API del database da utilizzare a livello globale.

## Connessione

Di seguito, puoi trovare una descrizione delle operazioni API di connessi per il connettore Python di Amazon Redshift.

```
__init__(user, password, database[, host, ...])
```

Inizializza un oggetto di connessione raw.

### `cursor`

Crea un oggetto cursore associato a questa connessione.

### `commit`

Esegue il commit della transazione corrente del database.

## rollback

Ripristina la transazione corrente del database.

## close

Chiude la connessione del database.

## execute(cursor, operation, vals)

Esegue i comandi SQL specificati. È possibile fornire i parametri come sequenza o come mappatura, a seconda del valore di `redshift_connector.paramstyle`.

## run(sql[, stream])

Esegue i comandi SQL specificati. In alternativa, puoi fornire un flusso da utilizzare con il comando COPY.

## xid(format\_id, global\_transaction\_id, ...)

Crea un ID transazione. Solo il parametro `global_transaction_id` è usato in postgres. `format_id` e `branch_qualifier` non vengono utilizzati in postgres. La `global_transaction_id` può essere qualsiasi identificatore di stringa supportato da postgres che restituisce una tupla (`format_id, global_transaction_id, branch_qualifier`).

## tpc\_begin(xid)

Inizia una transazione TPC con un ID transazione `xid` costituito da un ID formato, un ID transazione globale e un qualificatore di filiale.

## tpc\_prepare

Esegue la prima fase di una transazione iniziata con `.tpc_begin`.

## tpc\_commit([xid])

Quando viene chiamato senza argomenti, `.tpc_commit` commette una transazione TPC precedentemente preparata con `.tpc_prepare ()`.

## tpc\_rollback([xid])

Quando viene chiamato senza argomenti, `.tpc_rollback` ripristina una transazione TPC.

## tpc\_recover

Restituisce un elenco di ID transazione in sospeso adatti all'uso con `.tpc_commit (xid)` o `.tpc_rollback (xid)`.

## Cursore

Di seguito, potete trovare una descrizione dell'operazione API del cursore.

```
__init__(connection[, paramstyle])
```

Inizializza un oggetto cursore non elaborato.

```
insert_data_bulk(filename, table_name, parameter_indices, column_names,  
delimiter, batch_size)
```

Esegue un'istruzione INSERT in blocco.

```
execute(operation[, args, stream, ...])
```

Esegue un'operazione di database.

```
executemany(operation, param_sets)
```

Prepara un'operazione di database e quindi la esegue per tutte le sequenze di parametri o mappature fornite.

```
fetchone
```

Recupera la riga successiva di un set di risultati della query.

```
fetchmany([num])
```

Recupera il prossimo set di righe del risultato di una query.

```
fetchall
```

Recupera tutte le righe rimanenti di un risultato di una query.

```
close
```

Chiude il cursore adesso.

```
__iter__
```

Un oggetto cursore può essere iterato per recuperare le righe da una query.

```
fetch_dataframe([num])
```

Restituisce un dataframe dei risultati dell'ultima query.

```
write_dataframe(df, table)
```

Scrive lo stesso dataframe della struttura in un database Amazon Redshift.

```
fetch_numpy_array([num])
```

Restituisce una NumPy matrice dei risultati dell'ultima query.

```
get_catalogs
```

Amazon Redshift non supporta più cataloghi provenienti da una singola connessione. Amazon Redshift restituisce solo il catalogo corrente.

```
get_tables([catalog, schema_pattern, ...])
```

Restituisce le tabelle pubbliche univoche definite dall'utente all'interno del sistema.

```
get_columns([catalog, schema_pattern, ...])
```

Restituisce un elenco di tutte le colonne di una tabella specifica in un database Amazon Redshift.

### AdfsCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del AdfsCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.AdfsCredentialsProvider()
```

### AzureCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del AzureCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.AzureCredentialsProvider()
```

### BrowserAzureCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del BrowserAzureCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.BrowserAzureCredentialsProvider()
```

## BrowserSamlCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del BrowserSamlCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.BrowserSamlCredentialsProvider()
```

## OktaCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del OktaCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.OktaCredentialsProvider()
```

## PingCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del PingCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.PingCredentialsProvider()
```

## SamlCredentialsProvider plugin

Di seguito è riportata la sintassi per il funzionamento dell'API del SamlCredentialsProvider plug-in per il connettore Amazon Redshift Python.

```
redshift_connector.plugin.SamlCredentialsProvider()
```

## Integrazione con Amazon Redshift per Apache Spark

[Apache Spark](#) è un framework di elaborazione distribuito e un modello di programmazione che ti aiuta ad eseguire attività come machine learning, elaborazione di flussi o analisi di grafici. Come Apache Hadoop, Spark è un sistema di elaborazione distribuito open source utilizzato in genere per carichi di lavoro di Big Data. Spark dispone di un motore di esecuzione basato su grafo aciclico orientato

(DAG) ottimizzato e memorizza attivamente i dati nella cache. Ciò può migliorare le prestazioni, in particolare per determinati algoritmi e per le query interattive.

Questa integrazione ti fornisce un connettore Spark che puoi usare per creare applicazioni Apache Spark in grado di leggere e scrivere dati in Amazon Redshift e Amazon Redshift serverless. Queste applicazioni non compromettono le prestazioni delle applicazioni o la coerenza transazionale dei dati. Questa integrazione è inclusa automaticamente in [Amazon EMR](#) e [AWS Glue](#), pertanto puoi eseguire immediatamente i processi di Apache Spark che accedono e caricano i dati in Amazon Redshift nell'ambito delle tue pipeline di importazione e trasformazione dei dati.

Al momento, con questa integrazione puoi utilizzare le versioni 3.3.0, 3.3.1, 3.3.2 e 3.4.0 di Spark.

Questa integrazione fornisce quanto segue:

- AWS Identity and Access Management (IAM) autenticazione. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).
- Pushdown dei predicati e delle query per migliorare le prestazioni.
- Tipi di dati di Amazon Redshift.
- Connettività ad Amazon Redshift e Amazon Redshift serverless.

Considerazioni e limitazioni relative all'utilizzo del connettore Spark

- La URI tempdir punta a una posizione Amazon S3. Questa directory temporanea non viene pulita automaticamente e potrebbe comportare costi aggiuntivi. Si consiglia di utilizzare le [Policy del ciclo di vita di Amazon S3](#) nella Amazon Simple Storage Service User Guide (Guida per l'utente di Amazon Simple Storage Service) per definire le regole di conservazione del bucket Amazon S3.
- Per impostazione predefinita, le copie tra Amazon S3 e Redshift non funzionano se il bucket S3 e il cluster Redshift si trovano in regioni AWS diverse. Per utilizzare regioni AWS separate, imposta il parametro tempdir\_region sulla regione del bucket S3 utilizzato per tempdir.
- Scritture tra regioni tra S3 e Redshift se si scrivono dati Parquet utilizzando il parametro tempformat.
- Si consiglia di utilizzare [Crittografia lato server di Amazon S3](#) per crittografare i bucket Amazon S3 utilizzati.
- Si consiglia di [bloccare l'accesso pubblico ai bucket Amazon S3](#).
- Si consiglia di non rendere accessibile pubblicamente il cluster Amazon Redshift.
- Si consiglia di abilitare la [registrazione dell'audit di Amazon Redshift](#).

- Si consiglia di abilitare la [crittografia dei dati inattivi di Amazon Redshift](#).
- Si consiglia di abilitare SSL per la connessione JDBC da Spark su Amazon EMR ad Amazon Redshift.
- Si consiglia di passare un ruolo IAM utilizzando il parametro `aws_iam_role` per il parametro di autenticazione di Amazon Redshift.

## Autenticazione con il connettore Spark

Il diagramma seguente descrive l'autenticazione tra Amazon S3, Amazon Redshift, il driver Spark e gli executor Spark.

## Autenticazione tra Redshift e Spark

Puoi utilizzare il driver JDBC versione 2 fornito da Amazon Redshift per connetterti ad Amazon Redshift con il connettore Spark specificando le credenziali di accesso. Per utilizzare IAM, [configura il tuo URL JDBC per l'utilizzo dell'autenticazione IAM](#). Per connetterti a un cluster Redshift da Amazon EMR o AWS Glue, assicurati che il tuo ruolo IAM disponga delle autorizzazioni necessarie per recuperare le credenziali IAM temporanee. L'elenco seguente descrive tutte le autorizzazioni necessarie al tuo ruolo IAM per recuperare le credenziali ed eseguire le operazioni di Amazon S3.

- [Redshift:GetClusterCredentials](#) (per cluster Redshift con provisioning)
- [Redshift:DescribeClusters](#) (per cluster Redshift con provisioning)
- [Redshift:GetWorkgroup](#) (per gruppi di lavoro Amazon Redshift serverless)
- [Redshift:GetCredentials](#) (per gruppi di lavoro Amazon Redshift Serverless)
- [s3:ListBucket](#)
- [s3:GetBucket](#)
- [s3:GetObject](#)
- [s3:PutObject](#)
- [s3:GetBucketLifecycleConfiguration](#)

Per ulteriori informazioni su `GetClusterCredentials`, consulta [Policy delle risorse per GetClusterCredentials](#).

Inoltre, devi assicurarti che Amazon Redshift possa assumere il ruolo IAM durante le operazioni COPY e UNLOAD.

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

Se utilizzi il driver JDBC più recente, esso gestirà automaticamente la transizione da un certificato autofirmato Amazon Redshift a un certificato ACM. Tuttavia, è necessario [specificare le opzioni SSL per l'URL JDBC](#).

Di seguito è riportato un esempio di come specificare URL del driver JDBC e `aws_iam_role` per la connessione ad Amazon Redshift.

```
df.write \
  .format("io.github.spark_redshift_community.spark.redshift ") \
  .option("url", "jdbc:redshift:iam://<the-rest-of-the-connection-string>") \
  .option("dbtable", "<your-table-name>") \
  .option("tempdir", "s3a://<your-bucket>/<your-directory-path>") \
  .option("aws_iam_role", "<your-aws-role-arn>") \
  .mode("error") \
  .save()
```

## Autenticazione tra Amazon S3 e Spark

Se utilizzi un ruolo IAM per l'autenticazione tra Spark e Amazon S3, usa uno dei seguenti metodi:

- L'SDK AWS per Java tenterà automaticamente di trovare le credenziali AWS utilizzando la catena di provider di credenziali predefinita implementata dalla classe `DefaultAWSCredentialsProviderChain`. Per ulteriori informazioni, consulta [Utilizzo della catena di provider delle credenziali predefinita](#).
- È possibile specificare le chiavi AWS tramite le [proprietà di configurazione di Hadoop](#). Ad esempio, se la configurazione `tempdir` punta a un file system `s3n://`, imposta le proprietà `fs.s3n.awsAccessKeyId` e `fs.s3n.awsSecretAccessKey` in un file di configurazione XML di

Hadoop o chiama `sc.hadoopConfiguration.set()` per modificare la configurazione Hadoop globale di Spark.

Ad esempio, se utilizzi il file system s3n, aggiungi:

```
sc.hadoopConfiguration.set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3n.awsSecretAccessKey", "YOUR_SECRET_ACCESS_KEY")
```

Per il file system s3a, aggiungi:

```
sc.hadoopConfiguration.set("fs.s3a.access.key", "YOUR_KEY_ID")
sc.hadoopConfiguration.set("fs.s3a.secret.key", "YOUR_SECRET_ACCESS_KEY")
```

Se utilizzi Python, utilizza le seguenti operazioni:

```
sc._jsc.hadoopConfiguration().set("fs.s3n.awsAccessKeyId", "YOUR_KEY_ID")
sc._jsc.hadoopConfiguration().set("fs.s3n.awsSecretAccessKey",
  "YOUR_SECRET_ACCESS_KEY")
```

- Codifica le chiavi di autenticazione nell'URL `tempdir`. Ad esempio, l'URI `s3n://ACCESSKEY:SECRETKEY@bucket/path/to/temp/dir` codifica la coppia di chiavi (ACCESSKEY, SECRETKEY).

## Autenticazione tra Redshift e Amazon S3

Se utilizzi i comandi COPY e UNLOAD nella query, devi anche concedere ad Amazon S3 l'accesso ad Amazon Redshift per eseguire le query per tuo conto. A tale scopo, per prima cosa [autorizza Amazon Redshift ad accedere ad altri servizi AWS](#), quindi autorizza le [operazioni COPY e UNLOAD utilizzando i ruoli IAM](#).

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

## Integrazione con AWS Secrets Manager

Puoi recuperare le credenziali del nome utente e della password di Redshift da un segreto archiviato in AWS Secrets Manager. Per fornire automaticamente le credenziali Redshift, utilizza il parametro

`secret.id`. Per ulteriori informazioni su come creare un segreto per le credenziali Redshift, consulta [Creazione di un segreto del database AWS Secrets Manager](#).

GroupID	ArtifactID	Revisioni supportate	Descrizione
com.amazonaws.secretsmanager	aws-secretsmanager-jdbc	1.0.12	La SQL Connection Library for Java di AWS Secrets Manager consente agli sviluppatori Java di connettersi facilmente ai database SQL utilizzando segreti archiviati in AWS Secrets Manager.

#### Note

Questa documentazione contiene codice e linguaggio di esempio sviluppati da [Apache Software Foundation](#) con [licenza Apache 2.0](#).

## Miglioramenti delle prestazioni con pushdown

Il connettore Spark applica automaticamente il pushdown dei predicati e delle query per ottimizzare le prestazioni. Questo significa che se utilizzi una funzione supportata nella tua query, il connettore Spark trasformerà la funzione in una query SQL ed eseguirà la query in Amazon Redshift. Questa ottimizzazione comporta il recupero di una quantità inferiore di dati, per cui Apache Spark dovrà elaborare meno dati e offrirà prestazioni migliori. Il pushdown è attivato automaticamente per impostazione predefinita. Per disattivarlo, imposta `autopushdown` su `False`.

```
import sqlContext.implicits._val
sample= sqlContext.read
    .format("io.github.spark_redshift_community.spark.redshift")
    .option("url",jdbcURL )
    .option("tempdir", tempS3Dir)
```

```
.option("dbtable", "event")  
.option("autopushdown", "false")  
.load()
```

Le seguenti funzioni sono supportate con il pushdown attivato. Se utilizzi una funzione non presente in questo elenco, il connettore Spark eseguirà la funzione in Spark anziché in Amazon Redshift e di conseguenza si avranno prestazioni non ottimizzate. Per un elenco completo delle funzioni in Spark, consulta la pagina relativa alle [funzioni integrate](#).

- Funzioni di aggregazione

- avg
- count
- max
- min
- sum
- stddev\_samp
- stddev\_pop
- var\_samp
- var\_pop

- Operatori booleani

- in
- isnull
- isnotnull
- contiene
- endswith
- startswith

- Operatori logici

- e
- oppure
- not (or !)

- Funzioni matematiche

- +
- -

- \*
- /
- - (unary)
- abs
- acos
- asin
- atan
- ceil
- cos
- exp
- floor
- greatest
- least
- log10
- pi
- pow
- round
- sin
- sqrt
- tan
- Funzioni varie
  - cast
  - coalesce
  - decimal
  - if
  - in
- Operatori relazionali
  - !=
  - =
  - >

- >=
- <
- <=
- Funzioni stringa
  - ascii
  - lpad
  - rpad
  - translate
  - upper
  - lower
  - length
  - trim
  - ltrim
  - rtrim
  - like
  - substring
  - concat
- Funzioni di data e ora
  - add\_months
  - date
  - date\_add
  - date\_sub
  - date\_trunc
  - timestamp
  - trunc
- Operazioni matematiche
  - CheckOverflow
  - PromotePrecision
- Operazioni relazionali
  - Alias (ad esempio, AS)

- CaseWhen
- Distinct
- InSet
- Joins e cross join
- Limiti
- Unions, union all
- ScalarSubquery
- Ordinamento (crescente e decrescente)
- UnscaledValue

### Altre opzioni di configurazione

#### Modifica la dimensione massima delle colonne di stringhe

Redshift crea colonne di stringhe come colonne di testo durante la creazione di tabelle, che vengono archiviate come VARCHAR(256). Se desideri colonne che supportino dimensioni maggiori, puoi usare `maxlength` per specificare la lunghezza massima delle colonne di stringhe. Di seguito è riportato un esempio di come specificare `maxlength`:

```
columnLengthMap.foreach { case (colName, length) =>
  val metadata = new MetadataBuilder().putLong("maxlength", length).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

#### Impostazione di un tipo di colonna

Per impostare un tipo di colonna, utilizza il campo `redshift_type`.

```
columnTypeMap.foreach { case (colName, colType) =>
  val metadata = new MetadataBuilder().putString("redshift_type", colType).build()
  df = df.withColumn(colName, df(colName).as(colName, metadata))
}
```

#### Impostazione di una codifica di compressione su una colonna

Per utilizzare una codifica di compressione specifica su una colonna, utilizza il campo di codifica. Per un elenco completo delle codifiche di compressione supportate, consulta [Codifiche di compressione](#).

## Creazione di una descrizione per una colonna

Per creare una descrizione, utilizza il campo `description`.

## Autenticazione tra Redshift e Amazon S3

Per impostazione predefinita, il risultato viene scaricato su Amazon S3 nel formato Parquet. Per scaricare il risultato come file di testo delimitato da pipe, specifica la seguente opzione.

```
.option("unload_s3_format", "TEXT")
```

## Esecuzione lenta di istruzioni pushdown

Parametro	Obbligatorio	Predefinito	Descrizione
<code>spark.datasource.redshift.community.autopushdown.lazyMode</code>	No	True	<p>Specifica se il connettore deve eseguire lentamente le istruzioni pushdown di Redshift.</p> <p>Se impostato su <code>true</code>, il connettore spark recupera tutti i modelli e le informazioni correlati prima di eseguire la query, il che in genere offre prestazioni migliori.</p> <p>Se <code>false</code>, il connettore e spark esegue le istruzioni pushdown immediatamente nel thread principale del driver Spark e viene serializzato tra le espressioni.</p>

## Parametri dei connettori

La mappa dei parametri o `OPTIONS` in Spark SQL supporta le seguenti impostazioni.

Parametro	Obbligatorio	Predefinito	Descrizione
<code>dbtable</code>	Sì, a meno che non venga specificata la query	N/D	La tabella da cui creare o da cui leggere in Redshift. Questo parametro è obbligatorio per il salvataggio dei dati su Redshift.
<code>query</code>	Sì, a meno che non sia specificato <code>dbtable</code>	N/D	La query da cui leggere in Redshift.
<code>user</code>	No	N/D	Il nome utente in Redshift. Deve essere utilizzato con il parametro <code>password</code> . Valido solo se l'utente e la password non sono parametri nell'URL. L'utilizzo di entrambi genera un errore.
<code>password</code>	No	N/D	La password in Redshift. Deve essere utilizzata con il parametro <code>utente</code> . Valido solo se l'utente e la password non sono parametri nell'URL.

Parametro	Obbligatorio	Predefinito	Descrizione
			L'utilizzo di entrambi genera un errore.

Parametro	Obbligatorio	Predefinito	Descrizione
url	No	N/D	<p>Un URL JDBC.</p> <p>Il formato è is jdbc:subprotocol:// host:port/database? user=username&amp;pa ssword=password.</p> <p>Il sottoprotocollo può essere postgresq l o Redshift, a seconda di quale driver JDBC è stato caricato. È important e notare che un driver compatibile con Redshift deve essere nel classpath e corrispondere a questo URL.</p> <p>L'host e la porta devono puntare al nodo principal e di Redshift, quindi è necessario configurare i gruppi di sicurezza e/o il VPC per consentir e l'accesso dall'appl icazione del driver.</p> <p>Database è il nome del database Redshift.</p>

Parametro	Obbligatorio	Predefinito	Descrizione
			Utente e password sono le credenziali per accedere al database che devono essere incorporate in questo URL per JDBC e l'utente del database deve disporre delle autorizzazioni necessarie per accedere alla tabella.
aws_iam_role	Solo se si utilizzano i ruoli IAM per autorizzare le operazioni COPY/UNLOAD di Redshift	N/D	ARN intero del ruolo IAM collegato al cluster Redshift.

Parametro	Obbligatorio	Predefinito	Descrizione
forward_spark_s3_credentials	No	False	Indica se questa libreria deve rilevare automaticamente le credenziali utilizzate e da Spark per connettersi ad Amazon S3 e se deve inoltrarle a Redshift tramite il driver JDBC. Queste credenziali vengono inviate nell'ambito della query JDBC. Pertanto, è consigliabile abilitare la crittografia SSL con connessione JDBC quando si utilizza questa opzione.
temporary_aws_access_key_id	No	N/D	Chiave di accesso AWS Sono necessari e le autorizzazioni di scrittura per il bucket S3.
temporary_aws_secret_access_key	No	N/D	La chiave di accesso segreta AWS corrispondente alla chiave di accesso.
temporary_aws_session_token	No	N/D	Token di sessione AWS corrispondente alla chiave di accesso fornita.

Parametro	Obbligatorio	Predefinito	Descrizione
tempdir	No	N/D	Una posizione scrivibile in Amazon S3. Questo parametro viene utilizzato per scaricare i dati durante la lettura e per caricare i dati Avro in Redshift durante la scrittura. Se utilizzi un'origin e dati Redshift per Spark nell'ambito di una normale pipeline ETL, può essere utile impostare una <a href="#">policy del ciclo di vita</a> su un bucket e utilizzarla come posizione temporanea per questi dati.

Parametro	Obbligatorio	Predefinito	Descrizione
jdbcdriver	No	Viene determinato dal sottoprotocollo dell'URL JDBC	Il nome della classe del driver JDBC da utilizzare. Questa classe deve trovarsi nel classpath . Nella maggior parte dei casi, non dovrebbe essere necessario specificare questa opzione, poiché il nome della classe del driver appropriato dovrebbe essere determinato automaticamente dal sottoprotocollo dell'URL JDBC.
diststyle	No	Even	Lo <a href="#">stile di distribuzione</a> Redshift da utilizzare durante la creazione di una tabella. Le opzioni valide sono EVEN, KEY o ALL. Quando si utilizza KEY, è necessario impostare anche una chiave di distribuzione con l'opzione distkey.

Parametro	Obbligatorio	Predefinito	Descrizione
distkey	No, a meno che non si utilizzi DISTSTYLE _KEY	N/D	Il nome di una colonna della tabella da utilizzare come chiave di distribuzione durante la creazione di una tabella.
sortkeyspec	No	N/D	Una definizione completa della <a href="#">chiave di ordinamento</a> Redshift.
include_column_list	No	False	Indica se la libreria deve estrarre automaticamente le colonne dallo schema e aggiungerle al comando COPY in base alle <a href="#">opzioni di mappatura delle colonne</a> .

Parametro	Obbligatorio	Predefinito	Descrizione
description	No	N/D	Una descrizione della tabella. La descrizione viene impostata con il comando SQL COMMENT e viene visualizzata nella maggior parte degli strumenti di query. Consulta i metadati <code>description</code> per impostare le descrizioni sulle singole colonne.

Parametro	Obbligatorio	Predefinito	Descrizione
preactions	No	N/D	Un elenco di comandi SQL delimitato da punto e virgola da eseguire prima di caricare il comando COPY. Potrebbe essere utile eseguire comandi DELETE o simili prima di caricare nuovi dati. Se il comando contiene %s, il nome della tabella verrà formattato prima dell'esecuzione (nel caso in cui si utilizzi una tabella di gestione temporanea). Se questo comando ha esito negativo, viene considerato un'eccezione. Se si utilizza una tabella di gestione temporanea, le modifiche verranno annullate e verrà ripristinata la tabella di backup se le azioni preliminari hanno esito negativo.

Parametro	Obbligatorio	Predefinito	Descrizione
extracopyoptions	No	N/D	<p>Un elenco di opzioni ulteriori da aggiungere e al comando COPY di Redshift durante il caricamento dei dati (ad esempio, TRUNCATECOLUMNS o MAXERROR n).</p> <p>Vedi <a href="#">Parametro opzionale</a> per un elenco completo dei parametri disponibili.</p> <p>È importante notare che, poiché queste opzioni vengono aggiunte alla fine del comando COPY, è possibile utilizzare e solo le opzioni rilevanti alla fine del comando. Questo dovrebbe coprire la maggior parte dei casi d'uso possibili.</p>

Parametro	Obbligatorio	Predefinito	Descrizione
sse_kms_key	No	N/D	L'ID della chiave AWS KMS da utilizzare per la crittografia lato server in S3 durante l'operazione UNLOAD di Redshift anziché la crittografia AWS predefinita. Il ruolo IAM di Redshift deve avere accesso alla chiave KMS per le operazioni di scrittura e il ruolo IAM di Spark deve avere accesso alla chiave per le operazioni di lettura. La lettura dei dati crittografati non richiede modifiche (di questo si occupa AWS), purché il ruolo IAM di Spark disponga dell'accesso corretto.

Parametro	Obbligatorio	Predefinito	Descrizione
tempformat	No	AVRO	Il formato in cui salvare i file temporanei in Amazon S3 durante la scrittura su Redshift. I valori validi sono AVRO, CSV e CSV GZIP (CSV compresso).
cvsnullstring (sperimentale)	No	Null	Il valore di stringa da scrivere per i valori null quando si utilizza il tempformat CSV. Dovrebbe trattarsi di un valore che non è presente nei dati effettivi.
autopushdown	No	True	Indica se applicare il pushdown di predicati e query acquisendo e analizzando i piani logici di Spark per le operazioni SQL. Le operazioni vengono tradotte in una query SQL e quindi eseguite in Redshift per migliorare le prestazioni.

Parametro	Obbligatorio	Predefinito	Descrizione
autopushdown.s3_result_cache	No	False	Memorizza nella cache la query SQL per scaricare i dati sulla mappatura dei percorsi di Amazon S3 in memoria, in modo che la stessa query non debba essere eseguita nuovamente nella stessa sessione di Spark. È supportato solo quando autopushdown è attivato. Non è consigliabile utilizzare questo parametro quando si combinano operazioni di lettura e scrittura, poiché i risultati memorizzati nella cache potrebbero contenere informazioni obsolete.

Parametro	Obbligatorio	Predefinito	Descrizione
unload_s3_format	No	Parquet	Il formato in cui scaricare i risultati delle query. Le opzioni valide sono Parquet e Text; quest'ultimo indica un formato di testo delimitato da pipe in cui scaricare i risultati delle query.
extraunloadoptions	No	N/D	Opzioni extra da aggiungere al comando <a href="#">UNLOAD</a> di Redshift. Non è garantito il funzionamento di tutte le opzioni poiché alcune opzioni potrebbero entrare in conflitto con altre opzioni impostate all'interno del connettore.
copydelay	No	30000	Il ritardo (in millisecondi) tra i tentativi per le operazioni COPY di Redshift.
copyretrycount	No	2	Il numero di volte in cui tentare le operazioni COPY di Redshift.

Parametro	Obbligatorio	Predefinito	Descrizione
tempdir_region	No	N/D	<p>La regione AWS in cui si trova tempdir. L'impostazione di questa opzione migliora le prestazioni del connettore per le interazioni con tempdir, oltre a fornire automaticamente questo valore come parte delle operazioni COPY e UNLOAD durante le operazioni di lettura e scrittura del connettore.</p> <p>Si consiglia di utilizzare questa impostazione nei seguenti casi:</p> <ol style="list-style-type: none"><li>1) Quando il connettore è in funzione all'esterno di AWS, poiché l'individuazione automatica della regione avrà esito negativo e influirà negativamente sulle prestazioni del connettore.</li></ol>

Parametro	Obbligatorio	Predefinito	Descrizione
			<p>2) Quando <code>tempdir</code> si trova in una regione diversa da quella del cluster Redshift, in quanto l'utilizzo di questa impostazione riduce la necessità di fornire la regione manualmente utilizzando i parametri <code>extracopy options</code> e <code>extraunlabeled adoptions</code>. <code>tempdir</code> non può trovarsi in una regione diversa da quella del cluster Redshift quando si utilizza <code>PARQUET</code> come <code>tempformat</code> anche se si utilizza questo parametro.</p> <p>3) Quando il connettore è in esecuzione in una regione diversa da quella di <code>tempdir</code>, poiché migliora le prestazioni di accesso al connettore e di <code>tempdir</code>.</p>

Parametro	Obbligatorio	Predefinito	Descrizione
secret.id	No	N/D	Il nome o l'ARN del tuo segreto archiviato o in AWS Secrets Manager. Puoi utilizzare questo parametro per fornire automaticamente le credenziali Redshift, ma solo se l'utente, la password e le credenziali DbUser non vengono passate nell'URL JDBC o come altre opzioni.

Parametro	Obbligatorio	Predefinito	Descrizione
secret.region	No	N/D	<p>La regione AWS primaria, ad esempio Stati Uniti orientali (Virginia settentrionale), in cui cercare il valore <code>secret.id</code>.</p> <p>Se non specifichi questa regione, il connettore proverà a utilizzare la <a href="#">catena di provider delle credenziali predefinita</a> per risolvere la regione del <code>secret.id</code>.</p> <p>In alcuni casi, ad esempio se utilizzi un connettore esterno a un connettore, questo non sarà in grado di trovare la regione. Si consiglia di utilizzare questa impostazione nei seguenti casi:</p> <ol style="list-style-type: none"><li>1) Quando il connettore funziona all'esterno di AWS, poiché il rilevamento automatico della regione non riuscirà</li></ol>

Parametro	Obbligatorio	Predefinito	Descrizione
			<p>e impedirà l'autenticazione con Redshift</p> <p>Quando il connettore è in esecuzione e in una regione diversa da quella di <code>secret.id</code>, poiché migliora le prestazioni di accesso del connettore al segreto.</p>
<code>secret.vpcEndpointUrl</code>	No	N/D	L'URL dell'endpoint DNS PrivateLink per AWS Secrets Manager quando si sovrascrive la <a href="#">catena di provider delle credenziali predefinita</a> .
<code>secret.vpcEndpointRegion</code>	No	N/D	La regione dell'endpoint DNS PrivateLink per AWS Secrets Manager quando si sovrascrive la <a href="#">catena di provider delle credenziali predefinita</a> .

Parametro	Obbligatorio	Predefinito	Descrizione
jdbc.*	No	N/D	Parametri aggiuntivi da passare al driver JDBC sottostante, dove il carattere jolly è il nome del parametro JDBC, ad esempio jdbc.ssl. Tieni presente che il prefisso jdbc verrà rimosso prima di essere passato al driver JDBC. Per visualizzare tutte le opzioni possibili per il driver JDBC Redshift, consulta <a href="#">Opzioni per la configurazione del driver JDBC versione 2.1.</a>

Parametro	Obbligatorio	Predefinito	Descrizione
etichetta	No	" "	<p>Un identificatore da includere nel gruppo di query impostato quando si eseguono query con il connettore. Deve contenere un massimo di 100 caratteri e tutti i caratteri devono essere unicodeIdentifierParts validi. Se l'identificatore contiene più di 100 caratteri, l'eccesso verrà rimosso. Quando esegui una query con il connettore, il gruppo di query verrà impostato come stringa di formato JSON, ad esempio</p> <pre>{"spark-redshift-connector": {"svc": "5.1.0-amzn-1-spark_3.3", "op": "Read", "lbl": ""}} )</pre> <p>. Questa opzione sostituisce il valore della chiave lbl.</p>

**Note**

Questa documentazione contiene codice e linguaggio di esempio sviluppati da [Apache Software Foundation](#) con [licenza Apache 2.0](#).

## Tipi di dati supportati

I seguenti tipi di dati sono supportati in Amazon Redshift con il connettore Spark. Per un elenco completo dei tipi di dati supportati in Amazon Redshift, consulta [Tipi di dati](#). Se un tipo di dati non è nella tabella seguente, non è supportato nel connettore Spark.

Tipo di dati	Alias
SMALLINT	INT2
INTEGER	INT, INT4
BIGINT	INT8
DECIMAL	NUMERIC
REAL	FLOAT4
DOUBLE PRECISION	FLOAT8, FLOAT
BOOLEAN	BOOL
CHAR	CHARACTER, NCHAR, BPCHAR
VARCHAR	CHARACTER VARYING, NVARCHAR, TEXT
DATE	
TIMESTAMP	Timestamp senza fuso orario
TIMESTAMPTZ	Timestamp con fuso orario
SUPER	
TIME	Ora senza fuso orario

Tipo di dati	Alias
TIMETZ	Ora con fuso orario
VARBYTE	VARBINARY, BINARY VARYING

## Tipi di dati complessi

Puoi usare il connettore spark per leggere e scrivere tipi di dati Spark complessi come `ArrayType`, `MapType` e `StructType` da e verso le colonne del tipo di dati Redshift SUPER. Se fornisci uno schema durante un'operazione di lettura, i dati nella colonna verranno convertiti nei tipi complessi corrispondenti in Spark, inclusi eventuali tipi nidificati. Inoltre, se `autopushdown` è abilitato, la proiezione degli attributi nidificati, dei valori delle mappe e degli indici degli array viene trasferita a Redshift in modo che l'intera struttura di dati nidificati non debba più essere caricata quando si accede solo a una parte dei dati.

Quando scrivi `DataFrames` dal connettore, qualsiasi colonna di tipo `MapType` (utilizzando `StringType`), `StructType` o `ArrayType` viene scritta in una colonna del tipo di dati Redshift SUPER. Quando si scrivono queste strutture di dati nidificati, il parametro `tempformat` deve essere di tipo `CSV`, `CSV GZIP` o `PARQUET`. L'utilizzo di `AVRO` causerà un'eccezione. Scrivere una struttura dati `MapType` con un tipo di chiave diverso da `StringType` causerà anche un'eccezione.

## StructType

L'esempio seguente mostra come creare una tabella con un tipo di dati SUPER che contiene una struttura

```
create table contains_super (a super);
```

È quindi possibile utilizzare il connettore per eseguire query su un campo `StringType` `hello` dalla colonna SUPER a nella tabella utilizzando uno schema come nell'esempio seguente.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
  StringType) :: Nil)) :: Nil)
```

```
val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a.hello")
```

L'esempio seguente mostra come scrivere una struttura nella colonna a.

```
import org.apache.spark.sql.types._
import org.apache.spark.sql._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", StructType(StructField("hello",
  StringType) :: Nil)) :: Nil)
val data = sc.parallelize(Seq(Row(Row("world"))))
val mydf = sqlContext.createDataFrame(data, schema)

mydf.write.format("io.github.spark_redshift_community.spark.redshift").
  option("url", jdbcUrl).
  option("dbtable", tableName).
  option("tempdir", tempS3Dir).
  option("tempformat", "CSV").
  mode(SaveMode.Append).save
```

## MapType

Se preferisci utilizzare MapType per rappresentare i dati, puoi usare una struttura i dati MapType nello schema e recuperare il valore corrispondente a una chiave nella mappa. Tieni presente che tutte le chiavi della struttura dati MapType deve essere di tipo String e tutti i valori devono essere dello stesso tipo, ad esempio int.

L'esempio seguente mostra come ottenere il valore della chiavehello nella colonna a.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", MapType(StringType, IntegerType))::Nil)
```

```
val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a['hello']")
```

## ArrayType

Se la colonna contiene un array anziché una struttura, puoi utilizzare il connettore per eseguire query sul primo elemento dell'array.

```
import org.apache.spark.sql.types._

val sc = // existing SparkContext
val sqlContext = new SQLContext(sc)

val schema = StructType(StructField("a", ArrayType(IntegerType)):: Nil)

val helloDF = sqlContext.read
  .format("io.github.spark_redshift_community.spark.redshift")
  .option("url", jdbcURL )
  .option("tempdir", tempS3Dir)
  .option("dbtable", "contains_super")
  .schema(schema)
  .load().selectExpr("a[0]")
```

## Restrizioni

L'utilizzo di tipi di dati complessi con il connettore spark presenta le seguenti limitazioni:

- Tutti i nomi dei campi di struttura nidificati e le chiavi delle mappe devono essere in minuscolo. Se esegui query su nomi di campo complessi con lettere maiuscole, puoi provare a omettere lo schema e utilizzare la funzione spark `from_json` per convertire la stringa restituita localmente come soluzione alternativa.
- Tutti i campi della mappa utilizzati nelle operazioni di lettura o scrittura devono avere solo chiavi `StringType`.
- Solo CSV, CSV GZIP e PARQUET sono valori `tempformat` supportati per scrivere tipi complessi su Redshift. Il tentativo di utilizzo di AVRO genererà un'eccezione.

## Configurazione di una connessione per il driver ODBC versione 2.x per Amazon Redshift

È possibile utilizzare una connessione ODBC per connettersi al cluster Amazon Redshift da numerose applicazioni e strumenti del client SQL di terze parti. Se il tuo strumento client supporta JDBC, potresti scegliere di usare quel tipo di connessione piuttosto che ODBC per la facilità di configurazione garantita da JDBC. Tuttavia, se il tuo strumento client non supporta JDBC, puoi seguire la procedura descritta in questa sezione per configurare una connessione ODBC sul computer client o sull'istanza Amazon EC2.

Amazon Redshift fornisce driver ODBC a 64 bit per i sistemi operativi Linux e Windows; i driver ODBC a 32 bit non sono più disponibili. Attualmente, macOS X non è supportato. Ulteriori aggiornamenti ai driver ODBC a 32 bit non verranno rilasciati, tranne che per le patch di sicurezza urgenti. Per scaricare e installare i driver ODBC per i sistemi operativi macOS X e a 32 bit, consulta [Configurazione di una connessione ODBC](#).

Per le informazioni più recenti sulle modifiche al driver ODBC, consultare il [log delle modifiche](#).

### Argomenti

- [Ottenimento dell'URL ODBC](#)
- [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#)
- [Installazione e configurazione del driver ODBC di Amazon Redshift su Linux](#)
- [Configurazione dell'autenticazione](#)
- [Conversione dei tipi di dati](#)
- [Configurazione delle opzioni del driver ODBC](#)
- [Versioni precedenti dei driver ODBC](#)

### Ottenimento dell'URL ODBC

Amazon Redshift visualizza l'URL ODBC per il cluster nella console Amazon Redshift. Questo URL contiene le informazioni per configurare la connessione tra il tuo computer client e il database.

Un URL ODBC ha il formato seguente:

```
Driver={driver}; Server=endpoint_host; Database=database_name; UID=user_name;  
PWD=password; Port=port_number
```

I campi del formato mostrato in precedenza hanno i seguenti valori:

#### Valori dei campi URL ODBC

Campo	Valore
<i>Driver</i>	Il nome del driver ODBC a 64 bit da utilizzare: Driver ODBC di Amazon Redshift (x64).
<i>Server</i>	L'host endpoint del cluster Amazon Redshift.
<i>Database</i>	Il database che hai creato per il tuo cluster.
<i>UID</i>	Nome utente di un account utente del database che dispone dell'autorizzazione e per connettersi al database. Nonostante questo valore sia un'autorizzazione a livello di database e non un'autorizzazione a livello di cluster, potrai utilizzare l'account utente amministratore di Redshift configurato all'avvio del cluster.
<i>PWD</i>	Password per l'account utente del database per connettersi al database.
<i>Port</i>	Numero di porta specificato all'avvio del cluster. In presenza di un firewall, assicurati che questa porta sia aperta per poterla utilizzare.

Di seguito è riportato un esempio di URL ODBC:

```
Driver={Amazon Redshift ODBC Driver (x64)}; Server=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com; Database=dev; UID=adminuser; PWD=insert_your_admin_user_password_here; Port=5439
```

Per informazioni su dove trovare l'URL ODBC, consulta [Ricerca della stringa di connessione al cluster](#).

## Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows

### Requisiti di sistema

Il driver ODBC di Amazon Redshift deve essere installato sui computer client che accedono a un data warehouse di Amazon Redshift. Ogni computer su cui hai installato il driver deve soddisfare i requisiti minimi elencati di seguito:

- Diritti di amministratore sulla macchina.
- La macchina deve soddisfare i seguenti requisiti di sistema:
  - Uno dei seguenti sistemi operativi:
    - Windows 10 o 8.1.
    - Windows Server 2019, 2016 o 2012.
  - 100 MB di spazio su disco disponibile.
  - Visual C++ Redistributable for Visual Studio 2015 per Windows a 64 bit installato. Puoi scaricare il pacchetto di installazione in [Download Visual C++ Redistributable per Visual Studio 2022](#) sul sito Web di Microsoft.

### Installazione del driver ODBC di Amazon Redshift

Utilizza la procedura seguente per scaricare e installare il driver ODBC di Amazon Redshift per i sistemi operativi Windows. Utilizzare un driver diverso dai precedenti solo se stai eseguendo un'applicazione di terze parti certificata per l'utilizzo con Amazon Redshift e che richiede un driver specifico.

Per scaricare e installare il driver ODBC:

1. Scarica il seguente driver: driver [ODBC a 64 bit versione 2.1.2.0 Nella regione Cina \(Pechino\)](#), [utilizza il seguente link: Driver](#) versione 2.1.2.0

Il nome di questo driver è Driver ODBC di Amazon Redshift (x64).

#### Note

I driver ODBC a 32 bit sono stati dichiarati come obsoleti. Ulteriori aggiornamenti non verranno rilasciati, tranne che per le patch di sicurezza urgenti. Per scaricare e installare

i driver ODBC per sistemi operativi a 32 bit, consulta [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).

2. Verifica la [Licenza del driver ODBC 2.x di Amazon Redshift](#).
3. Fai doppio clic sul file .msi, quindi completa le operazioni della procedura guidata di installazione del driver.

### Creazione di una voce DSN di sistema per una connessione ODBC

Dopo aver scaricato e installato il driver ODBC, aggiungere un nome di origine dati (DSN) al computer client o all'istanza Amazon EC2. Gli strumenti client SQL utilizzano questa origine dei dati per connettersi al database Amazon Redshift.

Ti consigliamo di creare un DSN di sistema anziché un DSN utente. Alcune applicazioni caricano i dati utilizzando un account utente del database diverso e potrebbero non essere in grado di rilevare i DSN utente creati con un altro account utente del database.

#### Note

Per l'autenticazione tramite credenziali AWS Identity and Access Management (IAM) o credenziali del provider di identità (IdP), sono necessari passaggi aggiuntivi. Per ulteriori informazioni, consulta [Configurazione di una connessione JDBC o ODBC per utilizzare le credenziali IAM](#).

Per creare una voce DSN di sistema per una connessione ODBC:

1. Nel menu Start (Avvio) digita "ODBC Data Sources" (Origini dati ODBC). Scegli ODBC Data sources (Origini dei dati ODBC).

Assicurarsi di scegliere l'amministratore dell'origine dati ODBC con gli stessi bit dell'applicazione client che si sta utilizzando per connettersi ad Amazon Redshift.

2. In ODBC Data Source Administrator (Amministratore origine dati ODBC), scegli la scheda Driver e individua la cartella del driver Driver ODBC di Amazon Redshift (x64).
3. Seleziona la scheda DSN sistema per configurare il driver per tutti gli utenti del computer o la scheda DSN utente per configurare il driver solo per l'account utente del database.
4. Scegli Aggiungi. Si aprirà la finestra Create New Data Source (Crea nuova origine dati).

5. Scegli il driver ODBC di Amazon Redshift (x64), quindi scegli Finish (Fine). Si aprirà la finestra Configurazione DNS del driver ODBC per Amazon Redshift.
6. Nella sezione Connection Settings (Impostazioni di connessione), inserisci le informazioni riportate di seguito:

- Nome origine dati

Inserisci un nome per l'origine dati. Ad esempio, se è stata seguita la Guida introduttiva di Amazon Redshift, è possibile digitare `exampleclusterdsn` per ricordare più facilmente il cluster che verrà associato a questo DSN.

- Server

Specifica l'host dell'endpoint per il cluster Amazon Redshift. Queste informazioni sono disponibili nella pagina dei dettagli del cluster della console Amazon Redshift. Per ulteriori informazioni, consulta [Configurazione delle connessioni in Amazon Redshift](#).

- Porta

Inserisci il numero di porta utilizzato dal database. A seconda della porta selezionata durante la creazione, la modifica o la migrazione del cluster, consenti l'accesso alla porta selezionata.

- Database

Immettere il nome del database Amazon Redshift. Se hai avviato il cluster senza specificare un nome di database, inserisci `dev`. In caso contrario, utilizza il nome scelto durante il processo di avvio. Se è stata seguita la Guida introduttiva di Amazon Redshift, immettere `dev`.

7. Nella sezione Authentication (Autenticazione), specifica le opzioni di configurazione per configurare l'autenticazione standard o IAM.

8. Scegli Opzioni SSL e specifica un valore per:

- Modalità di autenticazione

Seleziona una modalità per gestire Secure Sockets Layer (SSL). In un ambiente di test, puoi utilizzare `prefer`. Tuttavia, per gli ambienti di produzione e quando è necessario uno scambio sicuro di dati, utilizza `verify-ca` o `verify-full`.

- TLS minimo

Facoltativamente, scegli la versione minima di TLS/SSL che il driver consente all'archivio dati di utilizzare per crittografare le connessioni. Ad esempio, se specifichi TLS 1.2, TLS 1.1 non può essere utilizzato per crittografare le connessioni. La versione predefinita è TLS 1.2.

9. Nella scheda Proxy, specifica le impostazioni di connessione proxy.
10. Nella scheda Cursor (Cursore), specifica le opzioni su come restituire i risultati delle query allo strumento o all'applicazione client SQL.
11. In Opzioni avanzate, specificate i valori per `LogLevel`, `logPath`, `compression`, e altre opzioni.
12. Scegli Test (Esegui test). Se il computer client riesce a connettersi al database Amazon Redshift, viene visualizzato il messaggio seguente: Connessione riuscita. Se il computer client non riesce a connettersi al database, puoi risolvere i possibili problemi generando un file di registro e contattando AWS l'assistenza. Per informazioni sulla generazione di log, consulta [\(LINK\)](#).
13. Scegli OK.

## Installazione e configurazione del driver ODBC di Amazon Redshift su Linux

### Requisiti di sistema

Il driver ODBC di Amazon Redshift deve essere installato sui computer client che accedono a un data warehouse di Amazon Redshift. Ogni computer su cui hai installato il driver deve soddisfare i requisiti minimi elencati di seguito:

- Accesso root sulla macchina.
- Una delle seguenti distribuzioni:
  - Red Hat® Enterprise Linux® (RHEL) 8 o versione successiva
  - CentOS 8 o versione successiva.
- 150 MB di spazio su disco disponibile.
- unixODBC 2.2.14 o versione successiva.
- glibc 2.26 o versione successiva.

### Installazione del driver ODBC di Amazon Redshift

Per installare e configurare il driver ODBC di Amazon Redshift versione 2.x per Linux:

1. Scarica il seguente driver: driver [RPM a 64 bit versione 2.1.2.0 Nella regione Cina \(Pechino\)](#), [utilizza il seguente link: driver](#) versione 2.1.2.0

**Note**

I driver ODBC a 32 bit sono stati dichiarati come obsoleti. Ulteriori aggiornamenti non verranno rilasciati, tranne che per le patch di sicurezza urgenti.

2. Passare alla posizione in cui si è scaricato il pacchetto ed eseguire uno dei comandi seguenti. Utilizzare il comando corrispondente alla distribuzione Linux.

Sui sistemi operativi RHEL e CentOS, emetti il comando seguente:

```
yum --nogpgcheck localinstall RPMFileName
```

Sostituire *RPMFileName* con il nome del file del pacchetto RPM. Ad esempio, il comando seguente illustra l'installazione di un driver a 64 bit:

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-2.x.xx.xxxx.x86_64.rpm
```

### Utilizzo di un gestore di driver ODBC per configurare il driver ODBC su Linux

Su Linux, utilizzi un gestore di driver ODBC per configurare le impostazioni di connessione ODBC. I gestori di driver ODBC utilizzano i file di configurazione per definire e configurare i driver e le origini dati ODBC. La scelta del gestore di driver ODBC dipende dal sistema operativo utilizzato.

### Configurazione del driver ODBC utilizzando il gestore di driver unixODBC

Per configurare il driver ODBC di Amazon Redshift sono necessari i seguenti file:

- `amazon.redshiftdbc.ini`
- `odbc.ini`
- `odbcinst.ini`

Se l'installazione è stata eseguita nella posizione predefinita, il file di configurazione `amazon.redshiftdbc.ini` si trova in `/opt/amazon/redshiftdbcx64`.

Inoltre, in `/opt/amazon/redshiftdbcx64`, puoi trovare i file `odbc.ini` e `odbcinst.ini` di esempio. È possibile utilizzare questi file come esempi per configurare il driver ODBC di Amazon Redshift e il nome origine dati (DSN).

Si sconsiglia di usare la directory di installazione del driver ODBC di Amazon Redshift per i file di configurazione. I file di esempio nella directory di installazione sono a puro scopo illustrativo. Se si reinstalla il driver ODBC di Amazon Redshift in un secondo momento o si esegue l'aggiornamento a una versione più recente, la directory di installazione viene sovrascritta. Andranno perse tutte le modifiche apportate ai file nella directory di installazione.

Per evitare questo, copiare il file `amazon.redshiftdbc.ini` in una directory diversa dalla directory di installazione. Se si copia questo file nella home directory dell'utente, aggiungere un punto (`.`) alla parte iniziale del nome del file per renderlo nascosto.

Per i file `odbcinst.ini` e `odbc.ini`, utilizzare i file di configurazione nella home directory dell'utente o creare nuove versioni in un'altra directory. Per impostazione predefinita, il sistema operativo Linux dovrebbe avere un file `odbc.ini` e un file `odbcinst.ini` nella directory principale dell'utente (`/home/$USER` o `~/.`). Questi file predefiniti sono file nascosti, come indicato dal punto (`.`) davanti a ciascun nome del file. Questi file vengono visualizzati solo quando si utilizza il flag `-a` per elencare il contenuto della directory.

Qualunque sia l'opzione scelta per i file `odbc.ini` e `odbcinst.ini`, modificare i file per aggiungere le informazioni di configurazione del driver e del DSN. Se vengono creati nuovi file, è inoltre necessario impostare variabili di ambiente per specificare dove si trovano questi file di configurazione.

Per impostazione predefinita, i gestori del driver ODBC sono configurati per utilizzare versioni nascoste dei file di configurazione `odbc.ini` e `odbcinst.ini` (denominati `.odbc.ini` e `.odbcinst.ini`) che si trovano nella directory principale. Sono inoltre configurati per utilizzare il file `amazon.redshiftdbc.ini` nella directory di installazione del driver. Se si archiviano questi file di configurazione altrove, impostare le variabili di ambiente descritte di seguito in modo che il gestore dei driver possa individuare i file.

Se stai utilizzando `unixODBC`, procedi nel modo seguente:

- Imposta `ODBCINI` sul percorso completo e sul nome file del file `odbc.ini`.
- Imposta `ODBCSYSINI` sul percorso completo della directory che contiene il file `odbcinst.ini`.
- Imposta `AMAZONREDSHIFTODBCINI` sul percorso completo e sul nome file del file `amazon.redshiftdbc.ini`.

Di seguito è riportato un esempio di impostazione dei valori precedenti:

```
export ODBCINI=/usr/local/odbc/odbc.ini
export ODBCSYSINI=/usr/local/odbc
export AMAZONREDSHIFTODBCINI=/etc/amazon.redshiftoDBC.ini
```

Configurazione di una connessione utilizzando un nome origine dei dati (DSN) su Linux

Quando ti connetti all'archivio dati utilizzando un nome origine dei dati (DSN), configura il file `odbc.ini` per definire i DSN. Imposta le proprietà nel file `odbc.ini` per creare un DSN che specifica le informazioni di connessione per i data store.

Sui sistemi operativi Linux, usa il seguente formato:

```
[ODBC Data Sources]
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file
Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'esempio seguente mostra la configurazione per `odbc.ini` con il driver ODBC a 64 bit su sistemi operativi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift ODBC Driver (x64)

[Amazon_Redshift_x64]
Driver=/opt/amazon/redshiftoDBCx64/librsodbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932Database=dev
locale=en-US
```

## Configurazione di una connessione senza DSN su Linux

Per connetterti al data store tramite una connessione che non dispone di un DSN, devi definire il driver nel file `odbcinst.ini`. Quindi devi fornire una stringa di connessione senza DSN nell'applicazione.

Sui sistemi operativi Linux, usa il seguente formato:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file
...
```

L'esempio seguente mostra la configurazione per `odbcinst.ini` con il driver ODBC a 64 bit su sistemi operativi Linux.

```
[ODBC Drivers]
Amazon Redshift ODBC Driver (x64)=Installed

[Amazon Redshift ODBC Driver (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftdbcx64/librsodbc64.so
```

## Configurazione dell'autenticazione

Per proteggere i dati da accessi non autorizzati, gli archivi dati di Amazon Redshift richiedono l'autenticazione di tutte le connessioni tramite le credenziali utente.

La seguente tabella riporta le opzioni di connessione obbligatorie e facoltative per ogni metodo di autenticazione che può essere utilizzato per connettersi al driver ODBC Amazon Redshift versione 2.x:

## Opzioni di connessione richieste e facoltative per il metodo di autenticazione ODBC

Metodo di autenticazione	Richiesto	Facoltativo
Standard	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• UID</li> <li>• Password</li> </ul>	
Profilo IAM	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• Profilo</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• AutoCreate</li> <li>• EndpointURL</li> <li>• StsEndpointURL</li> <li>• InstanceProfile</li> </ul> <div data-bbox="1068 1003 1507 1367" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p> </div>
Credenziali IAM	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• AccessKeyID</li> <li>• SecretAccessChiave</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• AutoCreate</li> <li>• EndpointURL</li> <li>• StsEndpointURL</li> <li>• SessionToken</li> <li>• UID</li> </ul>

Metodo di autenticazione	Richiesto	Facoltativo
		<p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p>
AD FS	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• plugin_name</li> <li>• UID</li> <li>• Password</li> <li>• IdP_Host</li> <li>• IdP_Port</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• AutoCreate</li> <li>• EndpointUrl</li> <li>• StsEndpointUrl</li> <li>• preferred_role</li> <li>• accesso ToRp</li> <li>• ssl_insecure</li> </ul> <p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p>

Metodo di autenticazione	Richiesto	Facoltativo
Azure AD	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• plugin_name</li> <li>• UID</li> <li>• Password</li> <li>• idp_tenant</li> <li>• Client_ID</li> <li>• Client_Secret</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• AutoCreate</li> <li>• EndpointUrl</li> <li>• StsEndpointUrl</li> <li>• preferred_role</li> <li>• dbggroups_filter</li> </ul> <div data-bbox="1068 678 1510 1041" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p> </div>
JWT	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• plugin_name</li> <li>• web_identity_token</li> </ul>	<ul style="list-style-type: none"> <li>• provider_name</li> </ul>

Metodo di autenticazione	Richiesto	Facoltativo
Okta	<ul style="list-style-type: none"><li>• Host</li><li>• Porta</li><li>• Database</li><li>• IAM</li><li>• plugin_name</li><li>• UID</li><li>• Password</li><li>• IdP_Host</li><li>• App_Name</li><li>• App_ID</li></ul>	<ul style="list-style-type: none"><li>• ClusterID</li><li>• Regione</li><li>• AutoCreate</li><li>• EndpointUrl</li><li>• StsEndpointUrl</li><li>• preferred_role</li></ul> <div data-bbox="1068 621 1508 982"><p> <b>Note</b> ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p></div>

Metodo di autenticazione	Richiesto	Facoltativo
Ping Federate	<ul style="list-style-type: none"><li>• Host</li><li>• Porta</li><li>• Database</li><li>• IAM</li><li>• plugin_name</li><li>• UID</li><li>• Password</li><li>• IdP_Host</li><li>• IdP_Port</li></ul>	<ul style="list-style-type: none"><li>• ClusterID</li><li>• Regione</li><li>• AutoCreate</li><li>• EndpointUrl</li><li>• StsEndpointUrl</li><li>• preferred_role</li><li>• ssl_insecure</li><li>• partner_spid</li></ul> <div data-bbox="1068 737 1507 1098" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"><p> <b>Note</b></p><p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p></div>

Metodo di autenticazione	Richiesto	Facoltativo
Browser Azure AD	<ul style="list-style-type: none"><li>• Host</li><li>• Porta</li><li>• Database</li><li>• IAM</li><li>• plugin_name</li><li>• idp_tenant</li><li>• Client_ID</li><li>• UID</li></ul>	<ul style="list-style-type: none"><li>• ClusterID</li><li>• Regione</li><li>• AutoCreate</li><li>• EndpointUrl</li><li>• StsEndpointUrl</li><li>• preferred_role</li><li>• dbgroups_filter</li><li>• IdP_Response_Timeout</li><li>• listen_port</li></ul>

 **Note**

ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.

Metodo di autenticazione	Richiesto	Facoltativo
Browser SAML	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• plugin_name</li> <li>• login_url</li> <li>• UID</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• AutoCreate</li> <li>• EndpointUrl</li> <li>• StsEndpointUrl</li> <li>• preferred_role</li> <li>• dbgroups_filter</li> <li>• IdP_Response_Timeout</li> <li>• listen_port</li> </ul> <div data-bbox="1068 793 1507 1155" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p> </div>
Auth Profile	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• AccessKeyID</li> <li>• SecretAccessChiave</li> </ul>	

Metodo di autenticazione	Richiesto	Facoltativo
Browser Azure AD OAUTH2	<ul style="list-style-type: none"> <li>• Host</li> <li>• Porta</li> <li>• Database</li> <li>• IAM</li> <li>• plugin_name</li> <li>• idp_tenant</li> <li>• Client_ID</li> <li>• UID</li> </ul>	<ul style="list-style-type: none"> <li>• ClusterID</li> <li>• Regione</li> <li>• EndpointUrl</li> <li>• IdP_Response_Timeout</li> <li>• listen_port</li> <li>• scope</li> <li>• provider_name</li> </ul> <div data-bbox="1068 680 1507 1045" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>ClusterID e Region devono essere impostati su Host se non sono impostati separatamente.</p> </div>

## Utilizzo di un servizio di credenziali esterno

Oltre al supporto integrato per AD FS, Azure AD e Okta, la versione Windows del driver ODBC di Amazon Redshift fornisce anche il supporto per altri servizi di credenziali. Il driver può autenticare le connessioni utilizzando qualsiasi plug-in del provider di credenziali basato su SAML di tua scelta.

Per configurare un servizio di credenziali esterno su Windows:

1. Crea un profilo IAM che specifichi il plug-in del provider di credenziali e altri parametri di autenticazione in base alle esigenze. Il profilo deve essere codificato ASCII e deve contenere la seguente coppia chiave-valore, dove `PluginPath` è il percorso completo dell'applicazione plug-in:

```
plugin_name = PluginPath
```

Ad esempio:

```
plugin_name = C:\Users\kjson\myapp\CredServiceApp.exe
```

Per informazioni su come creare un profilo, consulta [Utilizzo di un profilo di configurazione](#) nella Guida alla gestione dei cluster Amazon Redshift.

2. Configura il driver per l'utilizzo di questo profilo. Il driver rileva e utilizza le impostazioni di autenticazione specificate nel profilo.

## Conversione dei tipi di dati

Il driver ODBC di Amazon Redshift versione 2.x supporta numerosi formati di dati comuni, convertendo le tipologie di dati Amazon Redshift ed SQL.

La tabella seguente riporta le mappature dei tipi di dati supportate.

Tipo di Amazon Redshift	Tipo SQL
BIGINT	SQL_BIGINT
BOOLEAN	SQL_BIT
CHAR	SQL_CHAR
DATE	SQL_TYPE_DATE
DECIMAL	SQL_NUMERIC
DOUBLE PRECISION	SQL_DOUBLE
GEOGRAPHY	SQL_LONGVARBINARY
GEOMETRY	SQL_LONGVARBINARY
INTEGER	SQL_INTEGER
REAL	SQL_REAL
SMALLINT	SQL_SMALLINT
SUPER	SQL_LONGVARCHAR
TEXT	SQL_LONGVARCHAR

Tipo di Amazon Redshift	Tipo SQL
TIME	SQL_TYPE_TIME
TIMETZ	SQL_TYPE_TIME
TIMESTAMP	SQL_TYPE_TIMESTAMP
TIMESTAMPTZ	SQL_TYPE_TIMESTAMP
VARBYTE	SQL_LONGVARBINARY
VARCHAR	SQL_VARCHAR

## Configurazione delle opzioni del driver ODBC

Puoi utilizzare le opzioni di configurazione del driver per controllare il comportamento del driver ODBC di Amazon Redshift. Le opzioni per i driver non distinguono tra maiuscole e minuscole.

In Microsoft Windows, in genere imposti le opzioni del driver quando configuri un nome dell'origine dati (DSN). Puoi anche impostare le opzioni del driver nella stringa di connessione quando ti connetti in modo programmatico oppure aggiungendo o modificando le chiavi di registro in `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN`. Per ulteriori informazioni sulla configurazione di un DSN, consultare [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).

Su Linux, imposta le opzioni di configurazione del driver nei file `odbc.ini` e `amazon.redshiftdbc.ini`, come descritto in [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#). Le opzioni di configurazione impostate in un file `amazon.redshiftdbc.ini` si applicano a tutte le connessioni. Al contrario, le opzioni di configurazione impostate in un file `odbc.ini` sono specifiche di una connessione. Le opzioni di configurazione impostate in `odbc.ini` hanno la precedenza sulle opzioni di configurazione impostate in `amazon.redshiftdbc.ini`.

Di seguito sono riportate le descrizioni per le opzioni che puoi specificare per la versione 2.x del driver JDBC di Amazon Redshift.

### AccessKeyID

- Valore predefinito: nessuno

- Tipo di dati: stringa

La chiave di accesso IAM per l'utente o il ruolo. Se si imposta questo parametro, è necessario specificare anche `SecretAccessKey`.

Questo parametro è facoltativo.

`app_id`

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID univoco fornito da Okta associato all'applicazione Amazon Redshift.

Questo parametro è facoltativo.

`Nome_App`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome dell'applicazione Okta utilizzata per autenticare la connessione ad Amazon Redshift.

Questo parametro è facoltativo.

`AuthProfile`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il profilo di autenticazione utilizzato per gestire le impostazioni di connessione. Se si imposta questo parametro, è necessario impostare anche `AccessKeyID` e `SecretAccessKey`.

Questo parametro è facoltativo.

`AuthType`

- Valore predefinito - Standard
- Tipo di dati: stringa

Questa opzione specifica la modalità di autenticazione utilizzata dal driver quando configuri un DSN utilizzando la finestra di dialogo Configurazione DSN del driver ODBC di Amazon Redshift:

- Standard: autenticazione standard tramite nome utente e password di Amazon Redshift.
- AWS Profilo: autenticazione IAM tramite un profilo.
- AWS Credenziali IAM: autenticazione IAM tramite credenziali IAM.
- Provider di identità: AD FS: autenticazione IAM tramite Active Directory Federation Services (AD FS).
- Identity Provider: Plugin di autenticazione: un plug-in di autorizzazione che accetta un token IAM Identity Center o token di identità (JWT) basati su JSON OpenID Connect (OIDC) da qualsiasi provider di identità Web collegato a IAM Identity Center.
- Provider di identità: Azure AD: autenticazione IAM tramite un portale Azure AD.
- Provider di identità: JWT: autenticazione IAM utilizzando un JSON Web token (JWT).
- Provider di identità: Okta: autenticazione IAM tramite Okta.
- Identity Provider: autenticazione IAM tramite. PingFederate PingFederate

Questa opzione è disponibile solo quando configuri un DSN utilizzando la finestra di dialogo Configurazione DSN del driver ODBC di Amazon Redshift nel driver di Windows. Quando si configura una connessione utilizzando una stringa di connessione o un computer non Windows, il driver determina automaticamente se utilizzare l'autenticazione Standard, AWS Profile o AWS IAM Credentials in base alle credenziali specificate. Per utilizzare un provider di identità, è necessario impostare la proprietà `plugin_name`.

Questo parametro è obbligatorio.

### AutoCreate

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver crea un nuovo utente quando l'utente specificato non esiste.

- 1 | TRUE: se l'utente specificato dall'UID non esiste, il driver crea un nuovo utente.
- 0 | FALSE: il driver non crea un nuovo utente. Se l'utente specificato non esiste, l'autenticazione avrà esito negativo.

Questo parametro è facoltativo.

### CaFile

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il percorso del file del certificato CA utilizzato per alcune forme di autenticazione IAM.

Questo parametro è disponibile solo su Linux.

Questo parametro è facoltativo.

### client\_id

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID client associato all'applicazione Amazon Redshift in Azure AD.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

### client\_secret

- Valore predefinito: nessuno
- Tipo di dati: stringa

La chiave del segreto associata all'applicazione Amazon Redshift in Azure AD.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

### ClusterId

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del cluster Amazon Redshift a cui desideri connetterti. Viene utilizzata nell'autenticazione IAM. L'ID del cluster non è specificato nel parametro Server.

Questo parametro è facoltativo.

compressione

- Valore predefinito: disattivato
- Tipo di dati: stringa

Il metodo di compressione utilizzato per la comunicazione del protocollo wire tra il server Amazon Redshift e il client o il driver.

Puoi specificare le seguenti valori:

- lz4: imposta il metodo di compressione utilizzato per le comunicazioni via cavo con Amazon Redshift su. lz4
- zstd: imposta il metodo di compressione utilizzato per le comunicazioni via cavo con Amazon Redshift su. zstd
- off: non utilizza la compressione per le comunicazioni via cavo con Amazon Redshift.

Questo parametro è facoltativo.

Database

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del database Amazon Redshift a cui desideri accedere.

Questo parametro è obbligatorio.

DatabaseMetadataCurrentDbSolo

- Valore predefinito: 1
- Tipo di dati: booleano

Un valore booleano che specifica se il driver restituisce metadati da più database e cluster.

- 1 | TRUE: il driver restituisce solo metadati dal database corrente.

- 0 | FALSE. Il driver restituisce i metadati su più database e cluster Amazon Redshift.

Questo parametro è facoltativo.

`dbgroups_filter`

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'espressione regolare che puoi specificare per filtrare DbGroups quella ricevuta dalla risposta SAML ad Amazon Redshift quando usi i tipi di autenticazione Azure, Browser Azure e Browser SAML.

Questo parametro è facoltativo.

`Driver`

- Valore predefinito: driver ODBC Amazon Redshift (x64)
- Tipo di dati: stringa

Il nome del driver. L'unico valore supportato è Driver ODBC Amazon Redshift (x64).

Questo parametro è obbligatorio se non viene impostato DSN.

`DSN`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome dell'origine dei dati del driver. L'applicazione specifica il DSN nell'API SQL. DriverConnect

Questo parametro è obbligatorio se non viene impostato Driver.

`EndpointUrl`

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'endpoint di sostituzione utilizzato per comunicare con Amazon Redshift Coral Service per l'autenticazione IAM.

Questo parametro è facoltativo.

#### ForceLowercase

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver inserisce in lettere minuscole tutto ciò che DbGroups viene inviato dal provider di identità ad Amazon Redshift quando si utilizza l'autenticazione Single Sign-On.

- 1 | TRUE: il driver mette in minuscolo tutto ciò che viene inviato dal provider di identità. DbGroups
- 0 | FALSE: il driver non cambia. DbGroups

Questo parametro è facoltativo.

#### group\_federation

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se l'`getClusterCredentialsWithIAMAPI` viene utilizzata per ottenere credenziali temporanee del cluster nei cluster predisposti. Questa opzione consente agli utenti IAM di integrarsi con i ruoli del database Redshift nei cluster con provisioning. Nota che questa opzione non si applica ai namespace Redshift Serverless.

- 1 | TRUE: il driver utilizza l'`getClusterCredentialsWithIAMAPI` per ottenere credenziali temporanee del cluster nei cluster assegnati.
- 0 | FALSO: il driver utilizza l'`getClusterCredentialsAPI` predefinita per ottenere le credenziali temporanee del cluster nei cluster predisposti.

Questo parametro è facoltativo.

#### https\_proxy\_host

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome host o l'indirizzo IP del server proxy attraverso il quale passare i processi di autenticazione IAM.

Questo parametro è facoltativo.

`https_proxy_password`

- Valore predefinito: nessuno
- Tipo di dati: stringa

La password utilizzata per l'accesso al server proxy. Viene utilizzata nell'autenticazione IAM.

Questo parametro è facoltativo.

`https_proxy_port`

- Valore predefinito: nessuno
- Tipo di dati: numero intero

Il numero della porta utilizzata dal server proxy per l'ascolto delle connessioni client. Viene utilizzato nell'autenticazione IAM.

Questo parametro è facoltativo.

`https_proxy_username`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome utente utilizzato per accedere al server proxy. È usato per l'autenticazione IAM.

Questo parametro è facoltativo.

`IAM`

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver utilizza un metodo di autenticazione IAM per autenticare la connessione.

- 1 | TRUE: il driver utilizza uno dei metodi di autenticazione IAM (utilizzando una coppia di chiave di accesso e chiave segreta, un profilo o un servizio di credenziali).
- 0 | FALSE. Il driver utilizza l'autenticazione standard (utilizzando il nome utente e la password del database).

Questo parametro è facoltativo.

`identity_namespace`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Lo spazio dei nomi di identità da utilizzare durante l'autenticazione tramite `IdpTokenAuthPlugin`. Consente a Redshift di determinare quale istanza Centro identità IAM utilizzare.

Questo parametro è facoltativo se esiste una sola istanza Centro identità IAM o se è impostato lo spazio dei nomi di identità predefinito. In caso contrario, è obbligatorio.

`idp_host`

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'host IdP (provider di identità) utilizzato per l'autenticazione in Amazon Redshift.

Questo parametro è facoltativo.

`idp_port`

- Valore predefinito: nessuno
- Tipo di dati: numero intero

La porta per un IdP (provider di identità) utilizzata per l'autenticazione in Amazon Redshift. A seconda della porta selezionata durante la creazione, la modifica o la migrazione del cluster, consenti l'accesso alla porta selezionata.

Questo parametro è facoltativo.

`idP_Response_Timeout`

- Valore predefinito: 120
- Tipo di dati: numero intero

Il tempo, in secondi, per cui il driver attende la risposta SAML dal provider di identità quando si usano i servizi SAML o Azure AD tramite un plug-in del browser.

Questo parametro è facoltativo.

`idp_tenant`

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'ID tenant Azure AD associato all'applicazione Amazon Redshift.

Questo parametro è obbligatorio se si esegue l'autenticazione tramite il servizio Azure AD.

`idp_use_https_proxy`

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver fa passare i processi di autenticazione per i gestori dell'identità digitale (IdP) attraverso un server proxy.

- 1 | TRUE: il driver fa passare i processi di autenticazione dell'IdP attraverso un server proxy.
- 0 | FALSE. Il driver non fa passare i processi di autenticazione dell'IdP attraverso un server proxy.

Questo parametro è facoltativo.

`InstanceProfile`

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver utilizza il profilo di istanza Amazon EC2, se configurato per l'utilizzo di un profilo per l'autenticazione.

- 1 | TRUE: il driver utilizza il profilo dell'istanza Amazon EC2.
- 0 | FALSE. Il driver utilizza il profilo dei ruoli concatenati specificato dall'opzione Nome profilo (Profilo).

Questo parametro è facoltativo.

### KeepAlive

- Valore predefinito: 1
- Tipo di dati: booleano

Un valore booleano che specifica se il driver utilizza i keepalive TCP al fine di impedire il timeout delle connessioni.

- 1 | TRUE: il driver utilizza i keepalive TCP al fine di impedire il timeout delle connessioni.
- 0 | FALSE. Il driver non utilizza keepalive TCP.

Questo parametro è facoltativo.

### KeepAliveConta

- Valore predefinito: 0
- Tipo di dati: numero intero

Il numero di pacchetti keepalive TCP che possono essere persi prima che la connessione sia considerata interrotta. Se questo parametro è impostato su 0, per questa impostazione il driver utilizza il valore predefinito di sistema.

Questo parametro è facoltativo.

### KeepAliveIntervallo

- Valore predefinito: 0
- Tipo di dati: numero intero

Il numero di secondi tra ciascuna ritrasmissione di keepalive TCP. Se questo parametro è impostato su 0, per questa impostazione il driver utilizza il valore predefinito di sistema.

Questo parametro è facoltativo.

#### KeepAliveTempo

- Valore predefinito: 0
- Tipo di dati: numero intero

Il numero di secondi di inattività prima che il driver invii un pacchetto keepalive TCP. Se questo parametro è impostato su 0, per questa impostazione il driver utilizza il valore predefinito di sistema.

Questo parametro è facoltativo.

#### listen\_port

- Valore predefinito: 7890
- Tipo di dati: numero intero

La porta utilizzata dal driver per ricevere la risposta SAML dal provider di identità quando si usano i servizi SAML o Azure AD tramite un plug-in del browser.

Questo parametro è facoltativo.

#### login\_url

- Valore predefinito: nessuno
- Tipo di dati: stringa

L'URL della risorsa sul sito Web del provider di identità quando si usa il plug-in Browser SAML generico.

Questo parametro è obbligatorio se si esegue l'autenticazione con SAML o i servizi Azure AD tramite un plug-in del browser.

#### effettuare il login ToRp

- Valore predefinito: urn:amazon:webservices

- Tipo di dati: stringa

La parte attendibile che si desidera utilizzare per il tipo di autenticazione AD FS.

Questa stringa è facoltativa.

LogLevel

- Valore predefinito: 0
- Tipo di dati: numero intero

Utilizza questa proprietà per attivare o disattivare la registrazione nel driver e per specificare il livello di dettaglio incluso nei file di log. Ti consigliamo di abilitare la registrazione solo per il tempo necessario a rilevare un problema, poiché la registrazione riduce le prestazioni e può richiedere una grande quantità di spazio su disco.

Imposta il parametro su uno dei seguenti valori:

- 0 = OFF. Disabilitare la registrazione.
- 1: ERROR. Registra gli eventi di errore che potrebbero consentire al driver di restare in esecuzione ma produce un errore.
- 2: API\_CALL. Registra le chiamate alle funzioni API ODBC con i valori degli argomenti della funzione.
- 3: INFO. Registra le informazioni generali che descrivono l'avanzamento del driver.
- 4: MSG\_PROTOCOL. Registra informazioni dettagliate sul protocollo dei messaggi del driver.
- 5: DEBUG. Registra l'attività di tutti i driver.
- 6: DEBUG\_APPEND. Continua ad aggiungere i registri per tutte le attività dei driver.

Quando la registrazione è abilitata, il driver produce i seguenti file di registro nella posizione specificata nella LogPathproprietà:

- Un file `redshift_odbc.log.1` che registra l'attività del driver che si verifica durante l'handshake di una connessione.
- Un file `redshift_odbc.log` per tutte le attività del driver dopo che è stata stabilita una connessione al database.

Questo parametro è facoltativo.

### LogPath

- Valore predefinito: la directory TEMP specifica del sistema operativo
- Tipo di dati: stringa

Il percorso completo della cartella in cui il driver salva i file di registro quando LogLevel è superiore a 0.

Questo parametro è facoltativo.

### Min\_TLS

- Valore predefinito: 1.2
- Tipo di dati: stringa

La versione minima di TLS/SSL che il driver consente all'archivio dati di utilizzare per crittografare le connessioni. Ad esempio, se viene specificato TLS 1.2, TLS 1.1 non può essere utilizzato per crittografare le connessioni.

Min\_TLS accetta i valori seguenti:

- 1.0: la connessione deve utilizzare almeno TLS 1.0.
- 1.1: la connessione deve utilizzare almeno TLS 1.1.
- 1.2: la connessione deve utilizzare almeno TLS 1.2.

Questo parametro è facoltativo.

### partner\_spid

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il valore SPID (ID del fornitore di servizi) del partner da utilizzare per l'autenticazione della connessione tramite il servizio. PingFederate

Questo parametro è facoltativo.

## Password | PWS

- Valore predefinito: nessuno
- Tipo di dati: stringa

La password corrispondente al nome utente del database fornito nel campo Utente (UID | User | LogonID).

Questo parametro è facoltativo.

## plugin\_name

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del plug-in del provider di credenziali da utilizzare per l'autenticazione.

Sono supportati i seguenti valori:

- `ADFS`: utilizza Active Directory Federation Services per l'autenticazione.
- `AzureAD`: utilizza Microsoft Azure Active Directory (AD) Service per l'autenticazione
- `BrowserAzureAD`: utilizza un plug-in del browser per il servizio Microsoft Azure Active Directory (AD) per l'autenticazione.
- `BrowserSAML`: utilizza un plug-in del browser per servizi SAML come Okta o Ping per l'autenticazione.
- `IdpTokenAuthPlugin`: Un plug-in di autorizzazione che accetta un token IAM Identity Center o token di identità (JWT) basati su JSON OpenID Connect (OIDC) da qualsiasi provider di identità Web collegato a IAM Identity Center.
- `JWT`: utilizza un JSON Web Token (JWT) per l'autenticazione.
- `Ping`: utilizza il servizio per l'autenticazione. `PingFederate`
- `Okta`: utilizza il servizio Okta per l'autenticazione.

Questo parametro è facoltativo.

## Porta | PortNumber

- Valore di default: 5439

- Tipo di dati: numero intero

Il numero della porta TCP utilizzata dal server Amazon Redshift per l'ascolto delle connessioni client.

Questo parametro è facoltativo.

`preferred_role`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il ruolo IAM che desideri assumere durante la connessione ad Amazon Redshift. Viene utilizzato nell'autenticazione IAM.

Questo parametro è facoltativo.

`Profilo`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome del AWS profilo utente utilizzato per l'autenticazione in Amazon Redshift.

- Se il parametro Use Instance Profile (la InstanceProfileproprietà) è impostato su 1 | TRUE, tale impostazione ha la precedenza e il driver utilizza invece il profilo dell'istanza Amazon EC2.
- La posizione predefinita per il file delle credenziali contenente i profili è `~/.aws/Credentials`. La variabile di ambiente `AWS_SHARED_CREDENTIALS_FILE` può essere utilizzata per fare riferimento a un file di credenziali diverso.

Questo parametro è facoltativo.

`provider_name`

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il provider di autenticazione creato dall'utente utilizzando la query `CREATE IDENTITY PROVIDER`. Viene utilizzato nell'autenticazione nativa di Amazon Redshift.

Questo parametro è facoltativo.

### ProxyHost

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome host o l'indirizzo IP del server proxy tramite il quale connettersi.

Questo parametro è facoltativo.

### ProxyPort

- Valore predefinito: nessuno
- Tipo di dati: numero intero

Il numero della porta utilizzata dal server proxy per l'ascolto delle connessioni client.

Questo parametro è facoltativo.

### ProxyPwd

- Valore predefinito: nessuno
- Tipo di dati: stringa

La password utilizzata per l'accesso al server proxy.

Questo parametro è facoltativo.

### ProxyUid

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome utente utilizzato per accedere al server proxy.

Questo parametro è facoltativo.

## ReadOnly

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver è in modalità di sola lettura.

- 1 | TRUE: la connessione è in modalità di sola lettura e non può scrivere nell'archivio dati.
- 0 | FALSE: la connessione non è in modalità di sola lettura e può scrivere nell'archivio dati.

Questo parametro è facoltativo.

## Regione

- Valore predefinito: nessuno
- Tipo di dati: stringa

La AWS regione in cui si trova il cluster.

Questo parametro è facoltativo.

## SecretAccessChiave

- Valore predefinito: nessuno
- Tipo di dati: stringa

La chiave del segreto IAM per l'utente o il ruolo. Se si imposta questo parametro, è necessario impostare anche l'AccessKeyID.

Questo parametro è facoltativo.

## SessionToken

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il token di sessione IAM temporaneo associato al ruolo IAM utilizzato per l'autenticazione.

Questo parametro è facoltativo.

Server | HostName | Host

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il server dell'endpoint a cui connettersi.

Questo parametro è obbligatorio.

ssl\_insecure

- Valore predefinito: 0
- Tipo di dati: booleano

Un valore booleano che specifica se il driver controlla l'autenticità del certificato del server IdP.

- 1 | TRUE: il driver non controlla l'autenticità del certificato del server IdP.
- 0 | FALSE: il driver controlla l'autenticità del certificato del server IdP.

Questo parametro è facoltativo.

SSLMode

- Valore predefinito: `verify-ca`
- Tipo di dati: stringa

La modalità di verifica del certificato SSL da utilizzare durante la connessione ad Amazon Redshift. I valori possibili sono i seguenti:

- `verify-full`: connessione solo tramite SSL, un'autorità di certificazione attendibile e un nome di server che corrisponda al certificato.
- `verify-ca`: connessione solo tramite SSL e un'autorità di certificazione attendibile.
- `require`: connessione solo tramite SSL.
- `prefer`: connessione tramite SSL, se disponibile. Altrimenti, connessione senza utilizzare SSL.

- `allow`: per impostazione predefinita, connessione senza utilizzare SSL. Se il server richiede connessioni SSL, allora utilizza SSL.
- `disable`: connessione senza utilizzare SSL.

Questo parametro è facoltativo.

#### StsConnectionTimeout

- Valore predefinito: 0
- Tipo di dati: numero intero

Il tempo massimo di attesa per le connessioni IAM, in secondi. Se impostato su 0 o non è specificato, l'autista attende 60 secondi per ogni AWS STS chiamata.

Questo parametro è facoltativo.

#### StsEndpointUrl

- Valore predefinito: nessuno
- Tipo di dati: stringa

Questa opzione specifica l'endpoint sovrascritto utilizzato per comunicare con (). AWS Security Token Service AWS STS

Questo parametro è facoltativo.

#### token

- Valore predefinito: nessuno
- Tipo di dati: stringa

Un token di accesso fornito da IAM Identity Center o un token Web JSON (JWT) OpenID Connect (OIDC) fornito da un provider di identità Web collegato a IAM Identity Center. L'applicazione deve generare questo token autenticando l'utente dell'applicazione con IAM Identity Center o un provider di identità collegato a IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## token\_type

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il tipo di token che viene utilizzato in. `IdpTokenAuthPlugin`

Puoi specificare le seguenti valori:

### ACCESS\_TOKEN

Inserisci questo valore se utilizzi un token di accesso fornito da IAM Identity Center.

### EXT\_JWT

Inserisci questo valore se utilizzi un JSON Web Token (JWT) OpenID Connect (OIDC) fornito da un provider di identità basato sul Web integrato con IAM Identity Center.

Questo parametro funziona con. `IdpTokenAuthPlugin`

## UID | User | LogonID

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il nome utente utilizzato per accedere al server Amazon Redshift.

Questo parametro è obbligatorio se utilizzi l'autenticazione del database.

## web\_identity\_token

- Valore predefinito: nessuno
- Tipo di dati: stringa

Il token OAUTH fornito dal provider di identità. È usato nel plug-in JWT.

Questo parametro è obbligatorio se impostate il parametro `plugin_name` su. `BasicJwtCredentialsProvider`

## Versioni precedenti dei driver ODBC

Scarica una versione precedente del driver ODBC versione 2.x di Amazon Redshift solo se lo strumento richiede una versione specifica del driver.

### Utilizzo delle versioni precedenti del driver ODBC per Microsoft Windows

Di seguito sono riportate le versioni precedenti del driver ODBC versione 2.x di Amazon Redshift per Microsoft Windows:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/AmazonRedshiftODBC64-2.1.1.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/AmazonRedshiftODBC64-2.1.0.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/AmazonRedshiftODBC64-2.0.1.0.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/AmazonRedshiftODBC64-2.0.0.11.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/AmazonRedshiftODBC64-2.0.0.9.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/AmazonRedshiftODBC64-2.0.0.8.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/AmazonRedshiftODBC64-2.0.0.7.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/AmazonRedshiftODBC64-2.0.0.6.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/AmazonRedshiftODBC64-2.0.0.5.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/AmazonRedshiftODBC64-2.0.0.3.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/AmazonRedshiftODBC64-2.0.0.1.msi>

## Utilizzo delle versioni precedenti del driver ODBC per Linux

Di seguito sono riportate le versioni precedenti del driver ODBC versione 2.x di Amazon Redshift per Linux:

- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/ AmazonRedshift ODBC-64-bit-2.1.1.0.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.1.0/ AmazonRedshift ODBC-64-bit-2.1.1.0.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/ AmazonRedshift ODBC-64-bit-2.1.0.0.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.1.0.0/ AmazonRedshift ODBC-64-bit-2.1.0.0.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC-64-bit-2.0.1.0.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.1.0/ AmazonRedshift ODBC-64-bit-2.0.1.0.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC-64-bit-2.0.0.11.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.11/ AmazonRedshift ODBC-64-bit-2.0.0.11.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC-64-bit-2.0.0.9.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.9/ AmazonRedshift ODBC-64-bit-2.0.0.9.x86_64.rpm) Nella regione Cina
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC-64-bit-2.0.0.8.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.8/ AmazonRedshift ODBC-64-bit-2.0.0.8.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC-64-bit-2.0.0.7.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.7/ AmazonRedshift ODBC-64-bit-2.0.0.7.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC-64-bit-2.0.0.6.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.6/ AmazonRedshift ODBC-64-bit-2.0.0.6.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC-64-bit-2.0.0.5.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.5/ AmazonRedshift ODBC-64-bit-2.0.0.5.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC-64-bit-2.0.0.3.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.3/ AmazonRedshift ODBC-64-bit-2.0.0.3.x86_64.rpm) Nella regione Cina
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC-64-bit-2.0.0.1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/2.0.0.1/ AmazonRedshift ODBC-64-bit-2.0.0.1.x86_64.rpm) Nella regione Cina

## Configurazione di una connessione ODBC

È possibile utilizzare una connessione ODBC per connettersi al cluster Amazon Redshift da numerose applicazioni e strumenti del client SQL di terze parti. A tale scopo, configurare la connessione sul computer client o sull'istanza Amazon EC2. Se il tuo strumento client supporta JDBC, potresti scegliere di usare quel tipo di connessione piuttosto che ODBC per la facilità di

configurazione garantita da JDBC. Tuttavia, se il tuo strumento client non supporta JDBC, segui la procedura descritta in questa sezione per configurare una connessione ODBC.

Amazon Redshift fornisce driver ODBC a 64 bit per i sistemi operativi Linux, Windows e macOS X. I driver ODBC a 32 bit vengono interrotti. Ulteriori aggiornamenti non verranno rilasciati, tranne che per le patch di sicurezza urgenti.

Per le informazioni più recenti sulle funzionalità e sui prerequisiti dei driver ODBC, consultare le [Note di rilascio del driver ODBC di Amazon Redshift](#).

Per informazioni sull'installazione e la configurazione per i driver ODBC di Amazon Redshift, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

Se desideri utilizzare una connessione ODBC, attieniti alla seguente procedura.

### Argomenti

- [Ottenerne l'URL ODBC per il cluster](#)
- [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#)
- [Installazione del driver ODBC di Amazon Redshift su Linux](#)
- [Installazione del driver ODBC di Amazon Redshift su macOS X](#)
- [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#)
- [Configurazione delle opzioni del driver ODBC](#)
- [Versioni precedenti dei driver ODBC](#)

### Ottenere l'URL ODBC per il cluster

Amazon Redshift visualizza l'URL ODBC per il cluster nella console Amazon Redshift. Questo URL contiene le informazioni per configurare la connessione tra il tuo computer client e il database.

Un URL ODBC ha il formato seguente:

```
Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=password
```

I campi del formato mostrato in precedenza hanno i seguenti valori.

Campo	Valore
Driver	Il nome del driver ODBC a 64 bit da utilizzare: Amazon Redshift (x64).

Campo	Valore
	Il nome del driver ODBC a 32 bit da utilizzare: Amazon Redshift (x86).
Server	L'endpoint del cluster Amazon Redshift.
Database	Il database che hai creato per il tuo cluster.
UID	Nome utente di un account utente che dispone dell'autorizzazione per connettersi al database. Questo valore è un'autorizzazione del database e non di Amazon Redshift, sebbene sia possibile usare l'account utente amministratore configurato all'avvio del cluster.
PWD	Password per l'account utente per connettersi al database.
Port	Numero di porta specificato all'avvio del cluster. In presenza di un firewall, assicurati che questa porta sia aperta per poterla utilizzare.

I campi delle tabelle precedenti possono contenere i seguenti caratteri speciali:

```
[ ] { } ( ) , ; ? * = ! @
```

Se si utilizzano questi caratteri speciali, è necessario racchiudere il valore tra parentesi graffe. Ad esempio, il valore della password `Your ; password123` in una stringa di connessione è rappresentato come `PWD={Your ; password123};`.

Poiché le coppie `Field=value` sono separate da punto e virgola, la combinazione di `}` e `;` con qualsiasi numero di spazi intermedi è considerata la fine di una coppia `Field={value};`. Consigliamo di evitare la sequenza `};` nei valori dei campi. Ad esempio, se imposti il valore della password su `PWD={This is a passwor} ;d};`, la password sarà `This is a passwor} ;` e l'URL genererà un errore.

Di seguito è riportato un esempio di URL ODBC.

```
Driver={Amazon Redshift (x64)};
        Server=examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com;
        Database=dev;
        UID=adminuser;
        PWD=insert_your_admin_user_password_here;
```

```
Port=5439
```

Per informazioni su come ottenere la tua connessione ODBC, consultare [Ricerca della stringa di connessione al cluster](#).

## Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows

### Requisiti di sistema

Il driver ODBC di Amazon Redshift viene installato sui computer client che accedono a un data warehouse Amazon Redshift. Ciascun computer su cui hai installato il driver deve soddisfare una serie di requisiti minimi di sistema: Per informazioni sui requisiti minimi di sistema, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

### Installazione del driver Amazon Redshift su sistemi operativi Windows

Utilizzare la procedura seguente per scaricare i driver ODBC di Amazon Redshift per i sistemi operativi Windows. Utilizzare un driver diverso dai precedenti solo se si sta eseguendo un'applicazione di terze parti certificata per l'utilizzo con Amazon Redshift e che richiede un driver specifico.

### Come installare il driver ODBC

1. Scarica uno dei driver seguenti in base all'architettura di sistema dello strumento client SQL o della applicazione:

- [Driver ODBC a 64 bit versione 1.5.9](#) versione 1.5.9.

Il nome per questo driver è Amazon Redshift (x64).

- [Driver ODBC a 32 bit versione 1.4.52](#) [32 bit versione 1.4.52](#)

Il nome per questo driver è Amazon Redshift (x86). I driver ODBC a 32 bit vengono interrotti. Ulteriori aggiornamenti non verranno rilasciati, tranne che per le patch di sicurezza urgenti.

#### Note

Scarica il pacchetto MSI corrispondente all'architettura di sistema dello strumento client SQL o della applicazione. Ad esempio, se il tuo strumento client SQL è a 64 bit, installa il driver a 64 bit.

Quindi, scaricare ed esaminare il [contratto di licenza del driver ODBC e JDBC di Amazon Redshift](#).

2. Fai doppio clic sul file .msi, quindi segui le fasi della procedura guidata di installazione del driver.

### Creazione di una voce DSN di sistema per una connessione ODBC su Microsoft Windows

Dopo aver scaricato e installato il driver ODBC, aggiungere un nome di origine dati (DSN) al computer client o all'istanza Amazon EC2. Gli strumenti client SQL utilizzano questa origine dati per connettersi al database Amazon Redshift.

Ti consigliamo di creare un DSN di sistema anziché un DSN utente. Alcune applicazioni caricano i dati utilizzando un account utente diverso. Queste applicazioni potrebbero non essere in grado di rilevare i DSN utente creati con un altro account utente.

#### Note

Per l'autenticazione tramite credenziali AWS Identity and Access Management (IAM) o credenziali del provider di identità (IdP), sono necessari passaggi aggiuntivi. Per ulteriori informazioni, consulta [Configurazione di una connessione JDBC o ODBC per utilizzare credenziali IAM](#).

Per informazioni su come creare una voce DSN di sistema, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

Per creare una voce DSN di sistema per una connessione ODBC in Windows

1. Nel menu Start (Avvio) apri ODBC Data Sources (Origini dati ODBC).  
  
Assicurarsi di scegliere l'amministratore dell'origine dati ODBC con gli stessi bit dell'applicazione client che si sta utilizzando per connettersi ad Amazon Redshift.
2. In Amministratore origine dati ODBC, scegli la scheda Driver e individua la cartella del driver.
  - Driver ODBC Amazon Redshift (64 bit)
  - Driver ODBC Amazon Redshift (32 bit)
3. Seleziona la scheda System DSN (DSN sistema) per configurare il driver per tutti gli utenti del computer o la scheda User DSN (DSN utente) per configurare il driver solo per l'account utente.

4. Scegli Aggiungi. Si aprirà la finestra Create New Data Source (Crea nuova origine dati).
5. Selezionare il driver ODBC di Amazon Redshift, quindi scegliere Termina. Si aprirà la finestra Configurazione DNS del driver ODBC per Amazon Redshift.
6. In Connection Settings (Impostazioni di connessione), inserire le informazioni riportate di seguito:

#### Nome origine dati

Inserisci un nome per l'origine dati. Puoi utilizzare qualsiasi nome per identificare l'origine dati successivamente quando crei la connessione al cluster. Ad esempio, se è stata seguita la Guida introduttiva di Amazon Redshift, è possibile digitare `exampleclusterdsn` per ricordare più facilmente il cluster che verrà associato a questo DSN.

#### Server

Specificare l'endpoint per il cluster Amazon Redshift. Queste informazioni sono disponibili nella pagina dei dettagli del cluster della console Amazon Redshift. Per ulteriori informazioni, consulta [Configurazione delle connessioni in Amazon Redshift](#).

#### Porta

Inserisci il numero di porta utilizzato dal database. Utilizza la porta configurata per il cluster al momento dell'avvio o della modifica.

#### Database

Immettere il nome del database Amazon Redshift. Se hai avviato il cluster senza specificare un nome di database, inserisci *dev*. In caso contrario, utilizza il nome scelto durante il processo di avvio. Se è stata seguita la Guida introduttiva di Amazon Redshift, immettere *dev*.

7. In Authentication (Autenticazione), specifica le opzioni di configurazione per configurare l'autenticazione standard o IAM. Per informazioni sulle opzioni di autenticazione, consultare "Configurazione dell'autenticazione su Windows" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.
8. In SSL Settings (Impostazioni SSL), specificare un valore per:

#### Autenticazione SSL

Seleziona una modalità per gestire Secure Sockets Layer (SSL). In un ambiente di test, puoi utilizzare `prefer`. Tuttavia, per gli ambienti di produzione e quando è necessario uno scambio sicuro di dati, utilizza `verify-ca` o `verify-full`. Per ulteriori informazioni sull'utilizzo di

SSL su Windows, consultare "Configurazione della verifica SSL su Windows" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.

9. In Additional Options (Opzioni aggiuntive), specifica le opzioni su come restituire i risultati delle query allo strumento o all'applicazione client SQL. Per ulteriori informazioni, consultare "Configurazione di opzioni aggiuntive su Windows" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.
10. In Logging Options (Opzioni di logging), specifica i valori per l'opzione di logging. Per ulteriori informazioni, consultare "Configurazione delle opzioni di registrazione su Windows" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.

Quindi scegli OK.

11. In Data Type Options (Opzioni tipo di dati), specifica i valori per i tipi di dati. Per ulteriori informazioni, consultare "Configurazione delle opzioni del tipo di dati su Windows" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.

Quindi scegli OK.

12. Scegli Test (Esegui test). Se il computer client riesce a connettersi al database Amazon Redshift, viene visualizzato il messaggio seguente: Connessione riuscita.

Se il computer client non riesce a connettersi al database, puoi provare a risolvere i possibili problemi. Per ulteriori informazioni, consulta [Risoluzione dei problemi di connessione in Amazon Redshift](#).

13. Configura keepalive TCP in Windows per impedire il timeout delle connessioni. Per informazioni su come configurare i keepalive TCP su Windows, consultare la Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.
14. Per facilitare la risoluzione dei problemi, configura il logging. Per informazioni su come configurare la registrazione su Windows, consultare la Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.

## Installazione del driver ODBC di Amazon Redshift su Linux

### Requisiti di sistema

Il driver ODBC di Amazon Redshift viene installato sui computer client che accedono a un data warehouse Amazon Redshift. Ciascun computer su cui hai installato il driver deve soddisfare una serie di requisiti minimi di sistema: Per informazioni sui requisiti minimi di sistema, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

## Installazione del driver di Amazon Redshift su sistemi operativi Linux

Usare la procedura descritta in questa sezione per scaricare e installare i driver ODBC di Amazon Redshift su una distribuzione Linux supportata. Tramite il processo di installazione vengono installati i file del driver nelle seguenti directory:

- /opt/amazon/redshiftdbc/lib/64 (per un driver a 64 bit)
- /opt/amazon/redshiftdbc/ErrorMessage
- /opt/amazon/redshiftdbc/Setup
- /opt/amazon/redshiftdbc/lib/32 (per un driver a 32 bit)

### Come installare il driver ODBC di Amazon Redshift

1. Scarica uno dei driver seguenti in base all'architettura di sistema dello strumento client SQL o della applicazione:
  - [Versione 1.5.9 del driver RPM a 64 bit](#) versione 1.5.9.
  - [Versione del driver Debian a 64 bit 1.5.9 : driver Debian a 64 bit versione 1.5.9.](#)
  - [Versione del driver RPM a 32 bit 1.4.52](#) 32 bit versione 1.4.52
  - [Versione del driver Debian a 32 bit 1.4.52](#) 32 bit versione 1.4.52

Il nome ciascuno di questi driver è Driver ODBC di Amazon Redshift. I driver ODBC a 32 bit vengono interrotti. Ulteriori aggiornamenti non verranno rilasciati, tranne che per le patch di sicurezza urgenti.

#### Note

Scaricare il pacchetto corrispondente all'architettura di sistema dello strumento client SQL o della applicazione. Ad esempio, se lo strumento client è a 64 bit, installare un driver a 64 bit.

Quindi, scaricare ed esaminare il [contratto di licenza del driver ODBC e JDBC di Amazon Redshift](#).

2. Passare alla posizione in cui si è scaricato il pacchetto ed eseguire uno dei comandi seguenti. Utilizzare il comando corrispondente alla distribuzione Linux.

- Nei sistemi operativi RHEL e CentOS , eseguire il comando seguente.

```
yum --nogpgcheck localinstall RPMFileName
```

Sostituire *RPMFileName* con il nome del file del pacchetto RPM. Ad esempio, il comando seguente illustra l'installazione di un driver a 64 bit.

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-64-bit-1.x.xx.xxxx-x.x86_64.rpm
```

- Su SLES, eseguire questo comando.

```
zypper install RPMFileName
```

Sostituire *RPMFileName* con il nome del file del pacchetto RPM. Ad esempio, il comando seguente illustra l'installazione di un driver a 64 bit.

```
zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
```

- Su Debian, eseguire il seguente comando.

```
sudo apt install ./DEBFileName.deb
```

Sostituire *DEBFileName.deb* con il nome del file del pacchetto Debian. Ad esempio, il comando seguente illustra l'installazione di un driver a 64 bit.

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

### Important

Una volta completata l'installazione dei driver, configurali per l'uso sul tuo sistema. Per ulteriori informazioni sulla configurazione dei driver, consulta [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#).

## Installazione del driver ODBC di Amazon Redshift su macOS X

## Requisiti di sistema

Il driver viene installato sui computer client che accedono a un data warehouse Amazon Redshift. Ciascun computer su cui hai installato il driver deve soddisfare una serie di requisiti minimi di sistema: Per informazioni sui requisiti minimi di sistema, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

## Installazione del driver ODBC di Amazon Redshift su macOS X

Utilizzare la procedura descritta in questa sezione per scaricare e installare il driver ODBC di Amazon Redshift su una versione supportata di macOS X. Il processo di installazione installa i file del driver nelle seguenti directory:

- /opt/amazon/redshift/lib/universal
- /opt/amazon/redshift/ErrorMessage
- /opt/amazon/redshift/Setup

## Come installare il driver ODBC di Amazon Redshift su macOS X

1. Se il sistema macOS X utilizza l'architettura Intel, scarica il [driver Intel versione 1.5.9 per macOS X](#). Se il sistema utilizza l'architettura ARM, scarica il [driver ARM versione 1.5.9 per macOS X](#). In entrambi i casi, il nome di questo driver è driver ODBC di Amazon Redshift.

Quindi, scaricare ed esaminare il [contratto di licenza del driver ODBC e JDBC di Amazon Redshift](#).

2. Fate doppio clic su ODBC.dmg AmazonRedshift per montare l'immagine del disco.
3. Fate doppio clic su AmazonRedshiftODBC.pkg per eseguire il programma di installazione.
4. Seguire la procedura nel programma di installazione per completare il processo di installazione del driver. Per eseguire l'installazione, sarà necessario accettare i termini dell'accordo di licenza.

### Important

Una volta completata l'installazione del driver, configuralo per l'uso sul tuo sistema. Per ulteriori informazioni sulla configurazione dei driver, consulta [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#).

## Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X

Sui sistemi operativi Linux e macOS X, utilizzi un gestore di driver ODBC per configurare le impostazioni di connessione ODBC. I gestori di driver ODBC utilizzano i file di configurazione per definire e configurare i driver e le origini dati ODBC. La scelta della gestione driver ODBC dipende dal sistema operativo utilizzato.

- Gestione dei driver unixODBC (per sistemi operativi Linux)
- Gestione driver iODBC (per il sistema operativo macOS X)

Per ulteriori informazioni sulla gestione driver ODBC supportata per configurare i driver ODBC di Amazon Redshift, consultare [Requisiti di sistema](#) per i sistemi operativi Linux e [Requisiti di sistema](#) per i sistemi operativi macOS X. Inoltre, consultare "Specifica della gestione driver ODBC in computer non Windows" nella [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

Per configurare il driver ODBC di Amazon Redshift, sono richiesti tre file:  
`amazon.redshiftdbc.ini`, `odbc.ini` e `odbcinst.ini`.

Se al momento dell'installazione hai utilizzato la posizione predefinita, il file di configurazione `amazon.redshiftdbc.ini` si trova in una delle directory seguenti:

- `/opt/amazon/redshiftdbc/lib/64` (per il driver a 64 bit su sistemi operativi Linux)
- `/opt/amazon/redshiftdbc/lib/32` (per il driver a 32 bit su sistemi operativi Linux)
- `/opt/amazon/redshift/lib` (per il driver su macOS X)

Inoltre, in `/opt/amazon/redshiftdbc/Setup Linux` o `/opt/amazon/redshift/Setup` su macOS X, vi sono i file di esempio `odbc.ini` e `odbcinst.ini`. È possibile utilizzare questi file come esempi per configurare il driver ODBC di Amazon Redshift e il nome origine dati (DSN).

Si sconsiglia di usare la directory di installazione del driver ODBC di Amazon Redshift per i file di configurazione. I file di esempio nella directory Setup sono a puro scopo illustrativo. Se si reinstalla il driver ODBC di Amazon Redshift in un secondo momento o si esegue l'aggiornamento a una versione più recente, la directory di installazione viene sovrascritta. Andranno pertanto perse tutte le modifiche apportate a tali file.

Per evitare questo, copiare il file `amazon.redshiftodbc.ini` in una directory diversa dalla directory di installazione. Se si copia questo file nella home directory dell'utente, aggiungere un punto (.) alla parte iniziale del nome del file per renderlo nascosto.

Per i file `odbcinst.ini` e `odbc.ini`, utilizzare i file di configurazione nella home directory dell'utente o creare nuove versioni in un'altra directory. Per impostazione predefinita, il sistema operativo Linux o macOS X dovrebbe avere un file `odbc.ini` e un file `odbcinst.ini` nella home directory dell'utente (`/home/$USER` o `~/.`). Questi file predefiniti sono file nascosti, come indicato dal punto (.) davanti a ciascun nome del file. Questi file vengono visualizzati solo quando si utilizza il flag `-a` per elencare il contenuto della directory.

Qualunque sia l'opzione scelta per i file `odbc.ini` e `odbcinst.ini`, modificare i file per aggiungere le informazioni di configurazione del driver e del DSN. Se vengono creati nuovi file, è inoltre necessario impostare variabili di ambiente per specificare dove si trovano questi file di configurazione.

Per impostazione predefinita, i gestori del driver ODBC sono configurati per utilizzare versioni nascoste dei file di configurazione `odbc.ini` e di `odbcinst.ini` (denominati `odbc.ini` e `odbcinst.ini`) che si trovano nella home directory. Sono inoltre configurati per utilizzare il file `amazon.redshiftodbc.ini` nella sotto-cartella `/lib` della directory di installazione del driver. Se si archiviano questi file di configurazione altrove, impostare le variabili di ambiente descritte di seguito in modo che il gestore dei driver possa individuare i file. Per ulteriori informazioni, consultare "Specifica delle posizioni dei file di configurazione del driver" nella [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

### Creazione di un nome origine dati su sistemi operativi Linux e macOS X

Quando ti connetti al data store utilizzando un nome origine dati (DSN), configura il file `odbc.ini` per definire il DSN. Imposta le proprietà nel file `odbc.ini` per creare un DSN che specifica le informazioni di connessione per i data store.

Per informazioni su come configurare il `odbc.ini` file, consulta «Creazione di un nome di origine dati su una macchina non Windows» nella guida all'installazione e alla configurazione del [connettore ODBC di Amazon Redshift Nella regione AWS Cina, utilizza il seguente link: Guida all'installazione e alla configurazione](#).

Usa il formato seguente sui sistemi operativi Linux.

```
[ODBC Data Sources]
```

```
driver_name=dsn_name

[dsn_name]
Driver=path/driver_file

Host=cluster_endpoint
Port=port_number
Database=database_name
locale=locale
```

L'esempio seguente mostra la configurazione di `odbc.ini` con il driver ODBC a 64 bit su sistemi operativi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftdbc/lib/64/libamazonredshiftdbc64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

L'esempio seguente mostra la configurazione di `odbc.ini` con il driver ODBC a 32 bit su sistemi operativi Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftdbc/lib/32/libamazonredshiftdbc32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Usa il formato seguente sui sistemi operativi macOS X.

```
[ODBC Data Sources]
driver_name=dsn_name
```

```
[dsn_name]  
Driver=path/lib/amazonredshiftodbc.dylib  
  
Host=cluster_endpoint  
Port=port_number  
Database=database_name  
locale=locale
```

L'esempio seguente mostra la configurazione per `odbc.ini` su sistemi operativi macOS X.

```
[ODBC Data Sources]  
Amazon_Redshift_dylib=Amazon Redshift DSN for macOS X  
  
[Amazon Redshift DSN for macOS X]  
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib  
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com  
Port=5932  
Database=dev  
locale=en-US
```

Configurazione di una connessione senza DSN su sistemi operativi Linux e macOS X

Per connetterti al data store tramite una connessione che non dispone di un DSN, devi definire il driver nel file `odbcinst.ini`. Quindi devi fornire una stringa di connessione senza DSN nell'applicazione.

Per informazioni su come configurare il file `odbcinst.ini` in questo caso, consultare "Configurazione di una connessione senza DSN in un computer non Windows" nella [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

Usa il formato seguente sui sistemi operativi Linux.

```
[ODBC Drivers]  
driver_name=Installed  
...  
  
[driver_name]  
Description=driver_description  
Driver=path/driver_file
```

```
...
```

L'esempio seguente mostra la configurazione `odbcinst.ini` per il driver a 64 bit installato nelle directory predefinite sui sistemi operativi Linux.

```
[ODBC Drivers]
Amazon Redshift (x64)=Installed

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

L'esempio seguente mostra la configurazione `odbcinst.ini` per il driver a 32 bit installato nelle directory predefinite sui sistemi operativi Linux.

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so
```

Usa il formato seguente sui sistemi operativi macOS X.

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib
...
```

L'esempio seguente mostra la configurazione di `odbcinst.ini` per il driver installato nella directory predefinita nei sistemi operativi macOS X.

```
[ODBC Drivers]
Amazon RedshiftODBC DSN=Installed
```

```
[Amazon RedshiftODBC DSN]
Description=Amazon Redshift ODBC Driver for macOS X
Driver=/opt/amazon/redshift/lib/amazonredshiftodbc.dylib
```

## Configurazione delle variabili d'ambiente

Utilizza il gestore driver ODBC corretto per caricare il driver corretto. A tale scopo, imposta la variabile di ambiente del percorso della libreria. Inoltre, consultare "Specifica della gestione driver ODBC in computer non Windows" nella [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

Per impostazione predefinita, i gestori del driver ODBC sono configurati per utilizzare versioni nascoste dei file di configurazione `odbc.ini` e di `odbcinst.ini` (denominati `odbc.ini` e `odbcinst.ini`) che si trovano nella home directory. Sono inoltre configurati per utilizzare il file `amazon.redshiftodbc.ini` nella sotto-cartella `/lib` della directory di installazione del driver. Se memorizzi questi file di configurazione altrove, imposta le variabili di ambiente in modo che il gestore dei driver possa individuare i file. Per ulteriori informazioni, consultare "Specifica delle posizioni dei file di configurazione del driver" nella Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift.

## Configurazione delle funzionalità di connessione

Puoi configurare le seguenti funzionalità di connessione per le tue impostazioni ODBC:

- Configurare il driver ODBC per fornire le credenziali e autenticare la connessione al database Amazon Redshift.
- Configurare il driver ODBC per la connessione a un socket abilitato con Secure Sockets Layer (SSL), se ci si connette a un server Amazon Redshift che ha abilitato SSL.
- Configurare il driver ODBC per la connessione ad Amazon Redshift tramite un server proxy.
- Configura il driver ODBC per utilizzare una modalità di elaborazione delle query per impedire che le query consumino troppa memoria.
- Configurare il driver ODBC per passare i processi di autenticazione IAM attraverso un server proxy.
- Configura il driver ODBC per l'uso di keepalive TCP al fine di impedire il timeout delle connessioni.

Per informazioni su queste caratteristiche di connessione, consultare la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

## Configurazione delle opzioni del driver ODBC

Le opzioni di configurazione possono essere utilizzate per controllare il comportamento del driver ODBC di Amazon Redshift.

In Microsoft Windows, in genere imposti le opzioni del driver quando configuri un nome dell'origine dati (DSN). Puoi anche impostare le opzioni del driver nella stringa di connessione quando ti connetti in modo programmatico oppure aggiungendo o modificando le chiavi di registro in `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN`. Per ulteriori informazioni sulla configurazione di un DSN, consultare [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).

In Linux e macOS X, imposta le opzioni di configurazione del driver nei file `odbc.ini` e `amazon.redshiftdbc.ini`, come descritto in [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#). Le opzioni di configurazione impostate in un file `amazon.redshiftdbc.ini` si applicano a tutte le connessioni. Al contrario, le opzioni di configurazione impostate in un file `odbc.ini` sono specifiche di una connessione. Le opzioni di configurazione impostate in `odbc.ini` hanno la precedenza sulle opzioni di configurazione impostate in `amazon.redshiftdbc.ini`.

Per informazioni su come impostare le opzioni di configurazione del driver ODBC, consulta la [Guida all'installazione e alla configurazione del connettore ODBC di Amazon Redshift](#).

## Versioni precedenti dei driver ODBC

Scaricare una versione precedente del driver ODBC di Amazon Redshift solo se lo strumento richiede una versione specifica del driver.

### Utilizzo delle versioni precedenti del driver ODBC per Windows

Di seguito sono riportati i driver a 64 bit:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC64-1.5.7.1007.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC64-1.4.65.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC64-1.4.62.1000.msi>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC64-1.4.59.1000.msi>

- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC64-1.4.56.1000.msi](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC64-1.4.56.1000.msi)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/ AmazonRedshift ODBC64-1.4.53.1000.msi](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.53.1000/AmazonRedshiftODBC64-1.4.53.1000.msi)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC64-1.4.52.1000.msi](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC64-1.4.52.1000.msi)

I driver a 32 bit sono dismessi e le versioni precedenti non sono supportate.

Utilizzo delle versioni precedenti del driver ODBC per Linux

Di seguito sono elencate le versioni precedenti del driver a 64 bit:

- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-64-bit-1.5.7.1007-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/AmazonRedshiftODBC-64-bit-1.5.7.1007-1.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ AmazonRedshift ODBC-64-bit-1.4.65.1000-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/AmazonRedshiftODBC-64-bit-1.4.65.1000-1.x86_64.rpm) Nella regione Cina
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-64-bit-1.4.62.1000-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/AmazonRedshiftODBC-64-bit-1.4.62.1000-1.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-bit-1.4.59.1000-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-64-bit-1.4.59.1000-1.x86\\_64.deb](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/AmazonRedshiftODBC-64-bit-1.4.59.1000-1.x86_64.deb)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-bit-1.4.56.1000-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-64-bit-1.4.56.1000-1.x86\\_64.deb](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/AmazonRedshiftODBC-64-bit-1.4.56.1000-1.x86_64.deb)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-bit-1.4.52.1000-1.x86\\_64.rpm](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.rpm)
- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-64-bit-1.4.52.1000-1.x86\\_64.deb](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/AmazonRedshiftODBC-64-bit-1.4.52.1000-1.x86_64.deb)

I driver a 32 bit sono dismessi e le versioni precedenti non sono supportate.

## Utilizzo delle versioni precedenti del driver ODBC per macOS X

Di seguito sono riportate le versioni del driver ODBC di Amazon Redshift per macOS X:

- [https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-1.5.7.1007.x86\\_64.dmg](https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.5.7.1007/ AmazonRedshift ODBC-1.5.7.1007.x86_64.dmg) Nella regione Cina, utilizzare
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.65.1000/ ODBC-1.4.65.1000.dmg> Nella regione Cina, utilizzare il seguente link. AmazonRedshift AWS
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.62.1000/ AmazonRedshift ODBC-1.4.62.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.59.1000/ AmazonRedshift ODBC-1.4.59.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.56.1000/ AmazonRedshift ODBC-1.4.56.1000.dmg>
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.52.1000/ AmazonRedshift ODBC-1.4.52.1000.dmg>

## Configurazione delle opzioni di sicurezza per le connessioni

Amazon Redshift supporta le connessioni Secure Sockets Layer (SSL) per crittografare i dati e i certificati server per convalidare il certificato del server a cui si connette il client.

### Connessione tramite SSL

Per supportare le connessioni SSL, Amazon Redshift crea e installa un certificato SSL emesso da [AWS Certificate Manager \(ACM\)](#) su ciascun cluster. I certificati ACM sono attendibili pubblicamente dalla maggior parte dei sistemi operativi, dei browser Web e dei client. Potresti aver bisogno di scaricare un bundle di certificati se i tuoi client o applicazioni SQL si connettono ad Amazon Redshift usando SSL con l'opzione di connessione `sslmode` impostata su `require`, `verify-ca`, o `verify-full`. Se il cliente ha bisogno di un certificato, Amazon Redshift fornisce un certificato di bundle come segue:

- Scarica il bundle da <https://s3.amazonaws.com/redshift-downloads/amazon-trust-ca-bundle.crt>.
  - Il numero di checksum MD5 previsto è 418dea9b6d5d5de7a8f1ac42e164cdf.
  - Il numero di checksum sha256 è 36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

Non utilizzare certificato di bundle precedente che si trovava in <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt>.

- [In Cina, scarica il pacchetto da https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt](https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/amazon-trust-ca-bundle.crt). **Regione AWS**
  - Il numero di checksum MD5 previsto è 418dea9b6d5d5de7a8f1ac42e164cdf.
  - Il numero di checksum sha256 è  
36dba8e4b8041cd14b9d60158893963301bcbb92e1c456847784de2acb5bd550.

Non utilizzare i certificati di bundle precedenti che si trovavano in <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ca-bundle.crt> e <https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem>

 Important

Amazon Redshift ha modificato la modalità di gestione dei certificati SSL. Potrebbe essere necessario aggiornare i certificati CA radice attendibili correnti per continuare a connettersi ai propri cluster utilizzando SSL. Per ulteriori informazioni, consultare [Passaggio ai certificati ACM per connessioni SSL](#).

Per impostazione predefinita, i database del cluster accettano una connessione, che utilizzi o meno SSL. Per configurare il cluster per richiedere una connessione SSL, imposta il parametro `require_ssl` su `true` nel gruppo di parametri associato con il cluster.

Amazon Redshift supporta una modalità SSL conforme al Federal Information Processing Standard (FIPS) 140-2. Per impostazione predefinita, la modalità SSL conforme allo standard FIPS è disabilitata.

 Important

Abilita la modalità SSL conforme a FIPS solo se il sistema deve essere conforme a FIPS.

Per abilitare la modalità SSL conforme a FIPS, imposta sia il `use_fips_ssl` parametro che il parametro `true` nel gruppo di parametri associato `require_ssl` al cluster Amazon Redshift o al

gruppo di lavoro Redshift Serverless. Per informazioni sulla modifica di un gruppo di parametri in un cluster, consulta. [Gruppi di parametri di Amazon Redshift](#). Per informazioni sulla modifica di un gruppo di parametri in un gruppo di lavoro, vedere. [Configurazione di una connessione SSL conforme a FIPS ad Amazon Redshift Serverless](#)

Amazon Redshift supporta il protocollo di accordo chiave Elliptic Curve DiffieHellman Ephemeral (ECDHE). Con il protocollo ECDHE, il client e il server hanno ciascuno una coppia di chiavi pubblica-privata a curva ellittica utilizzata per stabilire un segreto condiviso su un canale insicuro. Per abilitare ECDHE non è necessario eseguire alcuna configurazione in Amazon Redshift. Se ci si connette da uno strumento client SQL che utilizza ECDHE per crittografare la comunicazione tra il client e il server, Amazon Redshift utilizza l'elenco di crittografie fornito per stabilire la connessione appropriata. Per ulteriori informazioni, consultare [Elliptic curve diffie-hellman](#) su Wikipedia e [Ciphers](#) sul sito Web di OpenSSL.

## Utilizzo di certificati CA attendibili e SSL in ODBC

Se ci si connette utilizzando la versione più recente dei driver ODBC di Amazon Redshift (versione 1.3.7.1000 o successiva), è possibile saltare questa sezione. Per scaricare i driver più aggiornati, consultare [Configurazione di una connessione ODBC](#).

Potrebbe essere necessario aggiornare i certificati CA radice attendibili correnti per continuare a connettersi ai propri cluster utilizzando SSL. Per ulteriori informazioni, consultare [Connessione tramite SSL](#).

È possibile verificare che il certificato scaricato corrisponda a questo numero di checksum MD5 previsto. Per fare ciò, è possibile utilizzare il programma Md5sum sui sistemi operativi Linux o un altro strumento sui sistemi operativi Windows e macOS X.

I DSN ODBC contengono un'impostazione `sslmode` che determina come gestire la crittografia per le connessioni client e la verifica dei certificati del server. Amazon Redshift supporta i seguenti valori `sslmode` dalla connessione client:

- `disable`

Il protocollo SSL è disabilitato e la connessione non è crittografata.

- `allow`

Il protocollo SSL è utilizzato se il server lo richiede.

- `prefer`

Se il server lo supporta, è utilizzato il protocollo SSL. Amazon Redshift supporta SSL, quindi SSL viene utilizzato quando si imposta `sslmode` su `prefer`.

- `require`

Il protocollo SSL è obbligatorio.

- `verify-ca`

È necessario utilizzare il protocollo SSL e verificare il certificato del server.

- `verify-full`

È necessario utilizzare il protocollo SSL. È necessario verificare il certificato del server e il nome host del server deve corrispondere all'attributo del nome host sul certificato.

È possibile determinare se SSL viene utilizzato e se i certificati del server sono verificati in una connessione tra il client e il server. Per farlo, è necessario rivedere l'impostazione `sslmode` del DSN ODBC lato client e l'impostazione `require_SSL` del cluster Amazon Redshift sul server. La tabella seguente descrive il risultato della crittografia per varie combinazioni di configurazione di client e server:

<code>sslmode</code> (client)	<code>require_SSL</code> (server)	Risultato
<code>disable</code>	<code>false</code>	La connessione non è crittografata.
<code>disable</code>	<code>true</code>	Non è possibile stabilire la connessione perché il server richiede il protocollo SSL e il client lo ha disabilitato per la connessione.
<code>allow</code>	<code>true</code>	La connessione è crittografata.
<code>allow</code>	<code>false</code>	La connessione non è crittografata.
<code>prefer</code> o <code>require</code>	<code>true</code>	La connessione è crittografata.
<code>prefer</code> o <code>require</code>	<code>false</code>	La connessione è crittografata.

sslmode (client)	require_SSL (server)	Risultato
verify-ca	true	La connessione è crittografata e il certificato del server verificato.
verify-ca	false	La connessione è crittografata e il certificato del server verificato.
verify-full	true	La connessione è crittografata e il certificato del server e il nome host sono verificati.
verify-full	false	La connessione è crittografata e il certificato del server e il nome host sono verificati.

## Connessione tramite il certificato del server con ODBC su Microsoft Windows

Se si desidera connettersi al cluster utilizzando SSL e il certificato server, scaricare innanzitutto il certificato nel computer client o nell'istanza Amazon EC2. Quindi configurare il DSN ODBC.

1. Scaricare il bundle di autorità di certificazione di Amazon Redshift sul computer client nella cartella `lib` all'interno della directory di installazione del driver e salvare il file come `root.crt`. Per informazioni di download, consulta [Connessione tramite SSL](#).
2. Aprire ODBC Data Source Administrator (Amministratore di origini dati ODBC) e aggiungere o modificare la voce DSN di sistema per la connessione ODBC. Per SSL Mode (Modalità SSL), selezionare `verify-full` a meno che non si utilizzi un alias DNS. Se si utilizza un alias DNS, selezionare `verify-ca`. Quindi scegli Save (Salva).

Per ulteriori informazioni sulla configurazione di un DSN ODBC, consultare [Configurazione di una connessione ODBC](#).

## Utilizzo di certificati server e SSL in Java

Il protocollo SSL fornisce un livello di sicurezza crittografando i dati che si spostano tra client e cluster. Tramite l'uso di un certificato del server offre un ulteriore livello di sicurezza verificando che il cluster sia un cluster di Amazon Redshift. A tale scopo, verifica che il certificato del server sia installato automaticamente su tutti i cluster per cui effettui il provisioning. Per ulteriori informazioni

sull'utilizzo di certificati server con JDBC, consultare l'articolo sulla [configurazione del client](#) nella documentazione di PostgreSQL.

Connessione tramite certificati CA attendibili in Java

**⚠ Important**

Amazon Redshift ha modificato la modalità di gestione dei certificati SSL. Potrebbe essere necessario aggiornare i certificati CA radice attendibili correnti per continuare a connettersi ai propri cluster utilizzando SSL. Per ulteriori informazioni, consultare [Connessione tramite SSL](#).

Per connettersi tramite certificati CA attendibili

Puoi utilizzare il `redshift-keytool.jar` file per importare i certificati CA del bundle Amazon Redshift Certificate Authority in Java TrustStore o in un pacchetto privato. TrustStore

1. Se si utilizza l'opzione `-Djavax.net.ssl.trustStore` della riga di comando Java, rimuoverla dalla riga di comando, se possibile.
2. Scaricare [redshift-keytool.jar](#).
3. Esegui una di queste operazioni:
  - Per importare il pacchetto Amazon Redshift Certificate Authority in Java TrustStore, esegui il comando seguente.

```
java -jar redshift-keytool.jar -s
```

- Per importare il pacchetto Amazon Redshift Certificate Authority in modalità privata TrustStore, esegui il seguente comando:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

## Passaggio ai certificati ACM per connessioni SSL

Amazon Redshift sta sostituendo i certificati SSL nei cluster con certificati emessi da [AWS Certificate Manager \(ACM\)](#). ACM è un'autorità di certificazione (CA) pubblica considerata attendibile dalla maggior parte dei sistemi correnti. Potrebbe essere necessario aggiornare i certificati CA radice attendibili correnti per continuare a connettersi ai propri cluster utilizzando SSL.

Questo cambiamento ti riguarda solo in presenza di tutte le condizioni seguenti:

- Le tue applicazioni o i tuoi client SQL si connettono ai cluster Amazon Redshift tramite protocollo SSL con l'opzione di connessione `sslMode` impostata sull'opzione di configurazione `require`, `verify-ca` o `verify-full`.
- Non sono utilizzati i driver JDBC o ODBC di Amazon Redshift o sono utilizzati driver di Amazon Redshift precedenti a ODBC versione 1.3.7.1000 o JDBC versione 1.2.8.1005.

Se la modifica ti riguarda per le regioni Amazon Redshift commerciali, è necessario aggiornare i certificati emessi da una CA radice attendibili correnti prima del 23 ottobre 2017. Amazon Redshift completerà il passaggio dei cluster all'uso di certificati ACM tra la data odierna e il 23 ottobre 2017. Il cambiamento dovrebbe avere un effetto minimo o assente sulle prestazioni o la disponibilità del cluster.

Se questa modifica riguarda alcune regioni AWS GovCloud (US) (Stati Uniti), devi aggiornare i tuoi attuali certificati Trust Root CA prima del 1° aprile 2020 per evitare interruzioni del servizio. A partire da questa data, i client che si connettono a cluster Amazon Redshift che utilizzano connessioni crittografate SSL necessitano di una certification authority (CA) attendibile aggiuntiva. I client utilizzano le certification authority attendibili per confermare l'identità del cluster Amazon Redshift quando si connettono. L'operazione è necessaria per aggiornare i client SQL e le applicazioni al fine di utilizzare un bundle di certificati aggiornato che includa la nuova CA attendibile.

#### Important

Nelle regioni cinesi, il 5 gennaio 2021, Amazon Redshift sostituirà i certificati SSL sui cluster con certificati emessi da AWS Certificate Manager (ACM). Se questa modifica riguarda la regione Cina (Pechino) o la regione Cina (Ningxia), allora sarà necessario aggiornare i certificati CA root attendibili correnti prima del 5 gennaio 2021 per evitare interruzioni del servizio. A partire da questa data, i client che si connettono a cluster Amazon Redshift che utilizzano connessioni crittografate SSL necessitano di una certification authority (CA) attendibile aggiuntiva. I client utilizzano le certification authority attendibili per confermare l'identità del cluster Amazon Redshift quando si connettono. L'operazione è necessaria per aggiornare i client SQL e le applicazioni al fine di utilizzare un bundle di certificati aggiornato che includa la nuova CA attendibile.

- [Utilizzo dei driver ODBC o JDBC di Amazon Redshift più recenti](#)

- [Utilizzo dei driver ODBC o JDBC di Amazon Redshift meno recenti](#)
- [Utilizzo di altri tipi di connessione SSL](#)

### Utilizzo dei driver ODBC o JDBC di Amazon Redshift più recenti

Il metodo preferito prevede l'utilizzo dei driver ODBC o JDBC di Amazon Redshift più recenti. I driver Amazon Redshift a partire dalla versione ODBC 1.3.7.1000 e versione JDBC 1.2.8.1005 gestiscono automaticamente il passaggio da un certificato autofirmato di Amazon Redshift a un certificato ACM. Per scaricare i driver più aggiornati, consultare [Configurazione di una connessione ODBC](#) o [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).

Se utilizzi il driver JDBC di Amazon Redshift più recente, ti consigliamo di non usare `-Djavax.net.ssl.trustStore` nelle opzioni JVM. Se è necessario utilizzare `-Djavax.net.ssl.trustStore`, importare il bundle di autorità di certificazione di Redshift nel truststore a cui fa riferimento. Per informazioni di download, consulta [Connessione tramite SSL](#). Per ulteriori informazioni, consulta [Importazione del pacchetto di autorità di certificazione Amazon Redshift in un TrustStore](#).

### Utilizzo dei driver ODBC o JDBC di Amazon Redshift meno recenti

- Se il tuo DSN ODBC è configurato con `SSLCertPath`, sovrascrivi il file del certificato nel percorso specificato.
- Se `SSLCertPath` non è impostato, sovrascrivi il file del certificato denominato `root.crt` nella posizione del DLL del driver.

Se è necessario utilizzare un driver JDBC Amazon Redshift precedente alla versione 1.2.8.1005, completare una delle operazioni seguenti:

- Se la stringa di connessione JDBC utilizza l'opzione `sslCert`, rimuovi l'opzione `sslCert`. Quindi importa il pacchetto di autorità di certificazione Redshift nel tuo Java. TrustStore Per informazioni di download, consulta [Connessione tramite SSL](#). Per ulteriori informazioni, consulta [Importazione del pacchetto di autorità di certificazione Amazon Redshift in un TrustStore](#).
- Se si utilizza l'opzione `-Djavax.net.ssl.trustStore` della riga di comando Java, rimuoverla dalla riga di comando, se possibile. Quindi importa il pacchetto di autorità di certificazione Redshift nel tuo Java. TrustStore Per informazioni di download, consulta [Connessione tramite SSL](#). Per ulteriori informazioni, consulta [Importazione del pacchetto di autorità di certificazione Amazon Redshift in un TrustStore](#).

## Importazione del pacchetto di autorità di certificazione Amazon Redshift in un TrustStore

Puoi utilizzarli `redshift-keytool.jar` per importare i certificati CA nel bundle Amazon Redshift Certificate Authority in Java TrustStore o nel tuo truststore privato.

Per importare il pacchetto di autorità di certificazione Amazon Redshift in un TrustStore

1. Scaricare [redshift-keytool.jar](#).
2. Esegui una di queste operazioni:
  - Per importare il pacchetto Amazon Redshift Certificate Authority in Java TrustStore, esegui il comando seguente.

```
java -jar redshift-keytool.jar -s
```

- Per importare il pacchetto Amazon Redshift Certificate Authority in modalità privata TrustStore, esegui il seguente comando:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -  
p <keystore_password>
```

## Utilizzo di altri tipi di connessione SSL

Segui la procedura descritta in questa sezione se utilizzi uno dei seguenti metodi di connessione:

- Driver ODBC open source
- Driver JDBC open source
- L'interfaccia a riga di comando [Amazon Redshift RSQL](#)
- Qualsiasi connessione di linguaggio basata su libpq, come psycopg2 (Python) e ruby-pg (Ruby)

Per utilizzare i certificati ACM con altri tipi di connessione SSL:

1. Scaricare il bundle della certification authority di Amazon Redshift. Per informazioni di download, consulta [Connessione tramite SSL](#).
2. Posizionare i certificati del bundle nel file `root.crt`.
  - Sui sistemi operativi Linux e macOS X, il file è `~/postgresql/root.crt`
  - Su Microsoft Windows, il file è `%APPDATA%\postgresql\root.crt`

## Connessione da codice e strumenti client

Amazon Redshift fornisce l'editor di query Amazon Redshift v2 per la connessione ai cluster e ai gruppi di lavoro. Per ulteriori informazioni, consulta [Esecuzione di query in un database con l'editor di query v2 di Amazon Redshift](#).

Questa sezione fornisce alcune opzioni per la connessione mediante strumenti di terze parti. Inoltre, descrive come connettersi al cluster in modo programmatico.

### Argomenti

- [Connessione con Amazon Redshift RSQL](#)
- [Connettersi a un cluster con Amazon Redshift RSQL](#)
- [Comandi meta di Amazon Redshift RSQL](#)
- [Variabili di Amazon Redshift RSQL](#)
- [Codici di errore RSQL di Amazon Redshift](#)
- [Variabili di ambiente Amazon Redshift RSQL](#)

## Connessione con Amazon Redshift RSQL

Amazon Redshift RSQL è un client a riga di comando per interagire con cluster e database Amazon Redshift. Puoi connetterti a un cluster Amazon Redshift, descrivere oggetti di database, interrogare i dati e visualizzare i risultati delle query in diversi formati di output.

Amazon Redshift RSQL supporta le funzionalità dello strumento riga di comando PostgreSQL psql con un set aggiuntivo di funzionalità specifiche di Amazon Redshift. Questi sono i seguenti:

- Puoi usare l'autenticazione Single Sign-On usando ADFS, Okta PingIdentity, Azure ADm o altri provider di identità basati su SAML/JWT. Puoi anche utilizzare provider di identità SAML basati su browser per autenticazione a più fattori (MFA).
- Puoi descrivere le proprietà o gli attributi degli oggetti Amazon Redshift come le chiavi di distribuzione delle tabelle, le chiavi di ordinamento delle tabelle, le viste di associazione tardiva (LBV) e le viste materializzate. È inoltre possibile descrivere proprietà o attributi di tabelle esterne in un catalogo AWS Glue o Metastore Apache Hive, database esterni in Amazon RDS for PostgreSQL, Amazon Aurora edizione compatibile con PostgreSQL, RDS per MySQL (anteprima) e Amazon Aurora edizione compatibile con MySQL (anteprima) e tabelle condivise tramite la condivisione dei dati di Amazon Redshift.

- È inoltre possibile utilizzare comandi di controllo avanzati come IF (\ELSEIF, \ELSE, \ENDIF), \GOTO e \LABEL.

Con la modalità batch di Amazon Redshift RSQL, che esegue uno script passato come parametro di input, è possibile eseguire script che includono sia SQL che la logica di business complessa. Se disponi di data warehouse autogestiti on-premise, puoi utilizzare Amazon Redshift RSQL per sostituire gli script di estrazione, trasformazione, caricamento (ETL) e automazione esistenti, come gli script Teradata BTEQ. L'utilizzo di RSQL aiuta a evitare di reimplementare manualmente gli script in un linguaggio procedurale.

Amazon Redshift RSQL è disponibile per i sistemi operativi Linux, Windows e macOS X.

Per segnalare problemi per Amazon Redshift RSQL, scrivi a [<redshift-rsql-support@amazon.com>](mailto:redshift-rsql-support@amazon.com).

### Argomenti

- [Nozioni di base su Amazon Redshift RSQL](#)
- [Registro delle modifiche di Amazon Redshift RSQL](#)

### Nozioni di base su Amazon Redshift RSQL

Installare Amazon Redshift RSQL su un computer con sistema operativo Linux, macOS o Microsoft Windows.

### Scarica RSQL

- Linux 64-bit RPM: [RSQL Versione 1.0.8](#)
- Mac OS 64-bit DMG: [RSQL Versione 1.0.8](#)
- Windows 64-bit MSI: [RSQL Versione 1.0.8](#)

Consultare il registro delle modifiche e i download per le versioni precedenti in [Registro delle modifiche di Amazon Redshift RSQL](#).

### Installazione di RSQL per Linux

Segui la seguente procedura per installare RSQL per Linux.

1. Installare il driver manager mediante il comando seguente:

```
sudo yum install unixODBC openssl
```

OpenSSL è richiesto per le distribuzioni Linux. La libreria OpenSSL si trova nel repository Github [OpenSSL Linux](#). Per ulteriori informazioni su OpenSSL, consultare [OpenSSL](#).

2. Per installare il driver ODBC: [Installazione del driver di Amazon Redshift su sistemi operativi Linux](#)
3. Copia il file ini nella directory principale:

```
cp /opt/amazon/redshiftodbc/Setup/odbc.ini ~/.odbc.ini
```

4. Impostare le variabili di ambiente in modo che puntino alla posizione del file:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshiftodbc/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshiftodbc/lib/64/
amazon.redshiftodbc.ini
```

Per ulteriori informazioni sulla configurazione delle variabili dell'ambiente ODBC, consultare [Configurazione delle variabili d'ambiente](#).

5. È ora possibile installare RSQL eseguendo il comando seguente.

```
sudo rpm -i AmazonRedshiftRsql-<version>-1.x86_64.rpm
```

## Installazione di RSQL per Mac

Segui la seguente procedura per installare RSQL per Mac OSX.

1. Installare il driver manager mediante il comando seguente:

```
brew install unixodbc openssl@1.1 --build-from-source
```

2. Per installare il driver ODBC: [Installazione del driver ODBC di Amazon Redshift su macOS X](#)
3. Copia il file ini nella directory principale:

```
cp /opt/amazon/redshift/Setup/odbc.ini ~/.odbc.ini
```

4. Impostare le variabili di ambiente in modo che puntino alla posizione del file:

```
export ODBCINI=~/.odbc.ini
export ODBCSYSINI=/opt/amazon/redshift/Setup
export AMAZONREDSHIFTODBCINI=/opt/amazon/redshift/lib/amazon.redshiftdbc.ini
```

Per ulteriori informazioni sulla configurazione delle variabili dell'ambiente ODBC, consultare [Configurazione delle variabili d'ambiente](#).

5. Imposta DYLD\_LIBRARY\_PATH sulla posizione del tuo libodbc.dylib se non è in `/usr/local/lib`.

```
export DYLD_LIBRARY_PATH=$DYLD_LIBRARY_PATH:/usr/local/lib
```

6. Fare doppio clic sul file dmg per montare l'immagine del disco.
7. Fai doppio clic sul file pkg per eseguire il programma di installazione.
8. Seguire la relativa procedura guidata per completare l'installazione. Accetta i termini dell'accordo di licenza.

## Installazione di RSQL per Windows

Seguire le istruzioni su [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#) per installare il driver. Windows non richiede un driver manager.

OpenSSL è richiesto per Amazon Redshift RSQL su Windows. La libreria Windows OpenSSL si trova nell'archivio [Windows OpenSSL](#). GitHub Per ulteriori informazioni su OpenSSL, consultare [OpenSSL](#).

Fai doppio clic sul file di download di RSQL per eseguire il programma di installazione, quindi segui le istruzioni per completare l'installazione.

## Registro delle modifiche di Amazon Redshift RSQL

### 1.0.8 (19-06-2023)

#### Correzioni di bug

- È stato risolto un problema per cui l'output veniva troncato con i comandi SHOW.
- È stato aggiunto il supporto a `\de` per la descrizione di flussi Kinesis esterni e argomenti Kafka.

### 1.0.7 (22-03-2023)

## Correzioni di bug

- È stato risolto un problema che impediva a RSQL di descrivere le viste materializzate.
- È stato risolto un errore di autorizzazione negata su `stl_connection_log` quando si utilizza Amazon Redshift serverless.
- Risolto il problema a causa del quale RSQL poteva elaborare le etichette `\GOTO` in modo errato.
- Risolto il problema per cui i messaggi SSL vengono stampati in modalità silenziosa.
- Risolto il problema relativo alla visualizzazione di caratteri casuali durante la descrizione delle procedure archiviate.
- Risolto il problema con la stampa di messaggi ERROR/INFO duplicati.

## Novità

- RSQL ora ottiene informazioni SSL direttamente dal driver ODBC.

## 1.0.5 (22-02-2023)

### Correzioni di bug

- Risolto un problema per cui `\d` generava un errore - `invalid input syntax for integer: "xid"` (sintassi di input non valida per il numero intero "xid") - nella patch Redshift 1.0.46086 (P173).

## Novità

- File di installazione rinominati in base all'architettura supportata.

## 1.0.5 (27/06/2022)

### Correzioni di bug

- Invia i messaggi di errore SQL a un errore standard (`stderr`).
- Risolto il problema con i codici di uscita quando si utilizza `ON_ERROR_STOP`. Gli script ora terminano dopo aver riscontrato un errore e restituiscono i codici di uscita corretti.
- `Maxerror` adesso non fa distinzione tra maiuscole e minuscole.

## Novità

- Aggiunto il supporto per il driver ODBC 2.x.

### 1.0.4 (2022-03-19)

- Aggiungi il supporto per la variabile d'ambiente RSPASSWORD. Imposta una password per connetterti ad Amazon Redshift. Ad esempio, `export RSPASSWORD=TestPassw0rd.`

### 1.0.3 (2021-12-08)

#### Correzioni di bug

- Finestra di dialogo fissa quando si utilizza `\c` o `\logon` per passare da un database all'altro nel sistema operativo Windows.
- Risolto l'arresto anomalo durante il controllo delle informazioni ssl.

## Versioni precedenti di Amazon Redshift RSQL

Scegli uno dei collegamenti per scaricare la versione di Amazon Redshift RSQL necessaria in base al sistema operativo in uso.

### RPM Linux a 64 bit

- [RSQL versione 1.0.7](#)
- [RSQL versione 1.0.6](#)
- [RSQL versione 1.0.5](#)
- [RSQL versione 1.0.4](#)
- [RSQL versione 1.0.3](#)
- [RSQL versione 1.0.1](#)

### DMG Mac OS a 64 bit

- [RSQL versione 1.0.7](#)
- [RSQL versione 1.0.6](#)

- [RSQL versione 1.0.5](#)
- [RSQL versione 1.0.4](#)
- [RSQL versione 1.0.3](#)
- [RSQL versione 1.0.1](#)

#### MSI Windows a 64 bit

- [RSQL versione 1.0.7](#)
- [RSQL versione 1.0.6](#)
- [RSQL versione 1.0.5](#)
- [RSQL versione 1.0.4](#)
- [RSQL versione 1.0.3](#)
- [RSQL versione 1.0.1](#)

## Connettiti a un cluster con Amazon Redshift RSQL

### Connessione senza DSN

1. Sulla console Amazon Redshift, scegli il cluster a cui vuoi connetterti e annota l'endpoint, il database e la porta.
2. Al prompt dei comandi, specificate le informazioni di connessione usando i parametri della linea di comando.

```
rsql -h <endpoint> -U <username> -d <databasename> -p <port>
```

Qui si applicano le seguenti condizioni:

- *<endpoint>* è l'Endpoint registrato nella fase precedente.
- *<nomeutente>* è il nome di un utente con autorizzazioni per connettersi al cluster.
- *<databasename>* è il Database Name (Nome del database) registrato nella fase precedente.
- *<port>* è la porta che hai registrato nella fase precedente. *<port>* è un parametro facoltativo.

Di seguito è riportato un esempio.

```
rsql -h testcluster.example.amazonaws.com -U user1 -d dev -p 5439
```

3. Alla richiesta della password, immettere la password per l'utente *<nomeutente>*.

Una risposta di connessione riuscita appare come la seguente.

```
% rsql -h testcluster.example.com -d dev -U user1 -p 5349
Password for user user1:
DSN-less Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

Il comando per connettersi ha gli stessi parametri su Linux, Mac OS e Windows.

## Connessione tramite DSN

Puoi connettere RSQL ad Amazon Redshift utilizzando un nome origine dati (DSN) per semplificare l'organizzazione delle proprietà di connessione. Per ulteriori informazioni, consulta [Configurazione delle funzionalità di connessione](#). In questo argomento sono incluse le istruzioni per l'installazione del driver ODBC e le descrizioni delle proprietà DSN. Ad esempio, la sezione seguente, [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#), mostra come connettersi a un DSN utilizzando Windows.

## Utilizzo di una connessione DSN con una password

Di seguito viene illustrato un esempio di configurazione di connessione DSN che utilizza una password. Il `<path to driver>` predefinito per Mac OSX è `/opt/amazon/redshift/lib/libamazonredshiftdbc.dylib` e per Linux è `/opt/amazon/redshiftdbc/lib/64/libamazonredshiftdbc64.so`.

```
[testuser]
Driver=/opt/amazon/redshiftdbc/lib/64/libamazonredshiftdbc64.so
SSLMode=verify-ca
```

```
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<database port>
Database=<dbname>
UID=<username>
PWD=<password>
sslmode=prefer
```

L'output seguente deriva da una connessione riuscita.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

## Utilizzo di DSN Single Sign-On

È possibile configurare un DSN per l'autenticazione Single Sign-On. Di seguito viene illustrato un esempio di configurazione di connessione DSN che utilizza il servizio SSO di Okta.

```
[testokta]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-US
iam=1
plugin_name=<plugin name>
uid=<okta username>
pwd=<okta password>
idp_host=<idp endpoint>
app_id=<app id>
```

```
app_name=<app name>
preferred_role=<role arn>
```

Esempio di output da una connessione riuscita.

```
% rsql -D testokta
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=#
```

Di seguito viene illustrato un esempio di configurazione di connessione DSN che utilizza Azure Single Sign-On.

```
[testazure]
Driver=<path to driver>
SSLMode=verify-ca
Min_TLS=1.2
boolsaschar=0
Host=<server endpoint>
Port=<cluster port>
clusterid=<cluster id>
region=<region name>
Database=<dbname>
locale=en-us
iam=1
plugin_name=<plugin name>
uid=<azure username>
pwd=<azure password>
idp_tenant=<Azure idp tenant uuid>
client_id=<Azure idp client uuid>
client_secret=<Azure idp client secret>
```

## Utilizzo di una connessione DSN con un profilo IAM

Puoi connetterti ad Amazon Redshift utilizzando il profilo IAM configurato. Il profilo IAM deve avere privilegi per chiamare `GetClusterCredentials`. L'esempio seguente mostra le

proprietà DSN da utilizzare. I parametri `ClusterID` e `Region` sono obbligatori solo se il `Host` non è un endpoint fornito da Amazon come `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testiam]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Profile=default
```

Il valore per la `Profile` chiave è il profilo denominato che scegli tra le tue AWS credenziali CLI. In questo esempio vengono mostrate le credenziali per il profilo nominato `default`.

```
$ cat .aws/credentials
[default]
aws_access_key_id = ASIAIOSFODNN7EXAMPLE
aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
```

Di seguito è illustrata la risposta della connessione.

```
$ rsql -D testiam
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

### Utilizzo di una connessione DSN con un profilo dell'istanza

Puoi connetterti ad Amazon Redshift utilizzando il profilo dell'istanza Amazon EC2. Il profilo dell'istanza deve avere privilegi per chiamare `GetClusterCredentials`. Vedere l'esempio riportato di seguito per le proprietà DSN da utilizzare. I parametri `ClusterID` e `Region` sono obbligatori solo

se il Host non è un endpoint fornito da Amazon come `examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com`.

```
[testinstanceprofile]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
IAM=1
Instanceprofile=1
```

Di seguito è illustrata la risposta della connessione.

```
$ rsql -D testinstanceprofile
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) testuser@dev=>
```

Utilizzo di una connessione DSN con la catena di provider delle credenziali di default

Per connetterti utilizzando la catena di provider di credenziali predefinita, specifica solo la proprietà IAM e Amazon Redshift RSQL tenterà di acquisire le credenziali nell'ordine descritto in [Working AWS with Credentials in the SDK for Java](#). AWS Almeno uno dei fornitori della catena deve disporre di autorizzazioni `GetClusterCredentials`. Ciò è utile per il collegamento da container ECS, ad esempio.

```
[iamcredentials]
Driver=Default
Host=testcluster.example.com
Database=dev
DbUser=testuser
ClusterID=rsqltestcluster
Region=us-east-1
```

IAM=1

## Comandi meta di Amazon Redshift RSQL

I comandi meta di Amazon Redshift RSQL restituiscono registri informativi su database o oggetti di database specifici. I risultati possono includere varie colonne e metadati. Altri comandi eseguono azioni specifiche. Questi comandi sono preceduti da una barra rovesciata.

`\d[S+]`

Elenca le tabelle create dall'utente locale, le viste regolari, le viste di associazione tardiva e le viste materializzate. `\dS` elenca anche tabelle e viste, come `\d`, ma gli oggetti di sistema sono inclusi nei registri restituiti. Il `+` ha come risultato la colonna aggiuntiva dei metadati `description` per tutti gli oggetti elencati. Di seguito sono riportati i registri di esempio restituiti come risultato del comando.

```
List of relations
 schema | name      | type  | owner
-----+-----+-----+-----
 public | category | table | awsuser
 public | date     | table | awsuser
 public | event    | table | awsuser
 public | listing  | table | awsuser
 public | sales    | table | awsuser
 public | users    | table | awsuser
 public | venue    | table | awsuser
(7 rows)
```

`\d[S+] NOME`

Descrive una tabella, una vista o un indice. Include i nomi e i tipi di colonna. Fornisce inoltre `diststyle`, configurazione di backup, data di creazione (tabelle create dopo ottobre 2018) e vincoli. Ad esempio, `\dS+ sample` restituisce le proprietà dell'oggetto. L'aggiunta di `S+` ha come risultato colonne aggiuntive incluse nei registri restituiti.

```
Table "public.sample"
 Column |          Type          | Collation | Nullable | Default Value |
 Encoding | DistKey | SortKey
-----+-----+-----+-----+-----
+-----+-----+-----+-----+-----
 coll   | smallint                |           | NO       |               |
 none   | t                       | 1       |         |               |
```

```

col2 | character(100) | case_sensitive | YES | |
none | f | 2
col3 | character varying(100) | case_sensitive | YES | |
text32k | f | 3
col4 | timestamp without time zone | | YES | |
runlength | f | 0
col5 | super | | YES | |
zstd | f | 0
col6 | bigint | | YES | |
az64 | f | 0

```

Diststyle: KEY

Backup: YES

Created: 2021-07-20 19:47:27.997045

Unique Constraints:

"sample\_pkey" PRIMARY KEY (col1)

"sample\_col2\_key" UNIQUE (col2)

Foreign-key constraints:

"sample\_col2\_fkey" FOREIGN KEY (col2) REFERENCES lineitem(l\_orderkey)

Lo stile di distribuzione o Diststyle, della tabella può essere KEY, AUTO, EVEN o ALL.

Backup indica se la tabella viene sottoposta a backup quando viene scattato uno snapshot. I valori validi sono YES e NO.

Crea la data e l'ora di quando viene creata la tabella. La data di creazione non è disponibile per le tabelle Amazon Redshift create prima di novembre 2018. Le tabelle create prima di questa data vengono visualizzate n/d (non disponibile).

Vincoli unici elenca i vincoli di chiave primaria e univoca nella tabella.

Vincoli di chiave straniera elenca i vincoli di chiave straniera nella tabella.

\dC [+] [MODELLO]

Elenca i cast. Include il tipo di origine, il tipo di destinazione e se il cast è implicito.

Di seguito viene mostrato un sottoinsieme di risultati da \dC+.

```

List of casts
      source type | target type | function |
implicit? | description

```

"char"	character	bpchar	in
assignment			
"char"	character varying	text	in
assignment			
"char"	integer	int4	no
"char"	text	text	yes
"path"	point	point	no
"path"	polygon	polygon	in
assignment			
abstime	date	date	in
assignment			
abstime	integer	(binary coercible)	no
abstime	time without time zone	time	in
assignment			
abstime	timestamp with time zone	timestamptz	yes
abstime	timestamp without time zone	timestamp	yes
bigint	bit	bit	no
bigint	boolean	bool	yes
bigint	character	bpchar	in
assignment			
bigint	character varying	text	in
assignment			
bigint	double precision	float8	yes
bigint	integer	int4	in
assignment			
bigint	numeric	numeric	yes
bigint	oid	oid	yes
bigint	real	float4	yes
bigint	regclass	oid	yes

```

bigint          | regoper          | oid            | yes
|
bigint          | regoperator      | oid            | yes
|
bigint          | regproc          | oid            | yes
|
bigint          | regprocedure     | oid            | yes
|
bigint          | regtype          | oid            | yes
|
bigint          | smallint         | int2           | in
assignment |
bigint          | super            | int8_partiql   | in
assignment |

```

`\dd[S] [MODELLO]`

Mostra le descrizioni degli oggetti non visualizzate altrove.

`\de`

Elenca le tabelle esterne. Ciò include le tabelle nel catalogo AWS Glue dati, Hive Metastore e le tabelle federate delle tabelle di datashare Amazon RDS/Aurora MySQL, Amazon RDS/Aurora PostgreSQL e Amazon Redshift.

`\de NOME`

Descrive una tabella esterna.

AWS Glue L'esempio seguente mostra una tabella esterna.

```

# \de spectrum.lineitem
                                Glue External table "spectrum.lineitem"
  Column      | External Type | Redshift Type | Position | Partition Key | Nullable
-----+-----+-----+-----+-----+-----
l_orderkey    | bigint        | bigint        | 1        | 0              |
l_partkey     | bigint        | bigint        | 2        | 0              |
l_suppkey     | int           | int           | 3        | 0              |
l_linenumber  | int           | int           | 4        | 0              |
l_quantity    | decimal(12,2) | decimal(12,2) | 5        | 0              |
l_extendedprice | decimal(12,2) | decimal(12,2) | 6        | 0              |

```

l_discount	decimal(12,2)	decimal(12,2)	7	0	
l_tax	decimal(12,2)	decimal(12,2)	8	0	
l_returnflag	char(1)	char(1)	9	0	
l_linestatus	char(1)	char(1)	10	0	
l_shipdate	date	date	11	0	
l_commitdate	date	date	12	0	
l_receiptdate	date	date	13	0	
l_shipinstruct	char(25)	char(25)	14	0	
l_shipmode	char(10)	char(10)	15	0	
l_comment	varchar(44)	varchar(44)	16	0	

Location: s3://redshiftbucket/kfhose2019/12/31

Input\_format: org.apache.hadoop.mapred.TextInputFormat

Output\_format: org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat

Serialization\_lib: org.apache.hadoop.hive.serde2.lazy.LazySimpleSerDe

Serde\_parameters: {"field.delim": "|", "serialization.format": "|"}

Parameters:

{"EXTERNAL": "TRUE", "numRows": "178196721475", "transient\_lastDdlTime": "1577771873"}

## Un tavolo Hive Metastore.

```
# \de emr.lineitem
```

Hive Metastore External Table "emr.lineitem"

Column	External Type	Redshift Type	Position	Partition Key	Nullable
l_orderkey	bigint	bigint	1	0	
l_partkey	bigint	bigint	2	0	
l_suppkey	int	int	3	0	
l_linenumber	int	int	4	0	
l_quantity	decimal(12,2)	decimal(12,2)	5	0	
l_extendedprice	decimal(12,2)	decimal(12,2)	6	0	
l_discount	decimal(12,2)	decimal(12,2)	7	0	
l_tax	decimal(12,2)	decimal(12,2)	8	0	
l_returnflag	char(1)	char(1)	9	0	
l_linestatus	char(1)	char(1)	10	0	
l_commitdate	date	date	11	0	
l_receiptdate	date	date	12	0	
l_shipinstruct	char(25)	char(25)	13	0	
l_shipmode	char(10)	char(10)	14	0	
l_comment	varchar(44)	varchar(44)	15	0	
l_shipdate	date	date	16	1	

```

Location: s3://redshiftbucket/cetas
Input_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetInputFormat
Output_format: org.apache.hadoop.hive.ql.io.parquet.MapredParquetOutputFormat
Serialization_lib: org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe
Serde_parameters: {"serialization.format":"1"}
Parameters: {"EXTERNAL":"TRUE", "numRows":"4307207",
"transient_lastDdlTime":"1626990007"}

```

## Tabella esterna PostgreSQL.

```

# \de pgrsql.alltypes
                                Postgres Federated Table "pgrsql.alltypes"
Column |          External Type          |          Redshift Type          | Position |
Partition Key | Nullable
-----+-----+-----+-----+-----+
+-----+-----+-----+-----+-----+
col1   | bigint                          | bigint                          | 1        | 0
      |
col2   | bigint                          | bigint                          | 2        | 0
      |
col5   | boolean                         | boolean                         | 3        | 0
      |
col6   | box                             | varchar(65535)                  | 4        | 0
      |
col7   | bytea                           | varchar(65535)                  | 5        | 0
      |
col8   | character(10)                   | character(10)                   | 6        | 0
      |
col9   | character varying(10)           | character varying(10)          | 7        | 0
      |
col10  | cidr                            | varchar(65535)                  | 8        | 0
      |
col11  | circle                          | varchar(65535)                  | 9        | 0
      |
col12  | date                            | date                            | 10       | 0
      |
col13  | double precision                 | double precision                 | 11       | 0
      |
col14  | inet                            | varchar(65535)                  | 12       | 0
      |
col15  | integer                         | integer                         | 13       | 0
      |

```

col16	interval	varchar(65535)	14	0
col17	json	varchar(65535)	15	0
col18	jsonb	varchar(65535)	16	0
col19	line	varchar(65535)	17	0
col20	lseg	varchar(65535)	18	0
col21	macaddr	varchar(65535)	19	0
col22	macaddr8	varchar(65535)	20	0
col23	money	varchar(65535)	21	0
col24	numeric	numeric(38,20)	22	0
col25	path	varchar(65535)	23	0
col26	pg_lsn	varchar(65535)	24	0
col28	point	varchar(65535)	25	0
col29	polygon	varchar(65535)	26	0
col30	real	real	27	0
col31	smallint	smallint	28	0
col32	smallint	smallint	29	0
col33	integer	integer	30	0
col34	text	varchar(65535)	31	0
col35	time without time zone	varchar(65535)	32	0
col36	time with time zone	varchar(65535)	33	0
col37	timestamp without time zone	timestamp without time zone	34	0
col38	timestamp with time zone	timestamp with time zone	35	0

```

col139 | tsquery          | varchar(65535) | 36 | 0
      |
col140 | tsvector         | varchar(65535) | 37 | 0
      |
col141 | txid_snapshot   | varchar(65535) | 38 | 0
      |
col142 | uuid            | varchar(65535) | 39 | 0
      |
col143 | xml              | varchar(65535) | 40 | 0
      |

```

### `\df[anptw][S+] [MODELLO]`

Elenca funzioni di vario tipo. Il comando `\df`, ad esempio, restituisce un elenco di funzioni. I risultati includono proprietà come nome, tipo di dati restituito, privilegi di accesso e metadati aggiuntivi. I tipi di funzioni possono includere trigger, procedure archiviate, funzioni di finestra e altri tipi. Quando si aggiunge `S+` al comando, ad esempio `\dfantS+`, sono incluse colonne di metadati aggiuntive, ad esempio `owner`, `security`, e `access privileges`.

### `\dL[S+] [MODELLO]`

Elenca i dati sui linguaggi procedurali associati al database. Le informazioni includono il nome, come `plpgsql`, e altri metadati, che includono se sono attendibili, privilegi di accesso e descrizione. La chiamata di esempio è, ad esempio, `\dLS+`, che elenca le lingue e le loro proprietà. Quando si aggiunge `S+` al comando, sono incluse colonne di metadati aggiuntive, ad esempio `call handler`, e `access privileges`.

Risultati di esempio:

```

List of languages
 name      | trusted | internal language | call handler | description
 validator |         |                   | access privileges |
-----+-----+-----+-----+-----
c          | f       | t                 | -            |
fmgr_c_validator(oid)
Dynamically-loaded C functions
exfunc    | f       | f                 | exfunc_call_handler() | -
          |         |                   | rdsdb=U/rdsdb    |

```

```

internal | f      | t      | -      |
fmgr_internal_validator(oid)                |      |
Built-in functions
mlfunc   | f      | f      | mlfunc_call_handler() | -
        | rdsdb=U/rdsdb |
plpgsql  | t      | f      | plpgsql_call_handler() |
plpgsql_validator(oid)                      |      |
plpythonu | f     | f     | plpython_call_handler() |
plpython_compiler(cstring,cstring,cstring,cstring,cstring) | rdsdb=U/rdsdb |
sql      | t     | t     | -      |
fmgr_sql_validator(oid)                     | =U/rdsdb | SQL-
language functions

```

`\dm[S+] [MODELLO]`

Elenca le viste materializzate. Ad esempio, `\dmS+` elenca le viste materializzate e le relative proprietà. Quando si aggiunge `S+` al comando, sono incluse colonne di metadati aggiuntive.

`\dn[S+] [MODELLO]`

Elenca schemi. Quando si aggiunge `S+` al comando, ad esempio `\dnS+`, sono incluse colonne di metadati aggiuntive, ad esempio `description` e `access privileges`.

`\dp [MODELLO]`

Elenca i privilegi di accesso a tabella, vista e sequenza.

`\dt[S+] [MODELLO]`

Elenca tabelle. Quando si aggiunge `S+` al comando, ad esempio `\dtS+`, sono incluse colonne di metadati aggiuntive, ad esempio `description` in questo caso.

`\du`

Elenca gli utenti per il database. Include il nome e i ruoli, come utente con privilegi avanzati, e gli attributi.

`\dv[S+] [MODELLO]`

Elenca le viste. Include schema, tipo e dati del proprietario. Quando si aggiunge `S+` al comando, ad esempio `\dvS+`, sono incluse colonne di metadati aggiuntive.

`\H`

Attiva l'output HTML. Ciò è utile per restituire rapidamente risultati formattati. Ad esempio, `select * from sales; \H` restituisce i risultati della tabella di vendita, in HTML. Per tornare ai risultati tabulari, utilizzare `\q`, o silenzioso.

`\i`

Esegue comandi da un file. Ad esempio, supponendo di avere `rsql_steps.sql` nella directory di lavoro, il seguente esegue i comandi nel file: `\i rsql_steps.sql`.

`\l[+] [MODELLO]`

Elenca i database. Include proprietario, codifica e informazioni aggiuntive.

`\q`

L'uscita, o il comando `\q`, disconnette le sessioni del database ed esce da RSQL.

`\sv[+] VISUALIZZAZIONE NOME`

Mostra la definizione di una vista.

`\tempo`

Mostra il tempo di esecuzione, ad esempio per una query.

`\z [MODELLO]`

Lo stesso output di `\dp`.

`\?`

Mostra le informazioni di aiuto. Il parametro facoltativo specifica l'elemento da spiegare.

`\USCITA`

Disconnette tutte le sessioni del database ed esce da Amazon Redshift RSQL. Inoltre, puoi specificare un codice di uscita opzionale. Ad esempio, `\EXIT 15` uscirà dal terminale Amazon Redshift RSQL e restituirà il codice di uscita 15.

L'esempio seguente mostra l'output da una connessione e l'uscita da RSQL.

```
% rsql -D testuser
DSN Connected
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.34.1000
Rsql Version: 1.0.1
Redshift Version: 1.0.29306
Type "help" for help.

(testcluster) user1@dev=# \exit 15

% echo $?
15
```

## \EXPORT

Specifica il nome di un file di esportazione utilizzato da RSQL per memorizzare le informazioni del database restituite da una istruzione SQL SELECT successiva.

export\_01.sql

```
\export report file='E:\\accounts.out'
\rset rformat off
\rset width 1500
\rset heading "General Title"
\rset titledashes on
select * from td_dwh.accounts;
\export reset
```

Output della console:

```
Rformat is off.
Target width is 1500.
Heading is set to: General Title
Titledashes is on.
(exported 40 rows)
```

## \ CONNESSIONE

Si connette a un database. È possibile specificare i parametri di connessione utilizzando la sintassi posizionale o come stringa di connessione.

La sintassi dei comandi è la seguente: `\logon { [DBNAME | - USERNAME | - HOST | - PORT | - [PASSWORD]] | conninfo }`

La DBNAME è il nome del database a cui connettersi. Il USERNAME è il nome utente con cui connettersi. Il HOST predefinito è localhost. Il PORT predefinito è 5439.

Quando viene specificato un nome host in un comando `\LOGON`, diventa il nome host predefinito per ulteriori comandi `\LOGON`. Per modificare il nome host predefinito, specifica un nuovo HOST in un ulteriore comando `\LOGON`.

Output di esempio dal comando `\LOGON` per user1.

```
(testcluster) user1@redshiftdb=# \logon dev
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user1".
(testcluster) user1@dev=#
```

Output di esempio per user2.

```
(testcluster) user1@dev=# \logon dev user2 testcluster2.example.com
Password for user user2:
DBMS Name: Amazon Redshift
Driver Name: Amazon Redshift ODBC Driver
Driver Version: 1.4.27.1000
Rsql Version: 1.0.1
You are now connected to database "dev" as user "user2" on host
"testcluster2.example.com" at port "5439".
(testcluster2) user2@dev=#
```

## NOTA

Un'estensione del comando `\echo`. `\REMARK` stampa la stringa specificata sul flusso di output. `\REMARK` estende `\echo` aggiungendo la possibilità di rompere l'output su linee separate.

L'esempio seguente mostra l'output del comando.

```
(testcluster) user1@dev=# \remark 'hello//world'
hello
world
```

## \RSET

Il comando `\rset` imposta i parametri di comando e le variabili. `\rset` ha sia una modalità interattiva che una modalità batch. Non supporta le opzioni come opzioni bash, come `-x`, o argomenti, ad esempio `--<arg>`.

Imposta le variabili, come le seguenti:

- ERRORLEVEL
- HEADING e RTITLE
- RFORMAT
- MAXERROR
- TITLEDASHES
- WIDTH

Nell'esempio seguente viene specificata un'intestazione.

```
\rset heading "Winter Sales Report"
```

Per ulteriori esempi su come utilizzare `\rset`, consultare gli argomenti [Variabili di Amazon Redshift RSQL](#).

## \ESEGUI

Esegue lo script Amazon Redshift RSQL contenuto nel file specificato. `\RUN` estende il comando `\i` aggiungendo un'opzione per saltare le righe di intestazione in un file.

Se il nome del file include una virgola, un punto e virgola o uno spazio, racchiuderlo tra virgolette singole. Inoltre, se il testo segue il nome del file, racchiuderlo tra virgolette. In UNIX i nomi dei file rispettano la distinzione tra lettere maiuscole e minuscole. In Windows, i nomi di file non distinguono tra maiuscole e minuscole.

L'esempio seguente mostra l'output del comando.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as lineitem_cnt from lineitem;
select count(*) as customer_cnt from customer;
select count(*) as orders_cnt from orders;
```

```
(testcluster) user1@dev=# \run file=test.sql
lineitem_cnt
-----
      4307207
(1 row)

customer_cnt
-----
      37796166
(1 row)

orders_cnt
-----
          0
(1 row)

(testcluster) user1@dev=# \run file=test.sql skip=2
2 records skipped in RUN file.
orders_cnt
-----
          0
(1 row)
```

## \SISTEMA OPERATIVO

Un alias per il comando `\!`. `\OS` esegue il comando del sistema operativo passato come parametro. Il controllo ritorna ad Amazon Redshift RSQL dopo l'esecuzione del comando. Ad esempio, è possibile eseguire il comando seguente per stampare l'ora corrente del sistema e tornare al terminale RSQL:

```
\os date.
```

```
(testcluster) user1@dev=# \os date
Tue Sep 7 20:47:54 UTC 2021
```

## \VAI A

Un nuovo comando per Amazon Redshift RSQL. `\GOTO` salta tutti i comandi intervenuti e riprende l'elaborazione in base alle `\LABEL` specificate. La `\LABEL` deve essere un riferimento in avanti. Non puoi saltare a un `\LABEL` che precede lessicamente il `\GOTO`.

Di seguito viene mostrato l'output di esempio.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) as cnt from lineitem \gset
select :cnt as cnt;
\if :cnt > 100
    \goto LABELB
\endif

\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'
```

```
(testcluster) user1@dev=# \i test.sql
    cnt
-----
 4307207
(1 row)

\label LABELA ignored
\label LABELB processed
this is label LABELB
```

## \ETICHETTA

Un nuovo comando per Amazon Redshift RSQL. `\LABEL` stabilisce un punto di ingresso per l'esecuzione del programma, come obiettivo per un comando `\GOTO`.

L'esempio seguente mostra l'output del comando.

```
(testcluster) user1@dev=# \! cat test.sql
select count(*) from lineitem limit 5;
\goto LABELB
\remark "this step was skipped by goto label";
\label LABELA
\remark 'this is label LABELA'
\label LABELB
\remark 'this is label LABELB'
```

```
(testcluster) user1@dev=# \i testgoto.sql
    count
```

```
4307193
(1 row)
```

```
\label LABELA ignored
\label LABELB processed
this is label LABELB
```

## \SE (\ELSEIF, \ELSE, \ENDIF)

\IF e i comandi correlati eseguono in modo condizionale porzioni dello script di input. Un'estensione del comando PSQL `\if` (`\elif`, `\else`, `\endif`). \IF e \ELSEIF supportano espressioni booleane tra cui le condizioni AND, OR e NOT.

L'esempio seguente mostra un esempio di output dei comandi.

```
(testcluster) user1@dev=# \! cat test.sql
SELECT query FROM stv_inflight LIMIT 1 \gset
select :query as query;
\if :query > 1000000
    \remark 'Query id is greater than 1000000'
\elseif :query = 1000000
    \remark 'Query id is equal than 1000000'
\else
    \remark 'Query id is less than 1000000'
\endif
```

```
(testcluster) user1@dev=# \i test.sql
query
-----
994803
(1 row)

Query id is less than 1000000
```

Utilizza `ERRORCODE` nella tua logica di ramificazione.

```
\if :'ERRORCODE' = '00000'
    \remark 'The statement was executed without error'
\else
    \remark :LAST_ERROR_MESSAGE
\endif
```

Utilizza `\GOTO` all'interno di un blocco `\IF` per controllare come viene eseguito il codice.

## Variabili di Amazon Redshift RSQL

Alcune parole chiave funzionano come variabili in RSQL. È possibile configurare ciascuna parola chiave su un valore specifico o reimpostare il valore. La maggior parte delle parole chiave è impostata con `\rset`, che ha una modalità interattiva e una modalità batch. I comandi possono essere definiti in minuscolo o in maiuscolo.

### ACTIVITYCOUNT

Indica il numero di righe interessate dall'ultima richiesta inviata. Per una richiesta di restituzione dei dati, si tratta del numero di righe restituite a RSQL dal database. Il valore deve essere 0 o un numero intero positivo. Il valore massimo è 18.446.744.073.709.551.615.

La variabile appositamente trattata `ACTIVITYCOUNT` è analoga alla variabile `ROW_COUNT`. Tuttavia, `ROW_COUNT` non riporta all'applicazione client un conteggio delle righe interessate al completamento dei comandi per `SELECT`, `COPY` o `UNLOAD`. Lo fa invece `ACTIVITYCOUNT`.

activitycount\_01.sql:

```
select viewname, schemaname
from pg_views
where schemaname = 'not_existing_schema';
\if :ACTIVITYCOUNT = 0
\remark 'views do not exist'
\endif
```

Output della console:

```
viewname | schemaname
-----+-----
(0 rows)

views do not exist
```

### ERRORLEVEL

Assegna i livelli di gravità agli errori. Utilizzare i livelli di gravità per determinare una linea d'azione. Se il comando `ERRORLEVEL` non è stato usato, per impostazione predefinita il suo valore sarà `ON`.

errorlevel\_01.sql:

```
\rset errorlevel 42P01 severity 0

select * from tbl;

select 1 as col;

\echo exit
\quit
```

### Output della console:

```
Errorlevel is on.
rsql: ERROR: relation "tbl" does not exist
(1 row)

col
1

exit
```

## HEADING e RTITLE

Consente agli utenti di specificare un'intestazione visualizzata nella parte superiore di un report. L'intestazione specificata dal comando RSET RTITLE include automaticamente la data di sistema corrente del computer client.

### Contenuto di rset\_heading\_rtitle\_02.rsq1:

```
\remark Starting...
\rset rtitle "Marketing Department||Confidential//Third Quarter//Chicago"
\rset width 70
\rset rformat on
select * from rsq1_test.tbl_currency order by id limit 2;
\exit
\remark Finishing...
```

### Output della console:

```
Starting...
Rtitle is set to: &DATE||Marketing Department||Confidential//Third Quarter//Chicago
(Changes will take effect after RFORMAT is
switched ON)
```

```

Target width is 70.
Rformat is on.
09/11/20      Marketing      Department Confidential
              Third Quarter
              Chicago
id | bankid | name |      start_date
100 |      1 | USD | 2020-09-11 10:51:39.106905
110 |      1 | EUR | 2020-09-11 10:51:39.106905
(2 rows)

Press any key to continue . . .

```

## MAXERROR

Indica un livello massimo di gravità degli errori oltre il quale RSQL termina l'elaborazione dei processi. I codici restituiti sono valori interi che RSQL restituisce al sistema operativo client dopo aver completato ogni processo o attività. Il valore del codice restituito indica lo stato di completamento del processo o dell'attività. Se uno script contiene un'istruzione che produce un livello di gravità dell'errore maggiore del valore `maxerror` designato, RSQL termina immediatamente. Pertanto, per terminare RSQL su un livello di gravità degli errori pari a 8, utilizzare `RSET MAXERROR 7`.

Contenuto di `maxerror_01.sql`:

```

\rset maxerror 0

select 1 as col;

\quit

```

Output della console:

```

Maxerror is default.
(1 row)

col
1

```

## RFORMAT

Consente agli utenti di specificare se applicare le impostazioni per i comandi di formattazione.

Contenuto di `rset_rformat.rsq1`:

```

\remark Starting...
\pset border 2
\pset format wrapped
\pset expanded on
\pset title 'Great Title'
select * from rsql_test.tbl_long where id = 500;
\rset rformat
select * from rsql_test.tbl_long where id = 500;
\rset rformat off
select * from rsql_test.tbl_long where id = 500;
\rset rformat on
select * from rsql_test.tbl_long where id = 500;
\exit
\remark Finishing...

```

### Output della console:

```

Starting...
Border style is 2. (Changes will take effect after RFORMAT is switched ON)
Output format is wrapped. (Changes will take effect after RFORMAT is switched ON)
Expanded display is on. (Changes will take effect after RFORMAT is switched ON)
Title is "Great Title". (Changes will take effect after RFORMAT is switched ON)
id | long_string
500 | In general, the higher the number the more borders and lines the tables will
    | have, but details depend on the particular
    | format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
  1 ]+-----+
-----+
| id          | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
|             | will have, but details depend on the
|             | particular format. |
+-----+
+-----+
-----+

Rformat is off.

```

```

id | long_string
500 | In general, the higher the number the more borders and lines the tables will
    | have, but details depend on the particular format.
(1 row)

Rformat is on.
Great Title
+-[ RECORD
 1 ]+-----+
-----+
| id          | 500
|
| long_string | In general, the higher the number the more borders and lines the tables
|             | will have, but details depend on the
|             | particular format. |
+-----+
+-----+
-----+
Press any key to continue . . .

```

## ROW\_COUNT

Ottiene il numero di record interessati dalla query precedente. In genere viene utilizzato per controllare un risultato, come nel seguente frammento di codice:

```

SET result = ROW_COUNT;

IF result = 0
...

```

## TITLEDASHES

Questo controllo consente agli utenti di specificare se una riga di caratteri trattino deve essere stampata sopra i dati della colonna restituiti per le istruzioni SQL.

Esempio:

```

\rset titledashes on
select dept_no, emp_no, salary from rsql_test.EMPLOYEE
where dept_no = 100;
\rset titledashes off
select dept_no, emp_no, salary from rsql_test.EMPLOYEE

```

```
where dept_no = 100;
```

Output della console:

```
dept_no    emp_no    salary
-----
100        1000346   1300.00
100        1000245   5000.00
100        1000262   2450.00

dept_no    emp_no    salary
100        1000346   1300.00
100        1000245   5000.00
100        1000262   2450.00
```

## WIDTH

Imposta il formato di output su wrapping e specifica la larghezza di destinazione per ogni riga di un report. Senza un parametro, restituisce le impostazioni correnti sia per il formato che per la larghezza di destinazione.

Contenuto di rset\_width\_01.rsq1:

```
\echo Starting...
\rset width
\rset width 50
\rset width
\quit
\echo Finishing...
```

Output della console:

```
Starting...
Target width is 75.
Target width is 50.
Target width is 50.
Press any key to continue . . .
```

Esempio con parametro:

```
\echo Starting...
\rset rformat on
```

```

\pset format wrapped
select * from rsql_test.tbl_long where id = 500;
\rset width 50
select * from rsql_test.tbl_long where id = 500;
\quit
\echo Finishing...

```

Output della console:

```

Starting...
Rformat is on.
Output format is wrapped.
id |                               long_string
500 | In general, the higher the number the more borders and lines the ta.
    | .bles will have, but details depend on the particular format.
(1 row)

Target width is 50.
id |                               long_string
500 | In general, the higher the number the more.
    | . borders and lines the tables will have, b.
    | .ut details depend on the particular format.
    | ..
(1 row)
Press any key to continue . . .

```

## Codici di errore RSQL di Amazon Redshift

Messaggi di riuscita, avvisi ed eccezioni:

Codice di errore	Classe di errore	Nome della condizione
00000	Classe 00 – Completamento riuscito	successful_completion
01000	Classe 01 – Avvertenza	attenzione
0100C	Classe 01 – Avvertenza	dynamic_result_sets_returned
01008	Classe 01 – Avvertenza	implicit_zero_bit_padding

Codice di errore	Classe di errore	Nome della condizione
01003	Classe 01 – Avvertenza	null_value_eliminated_in_set_function
01007	Classe 01 – Avvertenza	privilege_not_granted
01006	Classe 01 – Avvertenza	privilege_not_revoked
01004	Classe 01 – Avvertenza	string_data_right_truncation
01P01	Classe 01 – Avvertenza	deprecated_feature
02000	Classe 02 – Nessun dato	no_data
02001	Classe 02 – Nessun dato	no_additional_dynamic_result_sets_returned
03000	Classe 03 – Istruzione SQL non ancora completata	sql_statement_not_yet_complete
08000	Classe 08 – Eccezione di connessione	connection_exception
08003	Classe 08 – Eccezione di connessione	connection_does_not_exist
08006	Classe 08 – Eccezione di connessione	connection_failure
08001	Classe 08 – Eccezione di connessione	sqlclient_unable_to_establish_sqlconnection
08004	Classe 08 – Eccezione di connessione	sqlserver_rejected_establishment_of_sqlconnection
08007	Classe 08 – Eccezione di connessione	transaction_resolution_unknown
08P01	Classe 08 – Eccezione di connessione	protocol_violation

Codice di errore	Classe di errore	Nome della condizione
09000	Classe 09 - Eccezione di azione attivata	triggered_action_exception
0A000	Classe 0A - Funzionalità non supportata	feature_not_supported
0A000	Classe 0A - Funzionalità non supportata	feature_not_supported
0B000	Classe 0B - Avvio transazione non valido	invalid_transaction_initiation
0F000	Classe 0F - Eccezione locator	locator_exception
0F001	Classe 0F - Eccezione locator	invalid_locator_specification
0L000	Classe 0L - Grantor non valido	invalid_grantor
0LP01	Classe 0L - Grantor non valido	invalid_grant_operation
0P000	Classe 0P - Specifica del ruolo non valida	invalid_role_specification
0Z000	Classe 0Z - Eccezione diagnostica	diagnostics_exception
0Z002	Classe 0Z - Eccezione diagnostica	stacked_diagnostics_accessed_without_active_handler
20000	Classe 20 - Caso non trovato	case_not_found
21000	Classe 21 - Violazione della cardinalità	cardinality_violation

Eccezioni di dati:

Codice di errore	Classe di errore	Nome della condizione
22000	Classe 22 - Eccezione dati	data_exception
2202E	Classe 22 - Eccezione dati	array_subscript_error
22021	Classe 22 - Eccezione dati	character_not_in_repertoire
22008	Classe 22 - Eccezione dati	datetime_field_overflow
22012	Classe 22 - Eccezione dati	division_by_zero
22005	Classe 01 – Avvertenza	error_in_assignment
2200B	Classe 01 – Avvertenza	escape_character_conflict
22022	Classe 01 – Avvertenza	indicator_overflow
22015	Classe 01 – Avvertenza	interval_field_overflow
2201E	Classe 01 – Avvertenza	invalid_argument_for_logarithm
2201F	Classe 01 – Avvertenza	invalid_argument_for_power_function
2201G	Classe 01 – Avvertenza	invalid_argument_for_width_bucket_function
22018	Classe 01 – Avvertenza	invalid_character_value_for_cast
22007	Classe 01 – Avvertenza	invalid_datetime_format
22019	Classe 01 – Avvertenza	invalid_escape_character
2200D	Classe 01 – Avvertenza	invalid_escape_octet
22025	Classe 01 – Avvertenza	invalid_escape_sequence
22P06	Classe 01 – Avvertenza	nonstandard_use_of_escape_character
22010	Classe 01 – Avvertenza	invalid_indicator_parameter_value
22023	Classe 01 – Avvertenza	invalid_parameter_value

Codice di errore	Classe di errore	Nome della condizione
2201B	Classe 01 – Avvertenza	invalid_regular_expression
22009	Classe 01 – Avvertenza	invalid_time_zone_displacement_value
2200C	Classe 01 – Avvertenza	invalid_use_of_escape_character
2200G	Classe 01 - Avvertenza	most_specific_type_mismatch
22004	Classe 01 – Avvertenza	null_value_not_allowed
22002	Classe 01 – Avvertenza	null_value_no_indicator_parameter
22003	Classe 01 – Avvertenza	numeric_value_out_of_range
22026	Classe 01 - Avvertenza	string_data_length_mismatch
22001	Classe 01 – Avvertenza	string_data_right_truncation
22011	Classe 01 – Avvertenza	substring_error
22027	Classe 01 – Avvertenza	trim_error
22024	Classe 01 – Avvertenza	unterminated_c_string
2200F	Classe 01 – Avvertenza	zero_length_character_string
22P01	Classe 01 – Avvertenza	floating_point_exception
22P02	Classe 01 – Avvertenza	invalid_text_representation
22P03	Classe 01 – Avvertenza	invalid_binary_representation
22P04	Classe 01 – Avvertenza	bad_copy_file_format
22P05	Classe 01 – Avvertenza	untranslatable_character

Violazioni dei vincoli di integrità:

Codice di errore	Classe di errore	Nome della condizione
23000	Classe 23 - Violazione dei vincoli di integrità	integrity_constraint_violation
23001	Classe 23 - Violazione dei vincoli di integrità	restrict_violation
23502	Classe 23 - Violazione dei vincoli di integrità	not_null_violation
23503	Classe 23 - Violazione dei vincoli di integrità	foreign_key_violation
23505	Classe 23 - Violazione dei vincoli di integrità	unique_violation
23514	Classe 23 - Violazione dei vincoli di integrità	check_violation
24000	Classe 24 - Stato cursore non valido	invalid_cursor_state
01004	Classe 01 – Avvertenza	string_data_right_truncation
25000	Classe 25 - Stato transazione non valido	invalid_transaction_state
25001	Classe 25 - Stato transazione non valido	active_sql_transaction
25002	Classe 25 - Stato transazione non valido	invalid_transaction_state
25008	Classe 25 - Stato transazione non valido	held_cursor_requires_same_isolation_level

Codice di errore	Classe di errore	Nome della condizione
25003	Classe 25 - Stato transazione non valido	inappropriate_access_mode_for_branch_transaction
25004	Classe 25 - Stato transazione non valido	inappropriate_isolation_level_for_branch_transaction
25005	Classe 25 - Stato transazione non valido	no_active_sql_transaction_for_branch_transaction
25006	Classe 25 - Stato transazione non valido	read_only_sql_transaction
25007	Classe 25 - Stato transazione non valido	no_active_sql_transaction_for_branch_transaction
25P01	Classe 25 - Stato transazione non valido	no_active_sql_transaction
25P02	Classe 25 - Stato transazione non valido	in_failed_sql_transaction
26000	Class 26 - Nome istruzione SQL non valido	invalid_sql_statement_name
28000	Classe 28 - Specifica di autorizzazione non valida	invalid_authorization_specification
2B000	Classe 2B - Esistono ancora descrittori di privilegi dipendenti	dependent_privilege_descriptors_still_exist
2BP01	Classe 2B - Esistono ancora descrittori di privilegi dipendenti	dependent_objects_still_exist

Codice di errore	Classe di errore	Nome della condizione
2D000	Classe 2D - Terminazione transazione non valida	invalid_transaction_termination
2F000	Classe 2F - Eccezione di routine SQL	sql_routine_exception
2F005	Classe 2F - Eccezione di routine SQL	function_executed_no_return_statement
2F002	Classe 2F - Eccezione di routine SQL	modifying_sql_data_not_permitted
2F003	Classe 2F - Eccezione di routine SQL	prohibited_sql_statement_attempted
2F004	Classe 2F - Eccezione di routine SQL	reading_sql_data_not_permitted
34000	Classe 34 - Nome cursore non valido	invalid_cursor_name
38000	Classe 38 - Eccezione di routine esterna	external_routine_exception
38001	Classe 38 - Eccezione di routine esterna	containing_sql_not_permitted
38002	Classe 38 - Eccezione di routine esterna	modifying_sql_data_not_permitted
38003	Classe 38 - Eccezione di routine esterna	prohibited_sql_statement_attempted
38004	Classe 38 - Eccezione di routine esterna	reading_sql_data_not_permitted

Codice di errore	Classe di errore	Nome della condizione
39000	Classe 39 - Eccezione di richiamo routine esterna	external_routine_invocation_exception
39001	Classe 39 - Eccezione di richiamo routine esterna	invalid_sqlstate_returned
39004	Classe 39 - Eccezione di richiamo routine esterna	null_value_not_allowed
39P01	Classe 39 - Eccezione di richiamo routine esterna	trigger_protocol_violated
39P02	Classe 39 - Eccezione di richiamo routine esterna	srf_protocol_violated
3D000	Classe 3D - Nome catalogo non valido	invalid_catalog_name
3F000	Classe 3F - Nome schema non valido	invalid_schema_name
42000	Classe 42 - Errore di sintassi o violazione delle regole di accesso	syntax_error_or_access_rule_violation
42601	Classe 42 - Errore di sintassi o violazione delle regole di accesso	syntax_error
42501	Classe 42 - Errore di sintassi o violazione delle regole di accesso	insufficient_privilege
42846	Classe 42 - Errore di sintassi o violazione delle regole di accesso	cannot_coerce

Codice di errore	Classe di errore	Nome della condizione
42803	Classe 42 - Errore di sintassi o violazione delle regole di accesso	grouping_error
42830	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_foreign_key
42602	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_name
42622	Classe 42 - Errore di sintassi o violazione delle regole di accesso	name_too_long
42939	Classe 42 - Errore di sintassi o violazione delle regole di accesso	reserved_name
42804	Classe 42 - Errore di sintassi o violazione delle regole di accesso	datatype_mismatch
42P18	Classe 42 - Errore di sintassi o violazione delle regole di accesso	indeterminate_datatype
42809	Classe 42 - Errore di sintassi o violazione delle regole di accesso	wrong_object_type
42703	Classe 42 - Errore di sintassi o violazione delle regole di accesso	undefined_column

Codice di errore	Classe di errore	Nome della condizione
42883	Classe 42 - Errore di sintassi o violazione delle regole di accesso	undefined_function
42P01	Classe 42 - Errore di sintassi o violazione delle regole di accesso	undefined_table
42P02	Classe 42 - Errore di sintassi o violazione delle regole di accesso	undefined_parameter
42704	Classe 42 - Errore di sintassi o violazione delle regole di accesso	undefined_object
42701	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_column
42P03	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_cursor
42P04	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_database
42723	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_function
42P05	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_prepared_statement

Codice di errore	Classe di errore	Nome della condizione
42P06	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_schema
42P07	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_table
42712	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_alias
42710	Classe 42 - Errore di sintassi o violazione delle regole di accesso	duplicate_object
42702	Classe 42 - Errore di sintassi o violazione delle regole di accesso	ambiguous_column
42725	Classe 42 - Errore di sintassi o violazione delle regole di accesso	ambiguous_function
42P08	Classe 42 - Errore di sintassi o violazione delle regole di accesso	ambiguous_parameter
42P09	Classe 42 - Errore di sintassi o violazione delle regole di accesso	ambiguous_alias
42P10	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_column_reference

Codice di errore	Classe di errore	Nome della condizione
42611	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_column_definition
42P11	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_cursor_definition
42 P 12	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_database_definition
42P13	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_function_definition
42P14	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_prepared_statement_definition
42P15	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_schema_definition
42P16	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_table_definition
42P17	Classe 42 - Errore di sintassi o violazione delle regole di accesso	invalid_object_definition
44000	Classe 44 - Violazione WITH CHECK OPTION	with_check_option_violation

Codice di errore	Classe di errore	Nome della condizione
53000	Classe 53 - Risorse non sufficienti	insufficient_resources
53100	Classe 53 - Risorse non sufficienti	disk_full
53200	Classe 53 - Risorse non sufficienti	out_of_memory
53300	Classe 53 - Risorse non sufficienti	too_many_connections
54000	Classe 54 - Limite del programma superato	program_limit_exceeded
54001	Classe 54 - Limite del programma superato	statement_too_complex
54011	Classe 54 - Limite del programma superato	too_many_columns
54023	Classe 54 - Limite del programma superato	too_many_arguments
55000	Classe 55 - Oggetto non in stato prerequisito	object_not_in_prerequisite_state
55006	Classe 55 - Oggetto non in stato prerequisito	object_in_use
55 P 02	Classe 55 - Oggetto non in stato prerequisito	cant_change_runtime_param
55P03	Classe 55 - Oggetto non in stato prerequisito	lock_not_available

Codice di errore	Classe di errore	Nome della condizione
57000	Classe 57 - Intervento dell'operatore	operator_intervention
57014	Classe 57 - Intervento dell'operatore	query_canceled
57P01	Classe 57 - Intervento dell'operatore	admin_shutdown
57P02	Classe 57 - Intervento dell'operatore	crash_shutdown
57P03	Classe 57 - Intervento dell'operatore	cannot_connect_now
58000	Classe 58 - Errore di sistema (errori esterni a PostgreSQL)	system_error
58030	Classe 58 - Errore di sistema (errori esterni a PostgreSQL)	io_error
58P01	Classe 58 - Errore di sistema (errori esterni a PostgreSQL)	undefined_file
58P02	Classe 58 - Errore di sistema (errori esterni a PostgreSQL)	duplicate_file
F0000	Classe F0 - Errore nel file di configurazione	duplicate_file
F0001	Classe F0 - Errore nel file di configurazione	lock_file_exists
P0000	Classe P0 - Errore PL/pgSQL	plpgsql_error
P0001	Classe P0 - Errore PL/pgSQL	raise_exception

Codice di errore	Classe di errore	Nome della condizione
P0002	Classe P0 - Errore PL/pgSQL	no_data_found
P0003	Classe P0 - Errore PL/pgSQL	too_many_rows
XX000	Classe XX - Errore interno	internal_error
XX001	Classe XX - Errore interno	data_corrupted
XX002	Classe XX - Errore interno	index_corrupted

## Variabili di ambiente Amazon Redshift RSQL

Amazon Redshift RSQL può utilizzare variabili di ambiente per selezionare i valori dei parametri predefiniti.

### RSPASSWORD

#### Important

Non è consigliabile utilizzare questa variabile di ambiente per motivi di sicurezza, poiché alcuni sistemi operativi consentono agli utenti non amministrativi di visualizzare le variabili di ambiente di processo.

Imposta la password di Amazon Redshift RSQL da utilizzare per la connessione ad Amazon Redshift. Questa variabile d'ambiente richiede Amazon Redshift RSQL 1.0.4 e versioni successive.

RSQL dà priorità a RSPASSWORD se questa è impostata. Se RSPASSWORD non è impostata e ci si connette utilizzando un DSN, RSQL prende la password dai parametri del file DSN. Infine, se RSPASSWORD non è impostata e non si utilizza un DSN, RSQL fornisce una richiesta di password dopo aver tentato di connettersi.

Di seguito è riportato un esempio di impostazione di RSPASSWORD:

```
export RSPASSWORD=TestPassw0rd
```

## Connessione con SQL Workbench/J

È possibile connettersi a un database utilizzando SQL Workbench/J, uno strumento di query SQL multiplatforma, gratuito e indipendente da DBMS.

Amazon Redshift non fornisce né installa alcuna libreria o alcuno strumento client SQL di terze parti, pertanto è necessario installare eventuali strumenti o librerie che si intende usare con il database. Per installare SQL Workbench/J, segui le istruzioni nella documentazione di SQL Workbench/J ([SQL Workbench/J](#)). In generale, per utilizzare SQL Workbench/J, effettua le seguenti operazioni:

- Verifica la licenza software di SQL Workbench/J.
- Scarica il pacchetto SQL Workbench/J appropriato per il sistema operativo sul computer client o sull'istanza Amazon EC2.
- Installa SQL Workbench/J sul sistema.

Verifica di avere l'ambiente di runtime Java (JRE) installato sul sistema. Assicurarsi di utilizzare la versione corretta di JRE richiesta dal client SQL Workbench/J.

- Connettiti al database attraverso una connessione JDBC in SQL Workbench/J.

Assicurati che il computer client o l'istanza Amazon EC2 dispongano del driver JDBC di Amazon Redshift consigliato. Per accedere ai collegamenti che consentono di scaricare i driver più recenti, consultare [Scarica il driver JDBC Amazon Redshift, versione 2.1](#). Inoltre, assicurati di aver configurato le impostazioni del firewall per consentire l'accesso al database. Per ulteriori informazioni, consulta la [Fase 4: autorizzare l'accesso al cluster nella Guida alle operazioni di base di Amazon Redshift Getting](#).

- Crea un nuovo profilo di connessione in SQL Workbench/J che utilizza il driver Amazon Redshift.

## Connect al tuo data warehouse in modo programmatico

Per informazioni sugli strumenti per creare applicazioni da connettere al data warehouse, consulta [Strumenti per creare in AWS](#).

## Connettersi ad Amazon Redshift con un profilo di autenticazione.

Se hai molte connessioni ad Amazon Redshift, può essere difficile gestire le impostazioni per tutte. Spesso, ogni connessione JDBC o ODBC utilizza opzioni di configurazione specifiche. Utilizzando un profilo di autenticazione, è possibile memorizzare insieme le opzioni di connessione. In questo modo,

gli utenti possono scegliere un profilo con cui connettersi ed evitare di gestire le impostazioni per le singole opzioni. I profili possono essere applicati a diversi scenari e tipi di utente.

Dopo aver creato un profilo di autenticazione, gli utenti possono aggiungere il ready-to-use profilo a una stringa di connessione. In questo modo, possono connettersi ad Amazon Redshift con le impostazioni corrette per ogni ruolo e caso d'uso.

[Per informazioni sull'API Amazon Redshift, consulta `CreateAuthentication Profile`.](#)

## Creazione di un profilo di autenticazione

Utilizzando AWS CLI, crei un profilo di autenticazione con il `create-authentication-profile` comando. In questo modo si presuppone l'esistenza di un cluster Amazon Redshift e di un database esistente. Le credenziali devono disporre dell'autorizzazione per connettersi al database Amazon Redshift e dei diritti per recuperare il profilo di autenticazione. È possibile fornire le opzioni di configurazione come stringa JSON o fare riferimento a un file contenente la stringa JSON.

```
create-authentication-profile --authentication-profile-name<value: String> --
authentication-profile-content<value: String>
```

Nell'esempio seguente viene creato un profilo denominato `ExampleProfileName`. Qui puoi aggiungere chiavi e valori che definiscono il nome del cluster e altre impostazioni di opzione, come stringa JSON.

```
create-authentication-profile --authentication-profile-name "ExampleProfileName"
--authentication-profile-content "{\"AllowDBUserOverride\": \"1\", \"Client_ID
\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID\", \"AutoCreate\": false,
\"enableFetchRingBuffer\": true, \"databaseMetadataCurrentDbOnly\": true}"
}
```

Questo comando crea il profilo con le impostazioni JSON specificate. Viene restituito quanto segue, che indica che il profilo è stato creato.

```
{ "AuthenticationProfileName": "ExampleProfileName",
  "AuthenticationProfileContent": "{\"AllowDBUserOverride\": \"1\",
  \"Client_ID\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID\",
  \"AutoCreate\": false, \"enableFetchRingBuffer\": true,
  \"databaseMetadataCurrentDbOnly\": true}" }
```

## Limitazioni e quote per la creazione di un profilo di autenticazione

Ogni cliente ha una quota di dieci (10) profili di autenticazione.

Alcuni errori possono verificarsi con i profili di autenticazione. Esempi sono se crei un nuovo profilo con un nome esistente o se superi la quota del profilo. Per ulteriori informazioni, vedere [CreateAuthenticationProfile](#).

Non è possibile memorizzare determinate chiavi di opzione e valori per le stringhe di connessione JDBC, ODBC e Python nell'archivio profili di autenticazione:

- AccessKeyID
- access\_key\_id
- SecretAccessKey
- secret\_access\_key\_id
- PWD
- Password
- password

Non è possibile memorizzare la chiave o il valore AuthProfile nell'archivio profili, per le stringhe di connessione JDBC o ODBC. Per le connessioni Python, non è possibile memorizzare auth\_profile.

I profili di autenticazione sono archiviati in Amazon DynamoDB e gestiti da AWS

## Utilizzo di profili di autenticazione

Dopo aver creato un profilo di autenticazione, è possibile includere il nome del profilo come opzione di connessione per JDBC versione 2.0 AuthProfile. L'utilizzo di questa opzione di connessione recupera le impostazioni memorizzate.

```
jdbc:redshift:iam://endpoint:port/database?AuthProfile=<Profile-Name>&AccessKeyID=<Caller-Access-Key>&SecretAccessKey=<Caller-Secret-Key>
```

Di seguito è riportato un esempio di stringa URL JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AuthProfile="ExampleProfile"&AccessKeyID="AKIAIOSFODNN7EXAMPLE"&SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

Specificare entrambi i modelli AccessKeyID e SecretAccessKey nell'URL JDBC, insieme al nome del profilo di autenticazione.

È inoltre possibile separare le opzioni di configurazione con delimitatori punto e virgola, ad esempio nell'esempio seguente, che include le opzioni per la registrazione.

```
jdbc:redshift:iam://my_redshift_end_point:5439/dev?LogLevel=6;LogPath=/
tmp;AuthProfile=my_profile;AccessKeyID="AKIAIOSFODNN7EXAMPLE";SecretAccessKey="wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY"
```

### Note

Non aggiungere informazioni riservate al profilo di autenticazione. Ad esempio, non memorizzare un valore AccessKeyID o SecretAccessKey in un profilo di autenticazione. L'archivio profili di autenticazione dispone di regole per vietare la memorizzazione di chiavi segrete. Viene visualizzato un errore se si tenta di memorizzare una chiave e un valore associati a informazioni sensibili.

## Come ottenere profili di autenticazione

Per elencare i profili di autenticazione esistenti, chiamare il seguente comando.

```
describe-authentication-profiles --authentication-profile-name <value: String>
```

L'esempio seguente mostra due profili recuperati. Tutti i profili vengono restituiti se non si specifica un nome di profilo.

```
{ "AuthenticationProfiles": [ { "AuthenticationProfileName":
"testProfile1", "AuthenticationProfileContent": "{ \"AllowDBUserOverride
\": \"1\", \"Client_ID\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID
\", \"AutoCreate\": false, \"enableFetchRingBuffer\": true,
\"databaseMetadataCurrentDbOnly\": true} } }, { "AuthenticationProfileName":
"testProfile2", "AuthenticationProfileContent": "{ \"AllowDBUserOverride
\": \"1\", \"Client_ID\": \"ExampleClientID\", \"App_ID\": \"ExampleAppID
```

```
\",\"AutoCreate\":false,\"enableFetchRingBuffer\":true,  
\"databaseMetadataCurrentDbOnly\":true}\" } ] }
```

## Risoluzione dei problemi di connessione in Amazon Redshift

Se riscontri anomalie nella connessione al cluster da uno strumento client SQL, è possibile circoscrivere il problema verificando diversi elementi. Se stai utilizzando certificati di server o SSL, prima rimuovi questa complessità mentre risolvi il problema relativo alla connessione. Quando trovi una soluzione, aggiungila nuovamente. Per ulteriori informazioni, consulta [Configurazione delle opzioni di sicurezza per le connessioni](#).

### Important

Amazon Redshift ha modificato la modalità di gestione dei certificati SSL. In caso di problemi di connessione tramite SSL, potrebbe essere necessario aggiornare i tuoi certificati CA radice attendibili correnti. Per ulteriori informazioni, consulta [Passaggio ai certificati ACM per connessioni SSL](#).

La seguente sezione include alcuni messaggi di errore di esempio e le possibili soluzioni per problemi di connessione. Dal momento che diversi strumenti client SQL forniscono messaggi di errore differenti, questo elenco non è completo ma rappresenta un buon punto di partenza per la risoluzione dei problemi.

### Argomenti

- [Connessione al di fuori di Amazon EC2: problema di timeout del firewall](#)
- [Connessione rifiutata o non riuscita](#)
- [Incompatibilità tra client e driver](#)
- [Query bloccate e talvolta impossibilitate a raggiungere il cluster](#)
- [Impostazione del parametro delle dimensioni del recupero JDBC](#)

## Connessione al di fuori di Amazon EC2: problema di timeout del firewall

### Esempio di problema

Al momento dell'esecuzione di query lunghe, come il comando COPY, la connessione del tuo client al database sembra scadere o interrompersi. In questo caso, è possibile che la console Amazon

Redshift mostri che la query è stata completata, ma lo strumento del client stesso sembra che la stia ancora eseguendo. I risultati della query potrebbero essere mancanti o incompleti, a seconda del momento in cui la connessione si è interrotta.

## Possibili soluzioni

Questo problema si verifica quando ci si connette ad Amazon Redshift da un computer diverso da un'istanza Amazon EC2. In questo caso, le connessioni inattive vengono terminate da un componente di rete intermedio, ad esempio un firewall, dopo un periodo di inattività. Questo comportamento è tipico quando ci si connette da una rete privata virtuale (VPN) o dalla rete locale.

Per evitare questi timeout, ti consigliamo di apportare le seguenti modifiche:

- Aumenta i valori del sistema client che gestiscono i timeout TCP/IP. Esegui queste modifiche sul computer che stai utilizzando per connetterti al cluster. Il periodo di timeout deve essere regolato per il tuo client e la tua rete. Per ulteriori informazioni, consulta [Modifica delle impostazioni del timeout TCP/IP](#).
- A scelta, puoi configurare il comportamento keepalive a livello DSN. Per ulteriori informazioni, consulta [Modifica delle impostazioni del timeout DSN](#).

## Modifica delle impostazioni del timeout TCP/IP

Per modificare le impostazioni del timeout TCP/IP, configurale in base al sistema operativo che utilizzi per connetterti al cluster.

- Linux: se il client è in esecuzione su Linux, emettere il comando seguente come utente root per cambiare le impostazioni di timeout per la sessione corrente:

```
/sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200  
net.ipv4.tcp_keepalive_probes=5
```

Per mantenere le impostazioni, crea o modifica il file `/etc/sysctl.conf` con i seguenti valori, quindi riavvia il sistema.

```
net.ipv4.tcp_keepalive_time=200  
net.ipv4.tcp_keepalive_intvl=200  
net.ipv4.tcp_keepalive_probes=5
```

- **Windows:** se il tuo client funziona su Windows, modifica i valori per le seguenti impostazioni di registro in HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControl Set\Services\Tcpip\Parameters\:
  - KeepAliveTempo: 30000
  - KeepAliveIntervallo: 1000
  - TcpMaxDataRetransmissions: 10

Queste impostazioni utilizzano il tipo di dati DWORD. Se non esistono nel percorso di registro, è possibile creare le impostazioni e specificare questi valori raccomandati. Per ulteriori informazioni sulla modifica del registro di Windows, consultare la documentazione di Windows.

Dopo aver impostato questi valori, riavvia il computer per rendere effettive le modifiche.

- **Mac:** se il client è in esecuzione su un Mac, emettere i comandi seguenti per cambiare le impostazioni di timeout per la sessione corrente:

```
sudo sysctl net.inet.tcp.keepintvl=200000
sudo sysctl net.inet.tcp.keepidle=200000
sudo sysctl net.inet.tcp.keepinit=200000
sudo sysctl net.inet.tcp.always_keepalive=1
```

Per mantenere le impostazioni, crea o modifica il file `/etc/sysctl.conf` con i seguenti valori:

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Riavvia il computer, quindi esegui i comandi seguenti per verificare che i valori siano stati impostati.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

## Modifica delle impostazioni del timeout DSN

A scelta, è possibile configurare il comportamento keepalive a livello DSN. Puoi farlo aggiungendo o modificando i parametri seguenti nel file `odbc.ini`:

### KeepAlivesConta

Il numero di pacchetti keepalive TCP che possono essere persi prima che la connessione sia considerata interrotta.

### KeepAlivesInattivo

Il numero di secondi di inattività prima che il driver invii un pacchetto keepalive TCP.

### KeepAlivesIntervallo

Il numero di secondi tra ciascuna ritrasmissione di keepalive TCP.

In Windows, si modificano questi parametri nel registro aggiungendo o cambiando le chiavi in `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN`. In Linux e macOS, aggiungi o modifichi questi parametri nella voce DSN di destinazione direttamente nel file `odbc.ini`. Per ulteriori informazioni sulla modifica del file `odbc.ini` su computer Linux e macOS, consultare [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#).

Se questi parametri non esistono o se hanno un valore pari a 0, il sistema utilizza i parametri keepalive specificati per TCP/IP per determinare il comportamento keepalive DSN. In Windows, puoi trovare i parametri TCP/IP nel Registro di sistema in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\`. In Linux e macOS, i parametri TCP/IP sono disponibili nel file `sysctl.conf`.

## Connessione rifiutata o non riuscita

### Esempi di errori

- "Failed to establish a connection to *<endpoint>*" ("Impossibile stabilire una connessione con *<endpoint>*").
- "Could not connect to server: Connection timed out. Is the server running on host '*<endpoint>*' and accepting TCP/IP connections on port '*<port>*'?" ("Il server è in esecuzione sull'*<endpoint>* dell'host e accetta le connessioni TCP/IP sulla porta *<port>*?").

- "Connection refused. Check that the hostname and port are correct and that the postmaster is accepting TCP/IP connections." ("Connessione rifiutata. Controlla che il nome host e la porta siano corretti e che il postmaster accetti le connessioni TCP/IP.")

## Possibili soluzioni

Generalmente, quando ricevi un messaggio di errore che indica l'impossibilità di stabilire una connessione, ciò significa che c'è un problema con l'autorizzazione per l'accesso al cluster o con il traffico di rete che raggiunge il cluster.

Per connetterti al cluster da uno strumento client esterno alla rete in cui si trova il cluster stesso, aggiungi una regola di ingresso al gruppo di sicurezza del cluster. La configurazione delle regole dipende dal fatto che il cluster Amazon Redshift sia creato in un cloud privato virtuale (VPC):

- Se il cluster Amazon Redshift è stato creato in un cloud privato virtuale (VPC) basato su Amazon VPC, aggiungi l'indirizzo CIDR/IP del client al gruppo di sicurezza VPC che specifica il CIDR client/indirizzo IP in Amazon VPC. Per ulteriori informazioni sulla configurazione dei gruppi di sicurezza VPC per il cluster, consulta [Gestione dei cluster in un VPC](#).
- Se è stato creato un cluster Amazon Redshift all'esterno di un VPC, è necessario aggiungere l'indirizzo CIDR/IP del client al gruppo di sicurezza del cluster in Amazon Redshift. Per ulteriori informazioni sulla configurazione di gruppi di sicurezza dei cluster, consulta [Gruppi di sicurezza dei cluster Amazon Redshift](#).

Se provi a connetterti al cluster da uno strumento client in un'istanza Amazon EC2, viene aggiunta anche una regola di entrata. In questo caso, aggiungi una regola al gruppo di sicurezza del cluster. La regola deve specificare il gruppo di sicurezza Amazon EC2 associato all'istanza Amazon EC2 dello strumento client.

In alcuni casi, potrebbe essere presente un layer tra il client e il server, ad esempio un firewall. In questi casi, assicurarti che il firewall accetti le connessioni in ingresso sulla porta configurata per il cluster.

## Incompatibilità tra client e driver

### Esempio di errore

"The specified DSN contains an architecture mismatch between the Driver and Application." ("Il DSN specificato presenta una mancata corrispondenza di architettura tra driver e applicazione.")

## Possibile soluzione

Quando tenti di connetterti e ricevi un errore relativo a una mancata corrispondenza dell'architettura, ciò significa che lo strumento client e il driver non sono compatibili. Ciò si verifica perché la loro architettura di sistema non corrisponde. Ad esempio, ciò può accadere se disponi di uno strumento client a 32 bit ma hai installato una versione a 64 bit del driver. Talvolta gli strumenti client a 64 bit possono utilizzare driver a 32 bit, ma non è possibile usare applicazioni a 32 bit con driver a 64 bit. Assicurati che il driver e lo strumento client utilizzino la stessa versione dell'architettura di sistema.

## Query bloccate e talvolta impossibilitate a raggiungere il cluster

### Esempio di problema

Riscontri un problema con il completamento delle query, che sembrano in esecuzione ma che si bloccano nello strumento client SQL. Talvolta le query non vengono visualizzate nel cluster, come nelle tabelle di sistema o nella console Amazon Redshift.

### Possibile soluzione

Questo problema può verificarsi a causa della perdita dei pacchetti. In questo caso, vi è una differenza nella dimensione massima unità di trasmissione (MTU) nel percorso di rete tra due host Internet Protocol (IP). La dimensione della MTU determina la dimensione massima, espressa in byte, di un pacchetto che può essere trasferito in un frame Ethernet su una connessione di rete. In AWS, alcuni tipi di istanze Amazon EC2 supportano un MTU di 1500 (frame Ethernet v2) e altri tipi di istanza supportano un MTU di 9001 (jumbo frame TCP/IP).

Per evitare problemi associati alle differenze di dimensione della MTU, ti consigliamo di procedere in uno dei modi seguenti:

- Se il cluster utilizza la piattaforma EC2-VPC, configurare il gruppo di sicurezza Amazon VPC con una regola ICMP (Internet Control Message Protocol) personalizzata in entrata che restituisce `Destination Unreachable`. Questa regola indica all'host di origine di utilizzare la dimensione della MTU minima sul percorso di rete. Per i dettagli su questo approccio, consulta [Configurazione dei gruppi di sicurezza per autorizzare il messaggio ICMP "Destination Unreachable"](#).
- Se il tuo cluster utilizza la piattaforma EC2-Classical, o non puoi autorizzare la regola in entrata ICMP, disabilita i jumbo frame TCP/IP in modo che vengano utilizzati i frame Ethernet v2. Per i dettagli su questo approccio, consulta [Configurazione della MTU di un'istanza](#).

## Configurazione dei gruppi di sicurezza per autorizzare il messaggio ICMP "Destination Unreachable"

In presenza di una differenza della dimensione della MTU nella rete tra due host, verifica innanzitutto che le impostazioni della tua rete non blocchino l'individuazione della MTU del percorso (PMTUD). La PMTUD consente all'host ricevente di rispondere all'host di origine con il seguente messaggio ICMP: `Destination Unreachable: fragmentation needed and DF set` (ICMP Type 3, Code 4). Questo messaggio indica all'host di origine di utilizzare la dimensione della MTU più piccola sul percorso di rete per inviare nuovamente la richiesta. Senza questa negoziazione, può verificarsi la perdita del pacchetto perché la richiesta è troppo grande per l'host ricevente. Per ulteriori informazioni sul messaggio ICMP, consultare [RFC792](#) sul sito Web Internet Engineering Task Force (IETF).

Se non si configura in modo esplicito questa regola in entrata ICMP per il gruppo di sicurezza Amazon VPC, la PMTUD viene bloccata. In AWS, i gruppi di sicurezza sono firewall virtuali che specificano le regole per il traffico in entrata e in uscita verso un'istanza. Per informazioni sui gruppi di sicurezza dei cluster Amazon Redshift, consultare [Gruppi di sicurezza dei cluster Amazon Redshift](#). Per i cluster che utilizzano la piattaforma EC2-VPC, Amazon Redshift usa i gruppi di sicurezza VPC che consentono o rifiutano il traffico al cluster. Per impostazione predefinita, i gruppi di sicurezza sono bloccati e rifiutano tutto il traffico in entrata. Per informazioni su come impostare le regole in entrata e in uscita per le istanze EC2-Classical o EC2-VPC, consulta Differenze [tra le istanze in EC2-Classical e un VPC nella Amazon](#) EC2 User Guide.

Per ulteriori informazioni su come aggiungere regole ai gruppi di sicurezza VPC, consultare [Gestione dei gruppi di sicurezza VPC per un cluster](#). Per ulteriori informazioni sulle impostazioni PMTUD specifiche richieste in questa regola, consulta [Path MTU discovery](#) nella Amazon EC2 User Guide.

## Configurazione della MTU di un'istanza

In alcuni casi, il cluster potrebbe utilizzare la piattaforma EC2 Classical o non potresti non consentire la regola ICMP personalizzata per il traffico in ingresso. In questi casi, consigliamo di regolare l'MTU su 1500 sull'interfaccia di rete (NIC) delle istanze EC2 da cui ci si connette al cluster Amazon Redshift. Questo adeguamento disabilita i jumbo frame TCP/IP per garantire che le connessioni utilizzino in modo coerente la stessa dimensione del pacchetto. Tuttavia, questa opzione riduce la velocità effettiva massima della rete per l'intera istanza, non solo per le connessioni ad Amazon Redshift. Per ulteriori informazioni, consultare le procedure seguenti.

## Per impostare la MTU su un sistema operativo Microsoft Windows

Se il client viene eseguito in un sistema operativo Microsoft Windows, è possibile rivedere e impostare il valore MTU per la scheda Ethernet tramite il comando `netsh`.

1. Eseguire il seguente comando per determinare il valore MTU corrente:

```
netsh interface ipv4 show subinterfaces
```

2. Rivedere il valore MTU per la scheda Ethernet nell'output.
3. Se il valore non è 1500, eseguire il seguente comando per impostarlo:

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
```

Dopo aver impostato questo valore, riavviare il computer per rendere effettive le modifiche.

### Per impostare la MTU su un sistema operativo Linux

Se il client viene eseguito in un sistema operativo Linux, è possibile rivedere e impostare il valore MTU tramite il comando `ip`.

1. Eseguire il seguente comando per determinare il valore MTU corrente:

```
$ ip link show eth0
```

2. Rivedere il valore successivo a `mtu` nell'output.
3. Se il valore non è 1500, eseguire il seguente comando per impostarlo:

```
$ sudo ip link set dev eth0 mtu 1500
```

### Per impostare la MTU su un sistema operativo Mac

- Seguire le istruzioni sul sito di supporto macOS per [How to change the MTU for troubleshooting purposes](#). Per ulteriori informazioni, cercare nel [sito del supporto](#).

### Impostazione del parametro delle dimensioni del recupero JDBC

Per impostazione predefinita, il driver JDBC raccoglie tutti i risultati di una query in una sola volta. Di conseguenza, quando si tenta di recuperare un set di risultati di grandi dimensioni tramite una connessione JDBC, è possibile che si verifichi un errore sul lato client. `out-of-memory` Per consentire al client di recuperare i set di risultati in batch anziché in un singolo recupero, impostate il parametro `all-or-nothing JDBC fetch size` nell'applicazione client.

**Note**

La dimensione del recupero non è supportata da ODBC.

Per le migliori prestazioni, imposta la dimensione del recupero sul valore più alto che non porti a errori di esaurimento della memoria. Un valore della dimensione del recupero più basso causa più viaggi del server, quindi tempi di esecuzione prolungati. Il server riserva le risorse, tra cui lo slot della query WLM e la memoria associata, fino al momento in cui il client recupera tutto l'insieme di risultati o la query viene cancellata. Quando ottimizzi in modo appropriato la dimensione del recupero, queste risorse vengono rilasciate più velocemente rendendole disponibili alle altre query.

**Note**

Se devi estrarre set di dati di grandi dimensioni, ti consigliamo di utilizzare un'istruzione [UNLOAD](#) per trasferire i dati su Amazon S3. Quando usi UNLOAD, i nodi di calcolo lavorano in parallelo per velocizzare il trasferimento dei dati.

Per ulteriori informazioni sull'impostazione del parametro della dimensione del recupero di JDBC, consultare [Ottenimento di risultati basato su un cursore](#) nella documentazione PostgreSQL.

## Uso dell'API dati di Amazon Redshift

È possibile accedere al database Amazon Redshift utilizzando l'API dati integrata di Amazon Redshift. Utilizzando questa API, puoi accedere ai dati di Amazon Redshift con applicazioni basate su servizi Web, tra cui notebook AWS Lambda Amazon e SageMaker AWS Cloud9. Per ulteriori informazioni su queste applicazioni [AWS Lambda](#), consulta [Amazon SageMaker](#) e [AWS Cloud9](#).

L'API dati non richiede una connessione permanente al database. Fornisce invece un endpoint HTTP sicuro e l'integrazione con gli AWS SDK. Puoi usare l'endpoint per eseguire istruzioni SQL senza gestire connessioni. Le chiamate all'API dati sono asincrone.

L'API Data utilizza credenziali archiviate nel database AWS Secrets Manager o credenziali temporanee del database. Non è necessario utilizzare alcuna password nelle chiamate API con entrambi i metodi di autorizzazione. Per ulteriori informazioni su AWS Secrets Manager, consulta [What Is? AWS Secrets Manager](#) nella Guida AWS Secrets Manager per l'utente.

Per ulteriori informazioni sulle operazioni API dati, consultare [Guida di riferimento dell'API dati di Amazon Redshift](#).

## Operazioni con l'API dati Amazon Redshift

Prima di utilizzare l'API dati Amazon Redshift, verificare quanto riportato di seguito:

1. Determinare se l'utente, come chiamante dell'API dati, è autorizzato. Per ulteriori informazioni sull'autorizzazione, consultare [Autorizzazione di accesso all'API dati di Amazon Redshift](#).
2. Determinare se si prevede di chiamare l'API dati con credenziali di autenticazione da Secrets Manager o con credenziali temporanee. Per ulteriori informazioni, consultare [Scelta delle credenziali di autenticazione del database quando si richiama l'API dati di Amazon Redshift](#).
3. Se si utilizza Secrets Manager impostare un segreto per le credenziali di autenticazione. Per ulteriori informazioni, consultare [Memorizzazione delle credenziali del database in AWS Secrets Manager](#).
4. Esaminare le considerazioni e le limitazioni quando si chiama l'API dati. Per ulteriori informazioni, consulta [Considerazioni da fare durante la chiamata all'API dati di Amazon Redshift](#).
5. Chiama l'API Data da AWS Command Line Interface (AWS CLI), dal tuo codice o utilizzando l'editor di query nella console Amazon Redshift. Per esempi di chiamate da AWS CLI, consulta [Chiamata dell'API dati](#).

## Considerazioni da fare durante la chiamata all'API dati di Amazon Redshift

Considerare quanto riportato di seguito quando si effettua la chiamata dell'API dati:

- L'API dati di Amazon Redshift può accedere ai database nei cluster sottoposti a provisioning di Amazon Redshift e nei gruppi di lavoro Redshift serverless. Per un elenco delle aree Regioni AWS in cui è disponibile l'API Redshift Data, consulta gli endpoint elencati per [Redshift Data API](#) nel Riferimenti generali di Amazon Web Services
- La durata massima di una query è di 24 ore.
- Il numero massimo di query attive (query STARTED e SUBMITTED) per cluster Amazon Redshift è 200.
- La dimensione massima dei risultati della query è 100 MB (dopo la compressione gzip). Se la chiamata restituisce più di 100 MB di dati di risposta, verrà terminata.
- Il tempo massimo di conservazione dei risultati delle query è 24 ore.

- La dimensione massima dell'istruzione della query è 100 KB.
- L'API dati è disponibile per eseguire query su cluster a nodo singolo e a più nodi dei seguenti tipi di nodo:
  - dc2.large
  - dc2.8xlarge
  - ra3.xlplus
  - ra3.4xlarge
  - ra3.16xlarge
- Il cluster deve trovarsi in un Virtual Private Cloud (VPC) basato sul servizio Amazon VPC.
- Per impostazione predefinita, gli utenti con ruolo IAM o autorizzazioni IAM uguali all'utente che ha eseguito un'operazione API `ExecuteStatement` o `BatchExecuteStatement` possono agire sulla stessa istruzione con le operazioni API `CancelStatement`, `DescribeStatement`, `GetStatementResult` e `ListStatements`. Per agire sulla stessa istruzione SQL di un altro utente, l'utente deve essere in grado di assumere il ruolo IAM dell'utente che ha eseguito l'istruzione SQL. Per ulteriori informazioni su come assumere un ruolo, consulta [Autorizzazione di accesso all'API dati di Amazon Redshift](#).
- Le istruzioni SQL nel parametro `Sqls` dell'operazione API `BatchExecuteStatement` vengono eseguite come una singola transazione. Vengono eseguiti in serie nell'ordine dell'array. Le istruzioni SQL successive non vengono avviate fino al completamento dell'istruzione precedente nell'array. Se un'istruzione SQL ha esito negativo, dal momento che viene eseguita come un'unica transazione, viene eseguito il rollback di tutta l'operazione.
- Il tempo massimo di conservazione per un token client utilizzato nell'operazione API `ExecuteStatement` o `BatchExecuteStatement` è di 8 ore.
- Ogni API nell'API di dati Redshift ha una quota di transazioni al secondo prima della limitazione (della larghezza di banda della rete) delle richieste. Per la quota, consulta [Quote per l'API di dati Amazon Redshift](#). Se la frequenza della richiesta supera la quota, viene restituito `ThrottlingException` con codice di stato HTTP 400. Per rispondere alla limitazione (della larghezza di banda della rete), utilizza una strategia di ripetizione dei tentativi, come descritto in [Retry behavior](#) nella Guida di riferimento di AWS SDK e strumenti. Questa strategia viene implementata automaticamente per correggere gli errori di limitazione in alcuni SDK. AWS

#### Note

Per impostazione predefinita AWS Step Functions, i nuovi tentativi non sono abilitati. Se devi chiamare un'API di dati Redshift in una macchina a stati Step Functions,

includi il parametro di idempotenza `ClientToken` nella chiamata API di dati Redshift. Il valore di `ClientToken` deve persistere tra un tentativo e l'altro. Nel frammento di esempio seguente di una richiesta all'API `ExecuteStatement`, l'espressione `States.ArrayGetItem(States.StringSplit($$.Execution.Id, ':'), 7)` utilizza una funzione intrinseca per estrarre la parte UUID di `$$.Execution.Id`, che è univoca per ogni esecuzione della macchina a stati. Per ulteriori informazioni, consulta [Intrinsic functions](#) nella Guida per sviluppatori di AWS Step Functions .

```
{
  "Database": "dev",
  "Sql": "select 1;",
  "ClusterIdentifier": "MyCluster",
  "ClientToken.$": "States.ArrayGetItem(States.StringSplit($$.Execution.Id,
  ':'), 7)"
}
```

## Scelta delle credenziali di autenticazione del database quando si richiama l'API dati di Amazon Redshift

Quando si chiama l'API dati, è possibile utilizzare uno dei seguenti metodi di autenticazione per alcune operazioni API. Ogni metodo richiede una diversa combinazione di parametri.

### AWS Secrets Manager

Con questo metodo, fornisci un segreto memorizzato in AWS Secrets Manager cui ha `username` e `password`. `secret-arn` Il segreto specificato contiene le credenziali per la connessione al database specificato. Quando ci si connette a un cluster, si forniscono anche il nome del database; se si fornisce un identificatore del cluster (`dbClusterIdentifier`), questo deve corrispondere all'identificatore del cluster archiviato nel segreto. Quando ci si connette a un gruppo di lavoro serverless, si fornisce anche il nome del database. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali del database in AWS Secrets Manager](#).

### Credenziali temporanee

Con questo metodo, scegli una delle seguenti opzioni:

- Quando ti connetti a un gruppo di lavoro serverless, specifica il nome del gruppo di lavoro e del database. Il nome utente del database deriva dall'identità IAM. Ad esempio, `arn:iam::123456789012:user:foo` ha il nome utente di database

IAM:foo. Inoltre, è richiesta l'autorizzazione a richiamare l'operazione `redshift-serverless:GetCredentials`.

- Quando ti connetti a un cluster come identità IAM, specifica l'identificatore del cluster e il nome del database. Il nome utente del database deriva dall'identità IAM. Ad esempio, `arn:iam::123456789012:user:foo` ha il nome utente di database IAM:foo. Inoltre, è richiesta l'autorizzazione a richiamare l'operazione `redshift:GetClusterCredentialsWithIAM`.
- Quando ti connetti a un cluster come utente del database, specifica l'identificatore del cluster, il nome del database e il nome utente del database. Inoltre, è richiesta l'autorizzazione a richiamare l'operazione `redshift:GetClusterCredentials`. Per informazioni su come unirsi a gruppi di database durante la connessione con questo metodo, vedere [Unirsi a gruppi di database durante la connessione a un cluster](#).

Con questi metodi, puoi anche fornire un `region` valore che specifica Regione AWS dove si trovano i tuoi dati.

## Mappatura dei tipi di dati JDBC quando si chiama l'API dati di Amazon Redshift

La tabella seguente associa i tipi di dati Java Database Connectivity (JDBC) ai tipi di dati specificati nelle chiamate API dati.

Tipo di dati JDBC	Tipo di dati API dati
INTEGER, SMALLINT, BIGINT	LONG
FLOAT, REAL, DOUBLE	DOUBLE
DECIMAL	STRING
BOOLEAN, BIT	BOOLEAN
BLOB, BINARY, LONGVARBINARY	BLOB
VARBINARY	STRING
CLOB	STRING
Altri tipi (inclusi i tipi correlati a data e ora)	STRING

I valori stringa vengono passati al database Amazon Redshift e convertiti implicitamente in un tipo di dati del database.

### Note

Al momento, l'API dati non supporta array di identificatori univoci universali (UUID).

## Esecuzione di istruzioni SQL con parametri quando si chiama l'API dati di Amazon Redshift

È possibile controllare il testo SQL inviato al modulo di gestione di database chiamando l'operazione dell'API dati utilizzando i parametri per parti dell'istruzione SQL. I parametri specificati forniscono un modo flessibile per passare i parametri nel testo SQL senza codificarli. Aiutano a riutilizzare il testo SQL ed evitare problemi di SQL injection.

L'esempio seguente mostra i parametri denominati di un `parameters` campo di un `execute-statement` AWS CLI comando.

```
--parameters "[{"name": "id", "value": "1"}, {"name": "address", "value": "Seattle"}]"
```

Considerare le informazioni seguenti durante l'utilizzo dei parametri specificati:

- I parametri denominati possono essere utilizzati solo per sostituire i valori nelle istruzioni SQL.
- È possibile sostituire i valori in un'istruzione `INSERT`, ad esempio `INSERT INTO mytable VALUES (:val1)`.

I parametri specificati possono essere in qualsiasi ordine e possono essere utilizzati più di una volta nel testo SQL. Nell'opzione dei parametri mostrata nell'esempio precedente, i valori `1` e `Seattle` vengono inseriti nelle colonne della tabella `id` e `address`. Nel testo SQL, specificare i parametri denominati come segue:

```
--sql "insert into mytable values (:id, :address)"
```

- È possibile sostituire i valori in una clausola di condizioni, ad esempio `WHERE attr >= :val1`, `WHERE attr BETWEEN :val1 AND :val2` e `HAVING COUNT(attr) > :val`.
- Non è possibile sostituire i nomi delle colonne in un'istruzione SQL, ad esempio `SELECT column-name, ORDER BY column-name` o `GROUP BY column-name`.

Ad esempio, l'istruzione SELECT seguente restituisce un errore con sintassi non valida.

```
--sql "SELECT :colname, FROM event" --parameters "[{"name": "colname", "value": "eventname"}]"
```

Se si descrive (operazione `describe-statement`) l'istruzione con l'errore di sintassi, il valore `QueryString` restituito non sostituisce il nome della colonna per il parametro ("`QueryString`": "SELECT :colname, FROM event") e viene segnalato un errore (ERROR: syntax error at or near "FROM"\n Position: 12).

- Non è possibile sostituire i nomi delle colonne in una funzione aggregata, ad esempio `COUNT(column-name)`, `AVG(column-name)` o `SUM(column-name)`.
- Non è possibile sostituire i nomi delle colonne in una clausola `JOIN`.
- Quando viene eseguito l'SQL, i dati vengono trasformati implicitamente in un tipo di dati. Per ulteriori informazioni sul casting del tipo di dati, consultare [Tipi di dati](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Non è possibile impostare un valore su `NULL`. L'API dati interpreta questo valore come la stringa letterale `NULL`. Nell'esempio seguente `id` viene sostituito con la stringa letterale `null`. Non il valore SQL `NULL`.

```
--parameters [{"name": "id", "value": "null"}]"
```

- Non è possibile impostare un valore con lunghezza zero. L'istruzione SQL dell'API dati non riesce. Nell'esempio seguente si prova a impostare `id` con un valore di lunghezza zero e ciò si traduce in un errore dell'istruzione SQL.

```
--parameters [{"name": "id", "value": ""}]"
```

- Non è possibile impostare un nome di tabella nell'istruzione SQL con un parametro. L'API dati segue la regola di `PreparedStatement JDBC`.
- L'output dell'operazione `describe-statement` restituisce i parametri di query di un'istruzione SQL.
- Solo l'operazione `execute-statement` supporta le istruzioni SQL con parametri.

## Esecuzione di istruzioni SQL con un token di idempotenza quando si chiama l'API dati di Amazon Redshift

Quando si effettua una richiesta API mutante, di solito restituisce un risultato prima del completamento dei flussi di lavoro asincroni dell'operazione. Le operazioni potrebbero inoltre scadere o riscontrare altri problemi relativi al server prima del completamento, anche se la richiesta ha già restituito un risultato. Ciò potrebbe rendere difficile determinare l'esito della richiesta e potrebbe comportare più tentativi per garantire che l'operazione venga completata correttamente. Tuttavia, se la richiesta originale e i tentativi successivi hanno esito positivo, l'operazione viene completata più volte, il che significa che potresti aggiornare più risorse del previsto.

L'idempotenza assicura che una richiesta API venga completata solo una volta. Quando si utilizza una richiesta idempotente, se la richiesta originale viene completata correttamente, tutti i tentativi successivi vengono completati correttamente senza alcuna azione aggiuntiva. Le operazioni delle API dei dati `ExecuteStatement` e `BatchExecuteStatement` hanno un parametro idempotente `ClientToken` opzionale. Il `ClientToken` scade dopo 8 ore.

### Important

Se chiami `ExecuteStatement` e esegui `BatchExecuteStatement` operazioni da un AWS SDK, questo genera automaticamente un token client da utilizzare in caso di nuovo tentativo. In questo caso, non è consigliabile utilizzare il parametro `client-token` con le operazioni `ExecuteStatement` e `BatchExecuteStatement`. Visualizza il CloudTrail registro per vedere il `ClientToken`. Per un esempio di CloudTrail registro, vedere [Esempi per l'API di dati di Amazon Redshift](#).

Il `execute-statement` AWS CLI comando seguente illustra il `client-token` parametro opzionale per l'idempotenza.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
  --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

La tabella seguente mostra alcune risposte comuni che si potrebbero ricevere per richieste API idempotenti e fornisce consigli per effettuare nuovi tentativi.

Risposta	Raccomandazione	Commenti
200 (OK)	Non riprovare	La richiesta originale è stata completata con successo. Qualsiasi tentativo successivo ottiene esito positivo.
Codici di risposta serie 400	Non riprovare	<p>La richiesta presenta uno dei problemi seguenti:</p> <ul style="list-style-type: none"> <li>• Include un parametro o una combinazione di parametri non validi.</li> <li>• Utilizza un'azione o una risorsa per la quale non si dispone delle autorizzazioni.</li> <li>• Utilizza una risorsa che sta cambiando stato.</li> </ul> <p>Se la richiesta riguarda una risorsa che sta cambiando stato, un nuovo tentativo potrebbe avere esito positivo.</p>
Codici di risposta serie 500	Riprova	L'errore è causato da un problema AWS sul lato server ed è generalmente temporaneo. Ripeti la richiesta con una strategia di backoff appropriata.

Per ulteriori informazioni sui codici di risposta di Amazon Redshift, consulta [Errori comuni](#) nella Documentazione di riferimento dell'API Amazon Redshift.

## Autorizzazione di accesso all'API dati di Amazon Redshift

Per accedere all'API dati, un utente deve essere autorizzato. È possibile consentire a un utente di accedere all'API dati aggiungendo una policy gestita, che è una policy AWS Identity and Access Management (IAM) predefinita, a tale utente. Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#). Per

visualizzare le autorizzazioni consentite e negate dalle policy gestite, consultare la console IAM (<https://console.aws.amazon.com/iam/>).

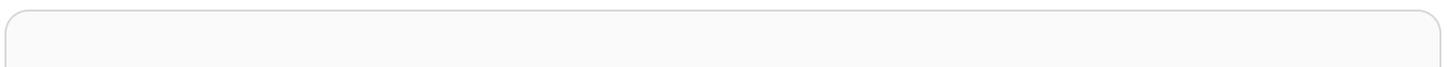
Amazon Redshift fornisce la policy gestita `AmazonRedshiftDataFullAccess`. Questa policy fornisce accesso completo alle operazioni API dati di Amazon Redshift. Questa policy consente inoltre l'accesso mirato a specifiche operazioni di Amazon Redshift AWS Secrets Manager e API IAM necessarie per autenticare e accedere a un cluster Amazon Redshift o a un gruppo di lavoro Serverless Redshift.

È possibile anche creare una policy IAM personalizzata che consente l'accesso a risorse specifiche. Per creare la policy, utilizzare la policy `AmazonRedshiftDataFullAccess` come modello di partenza. Dopo aver creato la policy, aggiungerla a ciascun utente che richiede l'accesso all'API dati.

Considera i seguenti requisiti della policy IAM associata all'utente:

- Se utilizzi l'autenticazione, conferma che la policy AWS Secrets Manager consenta l'utilizzo dell'operazione `secretsmanager:GetSecretValue` per recuperare il segreto etichettato con la chiave `RedshiftDataFullAccess`
- Se per l'autenticazione in un cluster vengono utilizzate credenziali temporanee, confermare che la policy consenta l'uso dell'operazione `redshift:GetClusterCredentials` al nome utente del database `redshift_data_api_user` per qualsiasi database nel cluster. Questo nome utente deve essere già stato creato nel database.
- Se utilizzi credenziali temporanee per eseguire l'autenticazione in un gruppo di lavoro serverless, verifica che la policy consenta l'uso dell'operazione `redshift-serverless:GetCredentials` per richiamare il gruppo di lavoro taggato con la chiave `RedshiftDataFullAccess`. L'utente del database viene mappato 1:1 all'identità di origine AWS Identity and Access Management (IAM). Ad esempio, l'utente `sample_user` è mappato all'utente del database IAM: `sample_user` e il ruolo IAM `sample_role` è mappato a IAMR: `sample_role`. Per ulteriori informazioni sulle diverse identità IAM, consulta [Identità IAM \(utenti, gruppi di utenti e ruoli\)](#) nella Guida per l'utente IAM.

Per eseguire una query su un cluster di proprietà di un altro account, l'account proprietario deve fornire un ruolo IAM che l'API dati può assumere nell'account chiamante. Si supponga, ad esempio, che l'Account B sia proprietario di un cluster a cui l'Account A deve accedere. L'account B può allegare la policy AWS-managed `AmazonRedshiftDataFullAccess` al ruolo IAM dell'account B. Quindi l'Account B considera attendibile l'Account A utilizzando una policy di attendibilità come la seguente:



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Infine, il ruolo IAM dell'Account A deve essere in grado di assumere il ruolo IAM dell'Account B.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

I seguenti link forniscono ulteriori informazioni sulla AWS Identity and Access Management IAM User Guide.

- Per ulteriori informazioni sulla creazione dei ruoli IAM, consultare [Creazione di ruoli IAM](#).
- Per informazioni sulla creazione di una policy IAM, consultare [Creazione di policy IAM](#).
- Per informazioni sull'aggiunta di una policy IAM a un utente, consultare [Aggiunta e rimozione di autorizzazioni per identità IAM](#).

## Memorizzazione delle credenziali del database in AWS Secrets Manager

Quando si richiama l'API dati, è possibile passare le credenziali per il cluster o il gruppo di lavoro serverless utilizzando un segreto in AWS Secrets Manager. Per utilizzare questo metodo per passare le credenziali, specifica il nome del segreto o l'Amazon Resource Name (ARN) del segreto.

Per archiviare le credenziali con Secrets Manager, è necessaria l'autorizzazione per la policy gestita da `SecretManagerReadWrite`. Per ulteriori informazioni sulle autorizzazioni minime, vedere [Creating and Managing Secrets with AWS Secrets Manager](#) nella Guida per l'AWS Secrets Manager utente.

Come archiviare le credenziali in un segreto per un cluster Amazon Redshift

1. Usa la AWS Secrets Manager console per creare un segreto che contenga le credenziali per il tuo cluster:
  - Quando si sceglie Archivia un nuovo segreto, selezionare Credenziali per il cluster Redshift.
  - Archiviare i valori per Nome utente (utente del database), Password e Cluster database(identificatore del cluster) nel segreto.
  - Taggare il segreto con la chiave `RedshiftDataFullAccess`. La policy gestita da `AWSAmazonRedshiftDataFullAccess` consente solo l'operazione `secretsmanager:GetSecretValue` per i segreti taggati con la chiave `RedshiftDataFullAccess`.

Per le istruzioni, consultare [Creazione di un segreto di base](#) nella Guida per l'utente di AWS Secrets Manager .

2. Usa la AWS Secrets Manager console per visualizzare i dettagli del segreto che hai creato o esegui il `aws secretsmanager describe-secret` AWS CLI comando.

Prendere nota del nome e dell'ARN del segreto, Possono essere utilizzati nelle chiamate all'API dati.

Archiviazione delle credenziali in un segreto per un gruppo di lavoro serverless

1. Usa AWS Secrets Manager AWS CLI i comandi per archiviare un segreto che contiene le credenziali per il tuo gruppo di lavoro serverless:
  - Crea il tuo segreto in un file, ad esempio un file JSON denominato `mycreds.json`. Fornire i i valori per User name (Nome utente) (utente del database) e Password nel file.

```
{
  "username": "myusername",
  "password": "mypassword"
```

```
}
```

- Memorizzare i valori nel segreto e taggare il segreto con la chiave `RedshiftDataFullAccess`.

```
aws secretsmanager create-secret --name MyRedshiftSecret --tags
  Key="RedshiftDataFullAccess",Value="serverless" --secret-string file://
mycreds.json
```

Di seguito è riportato l'output.

```
{
  "ARN":
  "arn:aws:secretsmanager:region:accountId:secret:MyRedshiftSecret-mvLHxf",
  "Name": "MyRedshiftSecret",
  "VersionId": "a1603925-e8ea-4739-9ae9-e509eEXAMPLE"
}
```

Per ulteriori informazioni, consulta l'argomento relativo alla [creazione di un segreto di base con AWS CLI](#) nella Guida per l'utente di AWS Secrets Manager .

2. Usa la AWS Secrets Manager console per visualizzare i dettagli del segreto che hai creato o esegui il comando. `aws secretsmanager describe-secret` AWS CLI

Prendere nota del nome e dell'ARN del segreto, Possono essere utilizzati nelle chiamate all'API dati.

## Creazione di un endpoint Amazon VPC (AWS PrivateLink) per l'API dati

Amazon Virtual Private Cloud (Amazon VPC) consente di lanciare AWS risorse, come cluster e applicazioni Amazon Redshift, in un cloud privato virtuale (VPC). AWS PrivateLink fornisce connettività privata tra cloud privati virtuali (VPC) e AWS servizi in modo sicuro sulla rete Amazon. Utilizzando AWS PrivateLink, è possibile creare endpoint VPC che consentono di connettersi a servizi su account e VPC diversi basati su Amazon VPC. Per ulteriori informazioni AWS PrivateLink, consulta [VPC Endpoint Services \(AWS PrivateLink\)](#) nella Amazon Virtual Private Cloud User Guide.

Puoi chiamare l'API dati con gli endpoint Amazon VPC. L'uso di un endpoint Amazon VPC mantiene il traffico tra le applicazioni in Amazon VPC e l'API Data nella AWS rete, senza utilizzare indirizzi IP pubblici. Gli endpoint Amazon VPC consentono di soddisfare i requisiti di conformità e normativi

relativi alla limitazione della connettività Internet. Ad esempio, se utilizzi un endpoint Amazon VPC, puoi mantenere il traffico tra un'applicazione in esecuzione su un'istanza Amazon EC2 e l'API dati nei VPC che li contengono.

Dopo aver creato l'endpoint Amazon VPC, puoi iniziare a utilizzarlo senza apportare modifiche al codice o alla configurazione nell'applicazione.

Per creare un endpoint Amazon VPC per l'API dati

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. Scegliere Endpoint, quindi Create Endpoint (Crea endpoint).
3. Nella pagina Crea endpoint, per Categoria di servizio, seleziona Servizi AWS . Per Nome servizio, scegliere redshift-data (com.amazonaws.*region*.redshift-data).
4. Per VPC, scegliere il VPC in cui creare l'endpoint.

Scegliere il VPC che contiene l'applicazione che effettua chiamate API dati.

5. Per le sottoreti, scegli la sottorete per ogni zona di disponibilità (AZ) utilizzata dal AWS servizio che esegue l'applicazione.

Per creare un endpoint Amazon VPC, specificare l'intervallo di indirizzi IP privati in cui l'endpoint sarà accessibile. A tale scopo, scegliere la sottorete per ogni zona di disponibilità. Questo ha l'effetto di limitare l'endpoint VPC all'intervallo di indirizzi IP privati specifico per ciascuna zona di disponibilità e crea inoltre un endpoint Amazon VPC in ogni zona di disponibilità.

6. Per Enable DNS Name (Abilita nome DNS), seleziona Enable for this endpoint (Abilita per questo endpoint).

Il DNS privato risolve il nome host DNS dell'API dati standard ([https://redshift-data.\*region\*.amazonaws.com](https://redshift-data.<i>region</i>.amazonaws.com)) negli indirizzi IP privati associati al nome host DNS specifico dell'endpoint Amazon VPC. Di conseguenza, puoi accedere all'endpoint VPC Data API utilizzando AWS CLI o AWS SDK senza apportare modifiche al codice o alla configurazione per aggiornare l'URL dell'endpoint Data API.

7. Per Security group (Gruppo di sicurezza), scegli un gruppo di sicurezza da associare all'endpoint Amazon VPC.

Scegli il gruppo di sicurezza che consente l'accesso al AWS servizio su cui è in esecuzione l'applicazione. Ad esempio, se un'istanza Amazon EC2 esegue l'applicazione, scegli il gruppo

di sicurezza che consente l'accesso all'istanza Amazon EC2. Il gruppo di sicurezza consente di controllare il traffico verso l'endpoint Amazon VPC dalle risorse del VPC.

## 8. Seleziona Crea endpoint.

Dopo aver creato l'endpoint, scegli il link in AWS Management Console per visualizzare i dettagli dell'endpoint.

La scheda Details (Dettagli) dell'endpoint mostra i nomi host DNS generati durante la creazione dell'endpoint Amazon VPC.

È possibile utilizzare l'endpoint standard (`redshift-data.region.amazonaws.com`) o uno degli endpoint specifici di VPC per chiamare l'API dati all'interno di Amazon VPC. L'endpoint API dati standard esegue automaticamente l'instradamento all'endpoint Amazon VPC. Questo routing si verifica perché il nome host DNS privato è stato abilitato al momento della creazione dell'endpoint Amazon VPC.

Quando utilizzi un endpoint Amazon VPC in una chiamata API dati, tutto il traffico tra l'applicazione e l'API dati rimane nei Amazon VPC che li contengono. Puoi utilizzare un endpoint Amazon VPC per qualsiasi tipo di chiamata API dati. Per informazioni sulla chiamata dell'API dati, consultare [Considerazioni da fare durante la chiamata all'API dati di Amazon Redshift](#).

## Unirsi a gruppi di database durante la connessione a un cluster

I gruppi di database sono raccolte di utenti del database. I privilegi del database possono essere concessi ai gruppi. Un amministratore può configurare un ruolo IAM in modo che questi gruppi di database vengano presi in considerazione quando SQL viene eseguito con l'API Data. Per ulteriori informazioni sui gruppi di database, consultare [Gruppi](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Puoi configurare il ruolo IAM di un chiamante dell'API Data in modo che l'utente del database specificato nella chiamata si unisca ai gruppi del database quando l'API dei dati si connette a un cluster. Questa funzionalità è supportata solo quando ci si connette a cluster forniti. Non è supportato durante la connessione a gruppi di lavoro Redshift Serverless. Il ruolo IAM del chiamante dell'API Data deve inoltre consentire l'azione `redshift:JoinGroup`.

Configuralo aggiungendo tag ai ruoli IAM. L'amministratore del ruolo IAM del chiamante aggiunge i tag con la chiave `RedshiftDbGroups` e un valore chiave di un elenco di gruppi di database. Il valore è un elenco di nomi separati da due punti (:) di gruppi di database fino a una lunghezza totale

di 256 caratteri. I gruppi di database devono essere precedentemente definiti nel database connesso. Se un gruppo specificato non viene trovato nel database, viene ignorato. Ad esempio, per i gruppi di database `accounting` e `retail`, il valore-chiave è `accounting:retail`. La coppia chiave-valore del tag `{"Key": "RedshiftDbGroups", "Value": "accounting:retail"}` viene utilizzato dall'API Data per determinare quali gruppi di database sono associati all'utente del database fornito nella chiamata alla Data API.

Per aggiungere gruppi di database come tag a un ruolo IAM

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 riquadro di navigazione della console, scegliere Roles (Ruoli) e selezionare il nome del ruolo che si desidera modificare.
3. Scegliere la scheda Tag, quindi scegliere Gestisci tag.
4. Scegli Aggiungi tag, quindi aggiungi la chiave `RedshiftDbGroups` e un valore che è un elenco di *database-groups-colon-separated*.
5. Seleziona Salvataggio delle modifiche.

Ora, quando un principal IAM (con questo ruolo IAM associato) chiama l'API dei dati, l'utente del database specificato si unisce ai gruppi di database specificati nel ruolo IAM.

Per ulteriori informazioni su come collegare un tag a un principale, inclusi i ruoli e gli utenti IAM, consultare [Assegnazione di tag di risorse IAM](#) nella Guida per l'utente di IAM.

## Chiamata dell'API dati

Puoi chiamare l'API Data o eseguire istruzioni SQL sul tuo cluster o AWS CLI gruppo di lavoro serverless. Le operazioni principali per eseguire le istruzioni SQL sono [ExecuteStatement](#) e [BatchExecuteStatement](#) nel Riferimento all'API dati di Amazon Redshift. L'API Data supporta i linguaggi di programmazione supportati dall' AWS SDK. Per ulteriori informazioni, consultare [Strumenti per creare in AWS](#).

Per vedere esempi di codice di chiamata all'API Data, consulta [Getting Started with Redshift Data API](#) in GitHub. Questo repository contiene esempi di utilizzo AWS Lambda per accedere ai dati di Amazon Redshift da Amazon EC2 e Amazon Runtime AWS Glue Data Catalog. SageMaker Esempi di linguaggi di programmazione includono Python, Go, Java e Javascript.

Puoi chiamare l'API dati utilizzando AWS CLI.

Gli esempi seguenti utilizzano AWS CLI per chiamare l'API Data. Per eseguire gli esempi, modificare i valori dei parametri in modo che corrispondano all'ambiente in uso. In molti esempi viene fornito un `cluster-identifier` per l'esecuzione in un cluster. Quando l'esecuzione avviene in un gruppo di lavoro serverless, viene fornito invece un `workgroup-name`. In questi esempi sono illustrate alcune delle operazioni dell'API dati. Per ulteriori informazioni, consultare la sezione relativa alle informazioni di riferimento ai comandi della AWS CLI .

I comandi nei seguenti esempi sono stati divisi e formattati per una maggiore leggibilità.

## Come eseguire un'istruzione SQL

Per eseguire un'istruzione SQL, utilizzare il `aws redshift-data execute-statement` AWS CLI comando.

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster e restituisce un identificatore per recuperare i risultati. In questo esempio viene utilizzato il AWS Secrets Manager metodo di autenticazione.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-hKgPwn"
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster e restituisce un identificatore per recuperare i risultati. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data execute-statement
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --sql "select * from stl_query limit 1"
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un gruppo di lavoro senza server e restituisce un identificatore per recuperare i risultati. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data execute-statement
  --database dev
  --workgroup-name myworkgroup
  --sql "select 1;"
```

Di seguito è riportato un esempio della risposta.

```
{
  "CreatedAt": "2022-02-11T06:25:28.748000+00:00",
  "Database": "dev",
  "DbUser": "IAMR:RoleName",
  "Id": "89dd91f5-2d43-43d3-8461-f33aa093c41e",
  "WorkgroupName": "myworkgroup"
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster e restituisce un identificatore per recuperare i risultati. Questo esempio utilizza il metodo di AWS Secrets Manager autenticazione e un token di idempotenza.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "select * from stl_query limit 1"
  --database dev
  --client-token b855dced-259b-444c-bc7b-d3e8e33f94g1
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-hKgPwn"
}
```

## Come eseguire un'istruzione SQL con parametri

Per eseguire un'istruzione SQL, utilizzare il comando `aws redshift-data execute-statement` AWS CLI

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster e restituisce un identificatore per recuperare i risultati. Questo esempio utilizza il AWS Secrets Manager metodo di autenticazione. Il testo SQL ha un parametro denominato `distance`. In questo caso, la distanza utilizzata nel predicato è 5. In un'istruzione `SELECT`, i parametri denominati per i nomi delle colonne possono essere utilizzati solo nel predicato. I valori per i parametri specificati per l'istruzione SQL vengono specificati nell'opzione `parameters`.

```
aws redshift-data execute-statement
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --sql "SELECT ratecode FROM demo_table WHERE trip_distance > :distance"
  --parameters "[{\"name\": \"distance\", \"value\": \"5\"}]"
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598323175.823,
  "Database": "dev",
  "Id": "c016234e-5c6c-4bc5-bb16-2c5b8ff61814",
  "SecretArn": "arn:aws:secretsmanager:us-west-2:123456789012:secret:yanruiz-secret-
hKgPwn"
}
```

La query seguente utilizza la tabella EVENT dal database di esempio. Per ulteriori informazioni, consultare [Tabella EVENT](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Se non si dispone già della tabella EVENT nel database, è possibile crearne una utilizzando l'API dati come segue:

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "create table event( eventid integer not null distkey,
                           venueid smallint not null,
                           catid smallint not null,
                           dateid smallint not null sortkey,
                           eventname varchar(200),
                           starttime timestamp)"
```

Il comando seguente inserisce una riga nella tabella EVENT.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event
values(:eventid, :venueid::smallint, :catid, :dateid, :eventname, :starttime)"
--parameters "[{"name": "eventid", "value": "1"}, {"name": "venueid",
"value": "1"},
{"name": "catid", "value": "1"},
{"name": "dateid", "value": "1"}]
```

```
{\"name\": \"eventname\", \"value\": \"event 1\"},
{\"name\": \"starttime\", \"value\": \"2022-02-22\"}]"
```

Il comando seguente inserisce una seconda riga nella tabella EVENT. Questo esempio esegue le operazioni seguenti:

- Il parametro denominato `id` viene utilizzato quattro volte nel testo SQL.
- Il tipo di conversione implicita viene applicato automaticamente quando si inserisce il parametro `starttime`.
- La colonna `venueid` è tipo `cast` per il tipo di dati `SMALLINT`.
- Le stringhe di caratteri che rappresentano il tipo di dati `DATE` vengono convertite implicitamente nel tipo di dati `TIMESTAMP`.
- All'interno del testo SQL è possibile utilizzare i commenti.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "insert into event values(:id, :id::smallint, :id, :id, :eventname, :starttime) /
*this is comment, and it won't apply parameterization for :id, :eventname or :starttime
here*/"
--parameters "[{\"name\": \"eventname\", \"value\": \"event 2\"},
                {\"name\": \"starttime\", \"value\": \"2022-02-22\"},
                {\"name\": \"id\", \"value\": \"2\"}]"
```

Di seguito sono riportate le due righe inserite:

eventid	venueid	catid	dateid	eventname	starttime
1	1	1	1	event 1	2022-02-22 00:00:00
2	2	2	2	event 2	2022-02-22 00:00:00

Il comando seguente utilizza un parametro denominato in una clausola `WHERE` per recuperare la riga in cui `eventid` è 1.

```
aws redshift-data execute-statement
--database dev
--cluster-id my-test-cluster
--db-user awsuser
--sql "select * from event where eventid=:id"
--parameters "[{"name": "id", "value": "1"}]"
```

Eseguire il comando seguente per ottenere i risultati SQL dell'istruzione SQL precedente:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Vengono restituiti i risultati seguenti:

```
{
  "Records": [
    [
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "longValue": 1
      },
      {
        "stringValue": "event 1"
      },
      {
        "stringValue": "2022-02-22 00:00:00.0"
      }
    ]
  ],
  "ColumnMetadata": [
    {
```

```
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "eventid",
    "length": 0,
    "name": "eventid",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "venueid",
    "length": 0,
    "name": "venueid",
    "nullable": 0,
    "precision": 5,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int2"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "catid",
    "length": 0,
    "name": "catid",
    "nullable": 0,
    "precision": 5,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int2"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
```

```
    "isSigned": true,
    "label": "dateid",
    "length": 0,
    "name": "dateid",
    "nullable": 0,
    "precision": 5,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "int2"
  },
  {
    "isCaseSensitive": true,
    "isCurrency": false,
    "isSigned": false,
    "label": "eventname",
    "length": 0,
    "name": "eventname",
    "nullable": 1,
    "precision": 200,
    "scale": 0,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "varchar"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "label": "starttime",
    "length": 0,
    "name": "starttime",
    "nullable": 1,
    "precision": 29,
    "scale": 6,
    "schemaName": "public",
    "tableName": "event",
    "typeName": "timestamp"
  }
],
"TotalNumRows": 1
}
```

## Come eseguire più istruzioni SQL

Per eseguire più istruzioni SQL con un solo comando, utilizzare il `aws redshift-data batch-execute-statement` AWS CLI comando.

Il AWS CLI comando seguente esegue tre istruzioni SQL su un cluster e restituisce un identificatore per recuperare i risultati. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data batch-execute-statement
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
  --sqls "set timezone to BST" "select * from mytable" "select * from another_table"
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

## Come elencare i metadati sulle istruzioni SQL

Per elencare i metadati relativi alle istruzioni SQL, utilizzate il comando `aws redshift-data list-statements` AWS CLI. L'autorizzazione per eseguire questo comando si basa sulle autorizzazioni IAM del chiamante.

Il AWS CLI comando seguente elenca le istruzioni SQL eseguite.

```
aws redshift-data list-statements
  --region us-west-2
  --status ALL
```

Di seguito è riportato un esempio della risposta.

```
{
  "Statements": [
    {
      "CreatedAt": 1598306924.632,
      "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
      "QueryString": "select * from stl_query limit 1",
      "Status": "FINISHED",
      "UpdatedAt": 1598306926.667
    },
    {
      "CreatedAt": 1598311717.437,
      "Id": "e0ebd578-58b3-46cc-8e52-8163fd7e01aa",
      "QueryString": "select * from stl_query limit 1",
      "Status": "FAILED",
      "UpdatedAt": 1598311719.008
    },
    {
      "CreatedAt": 1598313683.65,
      "Id": "c361d4f7-8c53-4343-8c45-6b2b1166330c",
      "QueryString": "select * from stl_query limit 1",
      "Status": "ABORTED",
      "UpdatedAt": 1598313685.495
    },
    {
      "CreatedAt": 1598306653.333,
      "Id": "a512b7bd-98c7-45d5-985b-a715f3cfde7f",
      "QueryString": "select 1",
      "Status": "FINISHED",
      "UpdatedAt": 1598306653.992
    }
  ]
}
```

## Come descrivere i metadati relativi a un'istruzione SQL

Per ottenere le descrizioni dei metadati per un'istruzione SQL, utilizzate il `aws redshift-data describe-statement` AWS CLI comando. L'autorizzazione per eseguire questo comando si basa sulle autorizzazioni IAM del chiamante.

Il AWS CLI comando seguente descrive un'istruzione SQL.

```
aws redshift-data describe-statement
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2
```

Di seguito è riportato un esempio della risposta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Duration": 1095981511,
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766",
  "QueryString": "select * from stl_query limit 1",
  "RedshiftPid": 20859,
  "RedshiftQueryId": 48879,
  "ResultRows": 1,
  "ResultSize": 4489,
  "Status": "FINISHED",
  "UpdatedAt": 1598306926.667
}
```

Di seguito è riportato un esempio di una risposta `describe-statement` dopo aver eseguito un comando `batch-execute-statement` con più istruzioni SQL.

```
{
  "ClusterIdentifier": "mayo",
  "CreatedAt": 1623979777.126,
  "Duration": 6591877,
  "HasResultSet": true,
  "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652",
  "RedshiftPid": 31459,
  "RedshiftQueryId": 0,
  "ResultRows": 2,
  "ResultSize": 22,
  "Status": "FINISHED",
  "SubStatements": [
    {
      "CreatedAt": 1623979777.274,
      "Duration": 3396637,
      "HasResultSet": true,
      "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:1",
      "QueryString": "select 1;",
      "RedshiftQueryId": -1,
      "ResultRows": 1,
    }
  ]
}
```

```

    "ResultSize": 11,
    "Status": "FINISHED",
    "UpdatedAt": 1623979777.903
  },
  {
    "CreatedAt": 1623979777.274,
    "Duration": 3195240,
    "HasResultSet": true,
    "Id": "b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2",
    "QueryString": "select 2;",
    "RedshiftQueryId": -1,
    "ResultRows": 1,
    "ResultSize": 11,
    "Status": "FINISHED",
    "UpdatedAt": 1623979778.076
  }
],
"UpdatedAt": 1623979778.183
}

```

## Come recuperare i risultati di un'istruzione SQL

Per recuperare il risultato da un'istruzione SQL eseguita, utilizzate il `redshift-data get-statement-result` AWS CLI comando. È possibile fornire un `Id` che viene ricevuto nella risposta a `execute-statement` o `batch-execute-statement`. Il valore `Id` per un'istruzione SQL eseguita da `batch-execute-statement` può essere recuperato nel risultato di `describe-statement` ed ha un suffisso formato da due punti e un numero di sequenza, ad esempio `b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2`. Se con `batch-execute-statement` vengono eseguite più istruzioni SQL, ogni istruzione SQL avrà un valore `Id` come mostrato nell'output di `describe-statement`. L'autorizzazione per eseguire questo comando si basa sulle autorizzazioni IAM del chiamante.

L'istruzione seguente restituisce il risultato di un'istruzione SQL eseguita da `execute-statement`.

```

aws redshift-data get-statement-result
  --id d9b6c0c9-0747-4bf4-b142-e8883122f766
  --region us-west-2

```

L'istruzione seguente restituisce il risultato della seconda istruzione SQL eseguita da `batch-execute-statement`.

```
aws redshift-data get-statement-result
--id b2906c76-fa6e-4cdf-8c5f-4de1ff9b7652:2
--region us-west-2
```

Di seguito è riportato un esempio della risposta a una chiamata a `get-statement-result`.

```
{
  "ColumnMetadata": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": true,
      "label": "userid",
      "length": 0,
      "name": "userid",
      "nullable": 0,
      "precision": 10,
      "scale": 0,
      "schemaName": "",
      "tableName": "stll_query",
      "typeName": "int4"
    },
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": true,
      "label": "query",
      "length": 0,
      "name": "query",
      "nullable": 0,
      "precision": 10,
      "scale": 0,
      "schemaName": "",
      "tableName": "stll_query",
      "typeName": "int4"
    },
    {
      "isCaseSensitive": true,
      "isCurrency": false,
      "isSigned": false,
      "label": "label",
      "length": 0,
```

```
    "name": "label",
    "nullable": 0,
    "precision": 320,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "bpchar"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "xid",
    "length": 0,
    "name": "xid",
    "nullable": 0,
    "precision": 19,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int8"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "pid",
    "length": 0,
    "name": "pid",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": true,
    "isCurrency": false,
    "isSigned": false,
    "label": "database",
    "length": 0,
    "name": "database",
    "nullable": 0,
```

```
    "precision": 32,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "bpchar"
  },
  {
    "isCaseSensitive": true,
    "isCurrency": false,
    "isSigned": false,
    "label": "querytxt",
    "length": 0,
    "name": "querytxt",
    "nullable": 0,
    "precision": 4000,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "bpchar"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "label": "starttime",
    "length": 0,
    "name": "starttime",
    "nullable": 0,
    "precision": 29,
    "scale": 6,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "timestamp"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "label": "endtime",
    "length": 0,
    "name": "endtime",
    "nullable": 0,
    "precision": 29,
    "scale": 6,
```

```
    "schemaName": "",
    "tableName": "stll_query",
    "type": 93,
    "typeName": "timestamp"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "aborted",
    "length": 0,
    "name": "aborted",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "insert_pristine",
    "length": 0,
    "name": "insert_pristine",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
    "tableName": "stll_query",
    "typeName": "int4"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": true,
    "label": "concurrency_scaling_status",
    "length": 0,
    "name": "concurrency_scaling_status",
    "nullable": 0,
    "precision": 10,
    "scale": 0,
    "schemaName": "",
```

```
        "tableName": "st11_query",
        "typeName": "int4"
    }
],
"Records": [
    [
        {
            "longValue": 1
        },
        {
            "longValue": 3
        },
        {
            "stringValue": "health"
        },
        {
            "longValue": 1023
        },
        {
            "longValue": 15279
        },
        {
            "stringValue": "dev"
        },
        {
            "stringValue": "select system_status from stv_gui_status;"
        },
        {
            "stringValue": "2020-08-21 17:33:51.88712"
        },
        {
            "stringValue": "2020-08-21 17:33:52.974306"
        },
        {
            "longValue": 0
        },
        {
            "longValue": 0
        },
        {
            "longValue": 6
        }
    ]
],
```

```
"TotalNumRows": 1
}
```

## Come descrivere una tabella

Per ottenere i metadati che descrivono una tabella, utilizzate il `aws redshift-data describe-table` AWS CLI comando.

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster e restituisce i metadati che descrivono una tabella. In questo esempio viene utilizzato il metodo AWS Secrets Manager di autenticazione.

```
aws redshift-data describe-table
  --region us-west-2
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
  --table sql_features
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
```

Di seguito è riportato un esempio della risposta.

```
{
  "ColumnList": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": false,
      "length": 2147483647,
      "name": "feature_id",
      "nullable": 1,
      "precision": 2147483647,
      "scale": 0,
      "schemaName": "information_schema",
      "tableName": "sql_features",
      "typeName": "character_data"
    },
    {
      "isCaseSensitive": false,
      "isCurrency": false,
```

```
        "isSigned": false,  
        "length": 2147483647,  
        "name": "feature_name",  
        "nullable": 1,  
        "precision": 2147483647,  
        "scale": 0,  
        "schemaName": "information_schema",  
        "tableName": "sql_features",  
        "typeName": "character_data"  
    }  
]  
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster che descrive una tabella. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data describe-table  
  --region us-west-2  
  --db-user myuser  
  --cluster-identifier mycluster-test  
  --database dev  
  --schema information_schema  
  --table sql_features
```

Di seguito è riportato un esempio della risposta.

```
{  
  "ColumnList": [  
    {  
      "isCaseSensitive": false,  
      "isCurrency": false,  
      "isSigned": false,  
      "length": 2147483647,  
      "name": "feature_id",  
      "nullable": 1,  
      "precision": 2147483647,  
      "scale": 0,  
      "schemaName": "information_schema",  
      "tableName": "sql_features",  
      "typeName": "character_data"  
    },  
    {
```

```
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "feature_name",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "sub_feature_id",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "sub_feature_name",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "is_supported",
```

```
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "is_verified_by",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  },
  {
    "isCaseSensitive": false,
    "isCurrency": false,
    "isSigned": false,
    "length": 2147483647,
    "name": "comments",
    "nullable": 1,
    "precision": 2147483647,
    "scale": 0,
    "schemaName": "information_schema",
    "tableName": "sql_features",
    "typeName": "character_data"
  }
]
}
```

## Come elencare i database in un cluster

Per elencare i database in un cluster, utilizzare il `aws redshift-data list-databases` AWS CLI comando.

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare i database. Questo esempio utilizza il metodo AWS Secrets Manager di autenticazione.

```
aws redshift-data list-databases
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
  --cluster-identifier mycluster-test
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "Databases": [
    "dev"
  ]
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare i database. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data list-databases
  --region us-west-2
  --db-user myuser
  --cluster-identifier mycluster-test
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "Databases": [
    "dev"
  ]
}
```

## Come elencare gli schemi in un database

Per elencare gli schemi in un database, utilizzare il `aws redshift-data list-schemas` AWS CLI comando.

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare gli schemi in un database. Questo esempio utilizza il metodo di AWS Secrets Manager autenticazione.

```
aws redshift-data list-schemas
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPWn
  --cluster-identifier mycluster-test
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare gli schemi in un database. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data list-schemas
  --region us-west-2
  --db-user mysuser
  --cluster-identifier mycluster-test
  --database dev
```

Di seguito è riportato un esempio della risposta.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

## Come elencare le tabelle in un database

Per elencare le tabelle in un database, utilizzare il `aws redshift-data list-tables` AWS CLI comando.

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare le tabelle in un database. Questo esempio utilizza il metodo AWS Secrets Manager di autenticazione.

```
aws redshift-data list-tables
  --region us-west-2
  --secret arn:aws:secretsmanager:us-west-2:123456789012:secret:myuser-secret-hKgPwn
  --cluster-identifier mycluster-test
  --database dev
  --schema information_schema
```

Di seguito è riportato un esempio della risposta.

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

Il AWS CLI comando seguente esegue un'istruzione SQL su un cluster per elencare le tabelle in un database. In questo esempio viene utilizzato il metodo di autenticazione con le credenziali temporanee.

```
aws redshift-data list-tables
  --region us-west-2
  --db-user myuser
```

```
--cluster-identifier mycluster-test
--database dev
--schema information_schema
```

Di seguito è riportato un esempio della risposta.

```
{
  "Tables": [
    {
      "name": "sql_features",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    },
    {
      "name": "sql_implementation_info",
      "schema": "information_schema",
      "type": "SYSTEM TABLE"
    }
  ]
}
```

## Risoluzione dei problemi relativi all'API dati di Amazon Redshift

Utilizza le seguenti sezioni, intitolate con messaggi di errori comuni, per aiutare a risolvere i problemi con l'API dati.

### Argomenti

- [Il pacchetto per la query è troppo grande](#)
- [La risposta del database è andata oltre il limite delle dimensioni](#)

### Il pacchetto per la query è troppo grande

Se viene visualizzato un errore che indica che il pacchetto per una query è troppo grande, in genere il set di risultati restituito per una riga è troppo grande. Il limite delle dimensioni dell'API dati è 64 KB per riga nel set di risultati restituito dal database.

Per risolvere questo problema, verifica che ogni riga in un set di risultati sia corrispondente o inferiore a 64 KB.

## La risposta del database è andata oltre il limite delle dimensioni

Se viene visualizzato un errore che indica che la risposta del database ha superato il limite delle dimensioni, in genere le dimensioni del set di risultati restituito dal database erano troppo grandi. Il limite dell'API dati è 100 MB nel set di risultati restituito dal database.

Per risolvere questo problema, assicurarsi che le chiamate all'API dati restituiscano 100 MB di dati o meno. Se è necessario restituire più di 100 MB, è possibile eseguire più chiamate a istruzioni con la clausola LIMIT nella query.

## Pianificazione delle operazioni di Amazon Redshift Data API con Amazon EventBridge

È possibile creare regole corrispondenti agli eventi selezionati nel flusso e instradarle alle destinazioni per le operazioni. È possibile anche utilizzare le regole per eseguire operazioni in base a una pianificazione prestabilita. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).

Per pianificare le operazioni Data API con EventBridge, il ruolo IAM associato deve affidarsi al principal for CloudWatch Events (events.amazonaws.com). Questo ruolo deve avere l'equivalente della policy gestita AmazonEventBridgeFullAccess collegata. Dovrebbe inoltre disporre delle autorizzazioni della policy AmazonRedshiftDataFullAccess che sono gestite dall'API dati. È possibile creare un ruolo IAM con queste autorizzazioni nella console IAM. Quando crei un ruolo sulla console IAM, scegli l'entità affidabile del AWS servizio per gli eventi. CloudWatch Specificate il ruolo IAM nel valore RoleArn JSON nella EventBridge destinazione. Per ulteriori informazioni sulla creazione di un ruolo IAM, consulta [Creating a Role for an AWS Service \(Console\)](#) nella IAM User Guide.

La name regola che crei in Amazon EventBridge deve corrispondere StatementName a quella inRedshiftDataParameters.

Gli esempi seguenti mostrano le variazioni della creazione di EventBridge regole con una o più istruzioni SQL e con un cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift Serverless come data warehouse.

Richiamo con un'unica istruzione SQL e un unico cluster

L'esempio seguente utilizza AWS CLI per creare una EventBridge regola che viene utilizzata per eseguire un'istruzione SQL su un cluster Amazon Redshift.

```
aws events put-rule
```

```
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Quindi viene creato un EventBridge obiettivo da eseguire secondo la pianificazione specificata nella regola.

```
aws events put-targets
--cli-input-json file://data.json
```

Di seguito è riportato il file data.json di input. La chiave JSON `Sql` indica che esiste una singola istruzione SQL. Il valore JSON `Arn` contiene un identificatore del cluster. Il valore JSON `RoleArn` contiene il ruolo IAM utilizzato per eseguire l'istruzione SQL come descritto in precedenza.

```
{
  "Rule": "test-redshift-cluster-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "DbUser": "root",
        "Sql": "select 1;",
        "StatementName": "test-redshift-cluster-data",
        "WithEvent": true
      }
    }
  ]
}
```

Richiamo con un'unica istruzione SQL e un unico gruppo di lavoro

L'esempio seguente utilizza AWS CLI per creare una EventBridge regola che viene utilizzata per eseguire un'istruzione SQL su un gruppo di lavoro Amazon Redshift Serverless.

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Quindi viene creato un EventBridge obiettivo da eseguire secondo la pianificazione specificata nella regola.

```
aws events put-targets
--cli-input-json file://data.json
```

Di seguito è riportato il file data.json di input. La chiave JSON `Sql` indica che esiste una singola istruzione SQL. Il valore JSON `Arn` contiene un nome del gruppo di lavoro. Il valore JSON `RoleArn` contiene il ruolo IAM utilizzato per eseguire l'istruzione SQL come descritto in precedenza.

```
{
  "Rule": "test-redshift-serverless-workgroup-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sql": "select 1;",
        "StatementName": "test-redshift-serverless-workgroup-data",
        "WithEvent": true
      }
    }
  ]
}
```

Richiamo con più istruzioni SQL e cluster

L'esempio seguente utilizza AWS CLI per creare una EventBridge regola che viene utilizzata per eseguire più istruzioni SQL su un cluster Amazon Redshift.

```
aws events put-rule
--name test-redshift-cluster-data
--schedule-expression "rate(1 minute)"
```

Quindi viene creato un EventBridge obiettivo da eseguire secondo la pianificazione specificata nella regola.

```
aws events put-targets
--cli-input-json file://data.json
```

Di seguito è riportato il file `data.json` di input. La chiave `JSON Sqls` indica che esistono più istruzioni SQL. Il valore `JSON Arn` contiene un identificatore del cluster. Il valore `JSON RoleArn` contiene il ruolo IAM utilizzato per eseguire l'istruzione SQL come descritto in precedenza.

```
{
  "Rule": "test-redshift-cluster-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift:us-east-1:123456789012:cluster:mycluster",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sqls": ["select 1;", "select 2;", "select 3;"],
        "StatementName": "test-redshift-cluster-data",
        "WithEvent": true
      }
    }
  ]
}
```

### Richiamo con più istruzioni SQL e gruppi di lavoro

L'esempio seguente utilizza AWS CLI per creare una EventBridge regola che viene utilizzata per eseguire più istruzioni SQL su un gruppo di lavoro Amazon Redshift Serverless.

```
aws events put-rule
--name test-redshift-serverless-workgroup-data
--schedule-expression "rate(1 minute)"
```

Quindi viene creato un EventBridge obiettivo da eseguire secondo la pianificazione specificata nella regola.

```
aws events put-targets
--cli-input-json file://data.json
```

Di seguito è riportato il file data.json di input. La chiave JSON `SqLs` indica che esistono più istruzioni SQL. Il valore JSON `Arn` contiene un nome del gruppo di lavoro. Il valore JSON `RoleArn` contiene il ruolo IAM utilizzato per eseguire l'istruzione SQL come descritto in precedenza.

```
{
  "Rule": "test-redshift-serverless-workgroup-data",
  "EventBusName": "default",
  "Targets": [
    {
      "Id": "2",
      "Arn": "arn:aws:redshift-serverless:us-east-1:123456789012:workgroup/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RoleArn": "arn:aws:iam::123456789012:role/Administrator",
      "RedshiftDataParameters": {
        "Database": "dev",
        "Sqls": ["select 1;", "select 2;", "select 3;"],
        "StatementName": "test-redshift-serverless-workgroup-data",
        "WithEvent": true
      }
    }
  ]
}
```

## Monitoraggio dell'API dati

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni della Data API e delle altre AWS soluzioni. AWS fornisce i seguenti strumenti di monitoraggio per monitorare la Data API, segnalare quando qualcosa non va e intraprendere azioni automatiche se necessario:

- Amazon EventBridge può essere utilizzato per automatizzare i AWS servizi e rispondere automaticamente agli eventi di sistema, come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale. Puoi compilare regole semplici che indichino quali eventi sono considerati di interesse per te e quali operazioni automatizzate intraprendere quando un evento corrisponde a una regola. Per ulteriori informazioni, consulta la [Amazon EventBridge User Guide](#).
- AWS CloudTrail acquisisce le chiamate API e gli eventi correlati effettuati da o per conto del tuo AWS account e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni su come è integrato

Amazon Redshift AWS CloudTrail, consulta [Logging with CloudTrail](#). Per ulteriori informazioni su CloudTrail, consulta la Guida per l'[AWS CloudTrail utente](#).

## Argomenti

- [Eventi di monitoraggio per l'Amazon Redshift Data API in Amazon EventBridge](#)

## Eventi di monitoraggio per l'Amazon Redshift Data API in Amazon EventBridge

Puoi monitorare gli eventi dell'API Data in EventBridge, che fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni software-as-a-service (SaaS) e AWS servizi. EventBridge indirizza tali dati verso destinazioni come AWS Lambda Amazon SNS. Questi eventi sono gli stessi che compaiono in CloudWatch Events, che fornisce un flusso quasi in tempo reale di eventi di sistema che descrivono i cambiamenti nelle risorse. AWS Gli eventi vengono inviati all'account che contiene il database Amazon Redshift. Ad esempio, se si assume un ruolo in un altro account, gli eventi vengono inviati a tale account. Per ulteriori informazioni, consulta [EventBridge gli eventi Amazon](#) nella Amazon EventBridge User Guide. .

Gli eventi dell'API dati vengono inviati quando l'operazione dell'API dati `ExecuteStatement` o `BatchExecuteStatement` imposta l'opzione `WithEvent` su `true`. Il campo `state` dell'evento può contenere uno dei seguenti valori:

- **INTERROTTO**: l'esecuzione della query è stata interrotta dall'utente.
- **FAILED**: l'esecuzione della query non è riuscita.
- **FINISHED**: l'esecuzione della query è terminata.

Gli eventi vengono consegnati su base garantita. Per ulteriori informazioni, consulta [Events from AWS services](#) nella Amazon EventBridge User Guide.

### Esempio di l'evento terminato dell'API dati

L'esempio seguente mostra un evento per l'API dati quando l'operazione dell'API `ExecuteStatement` termina. Nell'esempio, un'istruzione denominata `test.testtable` ha completato l'esecuzione.

```
{
  "version": "0",
  "id": "18e7079c-dd4b-dd64-caf9-e2a31640dab0",
```

```
"detail-type": "Redshift Data Statement Status Change",
"source": "aws.redshift-data",
"account": "123456789012",
"time": "2020-10-01T21:14:26Z",
"region": "us-east-1",
"resources": [
  "arn:aws:redshift:us-east-1:123456789012:cluster:redshift-cluster-1"
],
"detail": {
  "principal": "arn:aws:iam::123456789012:user/myuser",
  "statementName": "test.testtable",
  "statementId": "dd2e1ec9-2ee3-49a0-819f-905fa7d75a4a",
  "redshiftQueryId": -1,
  "state": "FINISHED",
  "rows": 1,
  "expireAt": 1601673265
}
}
```

# Gruppi di parametri di Amazon Redshift.

## Panoramica

In Amazon Redshift, a ogni cluster creato è associato un gruppo di parametri. Un gruppo di parametri è un insieme di parametri che vengono applicati a tutti i database creati nel cluster. Questi parametri configurano le impostazioni dei database, come timeout di query e stile delle date.

## Informazioni sui gruppi di parametri

Ogni gruppo di parametri include vari parametri per configurare le impostazioni del database. L'elenco di parametri disponibili dipende dalla famiglia di gruppi di parametri a cui il gruppo di parametri appartiene. La famiglia di gruppi di parametri è la versione del motore Amazon Redshift a cui si applicano i parametri nel gruppo di parametri. Il formato del nome della famiglia di gruppi di parametri è `redshift-version` dove *version* è la versione del motore. Ad esempio, la versione corrente del motore è `redshift-1.0`.

Amazon Redshift fornisce un gruppo di parametri di default per ogni famiglia di gruppi di parametri. Il gruppo di parametri predefinito comporta valori preimpostati per ognuno dei parametri e non può essere modificato. Il formato del nome del gruppo di parametri predefinito è `default.parameter_group_family`, dove *parameter\_group\_family* è la versione del motore a cui il gruppo di parametri appartiene. Ad esempio, il gruppo di parametri predefinito per la versione `redshift-1.0` è denominato `default.redshift-1.0`.

### Note

Al momento, `redshift-1.0` è l'unica versione del motore Amazon Redshift. Di conseguenza, `default.redshift-1.0` è il solo gruppo di parametri predefinito.

Se intendi utilizzare valori di parametri differenti da quelli del gruppo di parametri predefinito, è necessario creare un gruppo di parametri personalizzato e associarlo al tuo cluster. Inizialmente, i valori dei parametri di un gruppo di parametri personalizzato sono identici a quelli del gruppo di parametri predefinito. L'`source` iniziale per tutti i parametri è `engine-default` perché i valori sono preimpostati da Amazon Redshift. Dopo la modifica di un valore di parametro, `source` diventa `user` a indicare che il valore è stato modificato rispetto al relativo valore predefinito.

**Note**

La console Amazon Redshift non visualizza l'`source` di ogni parametro. È necessario utilizzare l'API Amazon Redshift AWS CLI, il o uno degli AWS SDK per visualizzare il `source`.

Per i gruppi di parametri che crei, puoi modificare un valore di parametro in qualsiasi momento oppure ripristinare i valori predefiniti di tutti i parametri. Puoi inoltre associare un differente gruppo di parametri a un cluster. In alcuni casi, puoi modificare i valori dei parametri in un gruppo di parametri già associato al cluster o associare un gruppo di parametri diversi a un cluster. In questi casi, potrebbe essere necessario riavviare il cluster affinché i valori aggiornati dei parametri abbiano validità. Se il cluster riporta un errore e viene riavviato da Amazon Redshift, le modifiche vengono applicate in quel momento. Se il cluster viene riavviato durante la manutenzione, le modifiche non vengono applicate. Per ulteriori informazioni, consultare [Proprietà WLM dinamiche e statiche](#).

## Valori di parametro predefiniti

La tabella seguente mostra i valori di parametro predefiniti con collegamenti a informazioni più dettagliate su ogni parametro. Questi sono i valori predefiniti per la famiglia del gruppo di parametri `redshift-1.0`.

Nome del parametro	Valore	Ulteriori informazioni
<code>auto_analyze</code>	<code>true</code>	<a href="#">auto_analyze</a> nella Guida per gli sviluppatori di database di Amazon Redshift
<code>auto_mv</code>	<code>true</code>	<a href="#">Viste materializzate automatizzate</a> nella Guida per sviluppatori del database di Amazon Redshift
<code>datestyle</code>	<code>ISO, MDY</code>	<a href="#">datestyle</a> nella Guida per gli sviluppatori di database di Amazon Redshift
<code>enable_case_sensitive_identifier</code>	<code>false</code>	<a href="#">enable_case_sensitive_identifier</a> nella Guida per gli sviluppatori di database di Amazon Redshift

Nome del parametro	Valore	Ulteriori informazioni
enable_user_activity_logging	false	<a href="#">Logging di controllo dei database</a> in questa guida
extra_float_digits	0	<a href="#">extra_float_digits</a> nella Guida per gli sviluppatori di database di Amazon Redshift
max_concurrency_scaling_clusters	1	<a href="#">max_concurrency_scaling_clusters</a> nella Guida per gli sviluppatori di database di Amazon Redshift
query_group	default	<a href="#">query_group</a> nella Guida per gli sviluppatori di database di Amazon Redshift
require_ssl	false	<a href="#">Configurazione delle opzioni di sicurezza per le connessioni</a> in questa guida
search_path	\$user, public	<a href="#">search_path</a> nella Guida per gli sviluppatori di database di Amazon Redshift
statement_timeout	0	<a href="#">statement_timeout</a> nella Guida per gli sviluppatori di database di Amazon Redshift
wlm_json_configuration	[{"auto_wlm":true}]	<a href="#">Configurazione della gestione del carico di lavoro</a> in questa guida
use_fips_ssl	false	Abilita la modalità SSL conforme a FIPS solo se il sistema deve essere conforme a FIPS.

### Note

Il parametro `max_cursor_result_set_size` è obsoleto. Per ulteriori informazioni sulla dimensione del set di risultati del cursore, consultare [Vincoli del cursore](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Puoi ignorare temporaneamente un parametro utilizzando il comando SET nel database. Il comando SET ignora il parametro soltanto per la durata della sessione corrente. Oltre ai parametri elencati nella tabella precedente, puoi anche regolare temporaneamente il numero di slot impostando `wlm_query_slot_count` nel database. Il parametro `wlm_query_slot_count` non è disponibile per la configurazione nei gruppi di parametri. Per ulteriori informazioni sulla regolazione del numero di slot, consultare [wlm\\_query\\_slot\\_count](#) nella Guida per gli sviluppatori di database di Amazon Redshift. Per ulteriori informazioni su come ignorare temporaneamente gli altri parametri, consultare [Modifica della configurazione del server](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Configurazione dei valori dei parametri utilizzando il AWS CLI

Per configurare i parametri di Amazon Redshift utilizzando AWS CLI, si utilizza il `modify-cluster-parameter-group` comando per un gruppo di parametri specifico. Il gruppo di parametri da modificare deve essere specificato in `parameter-group-name`. Per specificare le coppie nome/valore di ogni parametro da modificare nel gruppo di parametri, è necessario utilizzare il parametro `parameters` (per il comando `modify-cluster-parameter-group`).

### Note

Esistono alcune considerazioni speciali in relazione alla configurazione del parametro `wlm_json_configuration` con l' AWS CLI. Gli esempi in questa sezione sono validi per tutti i parametri ad eccezione di `wlm_json_configuration`. Per ulteriori informazioni sulla configurazione `wlm_json_configuration` utilizzando il AWS CLI, consulta.

[Configurazione della gestione del carico di lavoro](#)

Dopo la modifica dei valori di parametro, è necessario riavviare gli eventuali cluster associati al gruppo di parametri modificato. Lo stato del cluster visualizza `applying` per `ParameterApplyStatus` durante l'applicazione dei valori, quindi `pending-reboot` dopo l'applicazione dei valori. Dopo il riavvio, i database nel cluster iniziano a utilizzare i nuovi valori di parametro. Per ulteriori informazioni sul riavvio di cluster, consultare [Riavvio di un cluster](#).

### Note

Il parametro `wlm_json_configuration` contiene alcune proprietà dinamiche che non richiedono il riavvio dei cluster associati affinché le modifiche siano applicate. Per ulteriori

informazioni sulle proprietà dinamiche e statiche, consultare [Proprietà WLM dinamiche e statiche](#).

## Sintassi

La sintassi seguente mostra come utilizzare il comando `modify-cluster-parameter-group` per configurare un parametro. Specifica *parameter\_group\_name* e sostituisci *parameter\_name* e *parameter\_value* con un parametro effettivo da modificare e un valore per quel parametro. Se intendi modificare più parametri contemporaneamente, separa ogni set di parametri e di valori da quello successivo con uno spazio.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name
--parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

## Esempio

L'esempio seguente mostra come configurare i parametri `statement_timeout` e `enable_user_activity_logging` per il gruppo di parametri `myclusterparametergroup`.

### Note

Per motivi di leggibilità, l'esempio viene visualizzato su più righe, ma in realtà si AWS CLI tratta di una sola riga.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
ParameterName=enable_user_activity_logging,ParameterValue=true
```

È possibile gestire i gruppi di parametri tramite la console. Per ulteriori informazioni, consultare [Gestione di gruppi di parametri mediante la console](#).

## Configurazione della gestione del carico di lavoro

In Amazon Redshift, viene utilizzata la gestione del carico di lavoro (WLM) per definire il numero di code di query disponibili e il modo in cui le query sono instradate a tali code per l'elaborazione.

WLM è parte della configurazione del gruppo di parametri. Un cluster utilizza la configurazione WLM specificata nel relativo gruppo di parametri associato.

Quando crei un gruppo di parametri, la configurazione WLM predefinita contiene una coda che può eseguire fino a cinque query contemporaneamente. Puoi aggiungere ulteriori code e configurare le proprietà WLM in ognuna se vuoi avere un maggiore controllo sull'elaborazione delle query. Ogni coda aggiunta ha la stessa configurazione WLM predefinita fino a che non ne configuri le proprietà.

Quando aggiungi ulteriori code, l'ultima nella configurazione è la code predefinita. A meno che una query non sia instradata a un'altra coda in base ai criteri nella configurazione WLM, viene elaborata dalla coda predefinita. È possibile specificare la modalità e il livello di simultaneità (slot di query) per la coda predefinita, ma non è possibile specificare i gruppi di utenti o i gruppi di query per la coda predefinita.

Come per gli altri parametri, non puoi modificare la configurazione WLM nel gruppo di parametri predefinito. I cluster associati al gruppo di parametri predefinito utilizzano sempre la configurazione WLM predefinita. Per modificare la configurazione WLM, crea un nuovo gruppo di parametri e quindi associa quel gruppo a un cluster che richiede la configurazione WLM personalizzata.

## Proprietà WLM dinamiche e statiche

Le proprietà della configurazione WLM sono dinamiche o statiche. Puoi applicare proprietà dinamiche al database senza riavviare il cluster, ma le proprietà statiche richiedono un riavvio del cluster affinché le modifiche abbiano effetto. Per ulteriori informazioni sulle proprietà statiche e dinamiche, consultare [Proprietà WLM dinamiche e statiche](#).

## Proprietà del parametro `wlm_json_configuration`

Puoi configurare WLM utilizzando la console Amazon Redshift, AWS CLI l'API Amazon Redshift o uno degli SDK. AWS La configurazione WLM utilizza varie proprietà per definire il comportamento delle code, come l'allocazione di memoria tra le code, il numero di query eseguibili contemporaneamente in una coda e così via.

### Note

Le seguenti proprietà vengono visualizzate con i relativi nomi della console Amazon Redshift, con i nomi delle proprietà JSON corrispondenti nelle descrizioni.

La tabella seguente riepiloga se una proprietà è applicabile a WLM automatico o a WLM manuale.

Proprietà WLM	WLM automatico	WLM manuale
Auto WLM (WLM automatico)	Sì	Sì
Abilitazione dell'accelerazione di query brevi	Sì	Sì
Tempo di esecuzione massimo per query brevi	Sì	Sì
Priority (Priorità)	Sì	No
Queue type (Tipo di coda)	Sì	Sì
Nome coda	Sì	Sì
Modalità Dimensionamento simultaneo	Sì	Sì
Simultaneità	No	Sì
Gruppi di utenti	Sì	Sì
Carattere jolly per gruppi di utenti	Sì	Sì
Gruppi di query	Sì	Sì
Carattere jolly per gruppi di query	Sì	Sì
Ruoli utente	Sì	Sì
Carattere jolly del ruolo utente	Sì	Sì
Timeout	No	Deprecated
Memoria	No	Sì
Regole di monitoraggio delle query	Sì	Sì

L'elenco seguente descrive le proprietà WLM che puoi configurare.

### Auto WLM (WLM automatico)

Auto WLM (WLM automatico) impostato su `true` abilita il WLM automatico. La gestione automatica del carico di lavoro imposta i valori per Simultaneità su principale e Memoria (%) su Auto. Amazon Redshift gestisce le query simultanee e l'allocazione della memoria. Il valore predefinito è `true`.

Proprietà JSON: `auto_wlm`

### Abilitazione dell'accelerazione di query brevi

L'accelerazione di query brevi (SQA) rende prioritarie le query a esecuzione breve rispetto a quelle a esecuzione prolungata. SQA esegue le query a esecuzione breve in uno spazio dedicato, di modo che le query SQA non siano costrette ad attendere nelle code dietro le query più lunghe. Con SQA, l'esecuzione delle query brevi è più rapida e gli utenti vedono prima i risultati. Quando abiliti SQA, puoi anche specificare il tempo di esecuzione massimo per le query brevi. Per abilitare SQA, imposta `true`. Il valore predefinito è `false`. Questa impostazione viene applicata a ciascun gruppo di parametri anziché alla coda.

Proprietà JSON: `short_query_queue`

### Tempo di esecuzione massimo per query brevi

Quando abiliti SQA, puoi specificare 0 affinché WLM imposti dinamicamente il tempo di esecuzione massimo per le query brevi. In alternativa, è possibile specificare un valore fisso di 1-20 secondi, in millisecondi. Il valore predefinito è 0.

Proprietà JSON: `max_execution_time`

### Priority (Priorità)

La priorità imposta la priorità delle query eseguite in una coda. Per impostare la priorità, WLM mode (Modalità WLM) deve essere impostata su Auto WLM (WLM automatico); ovvero, `auto_wlm` deve essere `true`. I valori di priorità possono essere `highest`, `high`, `normal`, `low` e `lowest`. Il valore predefinito è `normal`.

Proprietà JSON: `priority`

## Queue type (Tipo di coda)

Il tipo di coda indica se una coda è utilizzata da Auto WLM (WLM automatico) o da Manual WLM (WLM manuale). Impostare `queue_type` su `auto` o su `manual`. Se non si specifica un valore predefinito, viene utilizzato `manual`.

Proprietà JSON: `queue_type`

## Nome coda

Il nome della coda. Puoi impostare il nome della coda in base alle tue esigenze. I nomi delle code devono essere univoci all'interno di una configurazione WLM, contenere fino a 64 caratteri alfanumerici, caratteri di sottolineatura o spazi e non possono contenere virgolette. Ad esempio, se disponi di una coda per le query ETL, puoi denominarla `ETL_queue`. Questo nome viene utilizzato nei parametri, nei valori della tabella di sistema e nella console Amazon Redshift per identificare la coda. Le query e i report che utilizzano il nome di queste origini devono essere in grado di gestire le modifiche del nome. In precedenza, i nomi delle code erano generati da Amazon Redshift. I nomi predefiniti delle code sono `Queue_1`, `Queue_2`, con l'ultima coda denominata `Default_queue`.

### Important

Se modifichi il nome di una coda, cambia anche il valore della `QueueName` dimensione delle metriche della coda WLM (come `WLM`, `WLM QueueWait Time`, `WLMQueueLength`, `WLM`, `WLM` e così via `QueriesCompletedPerSecond`). `QueryDuration RunningQueries` Pertanto, se si modifica il nome di una coda, potrebbe essere necessario modificare gli allarmi impostati. `CloudWatch`

Proprietà JSON: `name`

## Modalità dimensionamento della simultaneità

Per abilitare il dimensionamento della simultaneità su una coda, imposta la `Concurrency Scaling mode` (Modalità dimensionamento della simultaneità) su `auto`. Quando il numero di query instradate a una coda supera la simultaneità configurata della coda, le query idonee vengono inviate al cluster di dimensionamento. Quando gli slot diventano disponibili, le query vengono eseguite nel cluster principale. Il valore predefinito è `off`.

Proprietà JSON: `concurrency_scaling`

## Concurrency (Simultaneità)

Il numero di query eseguibili simultaneamente in una coda WLM manuale. Questa proprietà si applica solo a WLM manuale. Se il dimensionamento simultaneo è abilitato, le query idonee vengono inviate a un cluster di dimensionamento quando la coda raggiunge il livello di simultaneità (slot di query). Se il dimensionamento della simultaneità non è abilitato, le query attendono in coda fino a quando uno slot non diventa disponibile. L'intervallo è tra 1 e 50.

Proprietà JSON: `query_concurrency`

## Gruppi di utenti

Un elenco di nomi di gruppo utenti separati da virgola. Quando i membri del gruppo di utenti eseguono le query nel database, le relative query sono instradate alla coda associata di quel gruppo di utenti.

Proprietà JSON: `user_group`

## Carattere jolly per gruppi di utenti

Un valore booleano che indica se abilitare i caratteri jolly per gruppi di utenti. Se è 0, i caratteri jolly sono disabilitati; se è 1, sono abilitati. Quando sono abilitati, puoi utilizzare i caratteri jolly "\*" o "?" per specificare più gruppi di utenti quando esegui le query. Per ulteriori informazioni, consultare [Caratteri jolly](#).

Proprietà JSON: `user_group_wild_card`

## Gruppi di query

Un elenco di gruppi di query separati da virgola. Quando i membri del gruppo di query eseguono delle query nel database, le query sono instradate alla coda associata al relativo gruppo di query.

Proprietà JSON: `query_group`

## Carattere jolly per gruppi di query

Un valore booleano che indica se abilitare i caratteri jolly per gruppi di query. Se è 0, i caratteri jolly sono disabilitati; se è 1, sono abilitati. Quando sono abilitati, puoi utilizzare i caratteri jolly "\*" o "?" per specificare più gruppi di query quando esegui le query. Per ulteriori informazioni, consultare [Caratteri jolly](#).

Proprietà JSON: `query_group_wild_card`

## Ruoli utente

Un elenco di ruoli utente separati da virgola. Quando i membri con quel ruolo utente eseguono le query nel database, queste sono instradate alla coda associata con quel ruolo utente. Per ulteriori informazioni, consulta [Controllo accessi basato sui ruoli \(RBAC\)](#).

Proprietà JSON: `user_role`

### Carattere jolly dei ruoli utente

Un valore booleano che indica se abilitare i caratteri jolly per gruppi di query. Se è 0, i caratteri jolly sono disabilitati; se è 1, sono abilitati. Quando sono abilitati, puoi utilizzare i caratteri jolly "\*" o "?" per specificare più gruppi di query quando esegui le query. Per ulteriori informazioni, consultare [Caratteri jolly](#).

Proprietà JSON: `user_role_wild_card`

### Timeout (ms)

Il timeout WLM (`max_execution_time`) è sconsigliato. Non è disponibile se si utilizza WLM automatico. Al contrario, è necessario creare una regola di monitoraggio di query (QMR) utilizzando `query_execution_time` per limitare il tempo di esecuzione trascorso per una query. Per ulteriori informazioni, consultare [Regole di monitoraggio delle query WLM](#).

Il tempo massimo, in millisecondi, entro il quale le query possono essere eseguite prima di essere annullate. In alcuni casi, una query di sola lettura, come un'istruzione SELECT, può essere cancellata a causa di un timeout WLM. In questi casi, WLM tenta di indirizzare la query alla successiva coda corrispondente in base alle regole di assegnazione delle code WLM. Se la query non soddisfa nessun'altra definizione di coda, viene annullata e non viene quindi assegnata alla coda predefinita. Per ulteriori informazioni, consultare [Hop della coda di query WLM](#). Il timeout WLM non si applica a una query il cui stato è `returning`. Per visualizzare lo stato di una query, consultare la tabella di sistema [STV\\_WLM\\_QUERY\\_STATE](#).

Proprietà JSON: `max_execution_time`

### Memoria (%)

La percentuale di memoria da allocare alla coda. Se si specifica una percentuale di memoria per almeno una delle code, è necessario specificare una percentuale per tutte le altre code fino a un totale del 100%. Se l'allocazione della memoria è sotto il 100 per cento in tutte le code, la memoria non allocata viene gestita dal servizio. Il servizio può assegnare questa memoria non allocata temporaneamente a una coda che necessita di memoria aggiuntiva per l'elaborazione.

## Proprietà JSON: `memory_percent_to_use`

### Regole di monitoraggio delle query

Puoi utilizzare il monitoraggio delle query WLM per monitorare in modo continuo le code WLM per le query in base ai criteri o ai predicati che specifichi. Ad esempio, potresti monitorare le query che tendono a consumare una quantità eccessiva di risorse di sistema e quindi avviare una determinata azione quando una query supera i limiti delle prestazioni specificati.

#### Note

Se scegli di creare regole a livello di programmazione, ti consigliamo vivamente di utilizzare la console per generare il JSON da includere nella definizione del gruppo di parametri.

Una regola di monitoraggio viene associata a una specifica coda di query. Puoi avere fino a 25 regole per coda, che è anche il limite complessivo di tutte le code.

### Proprietà JSON: `rules`

#### Gerarchia delle proprietà JSON:

```
rules
  rule_name
  predicate
    metric_name
    operator
    value
  action
    value
```

Per ogni regola, specifichi le seguenti proprietà:

- `rule_name`: i nomi delle regole devono essere univoci nella configurazione WLM. Possono essere composti da un massimo di 32 caratteri alfanumerici o caratteri di sottolineatura e non possono contenere spazi o virgolette.
- `predicate`: è possibile avere fino a tre predicati per regola. Per ogni predicato, specifica le seguenti proprietà.
  - `metric_name`: per un elenco di parametri, consultare [Parametri di monitoraggio delle query](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

- `operator`: le operazioni sono =, < e >.
- `value`: il valore di soglia per il parametro specificato che avvia un'operazione.
- `action`: ogni regola è associata a un'operazione. Le operazioni valide sono:
  - `log`
  - `hop` (disponibile solo con WLM manuale)
  - `abort`
  - `change_query_priority` (disponibile solo con WLM automatico)

L'esempio seguente mostra il codice JSON di una regola di monitoraggio di query WLM denominata `rule_1`, con due predicati e l'operazione `hop`.

```
"rules": [  
  {  
    "rule_name": "rule_1",  
    "predicate": [  
      {  
        "metric_name": "query_execution_time",  
        "operator": ">",  
        "value": 100000  
      },  
      {  
        "metric_name": "query_blocks_read",  
        "operator": ">",  
        "value": 1000  
      }  
    ],  
    "action": "hop"  
  }  
]
```

Per ulteriori informazioni su ognuna di queste proprietà e strategie per la configurazione di code di query, consultare [Implementazione della gestione del carico di lavoro](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

# Configurazione del parametro `wlm_json_configuration` utilizzando il AWS CLI

Per configurare la gestione del carico di lavoro, è necessario modificare il parametro `wlm_json_configuration`. La dimensione massima del valore della proprietà `wlm_json_configuration` è 8000 caratteri. Il valore è formattato in Object Notation (JSON). JavaScript Se configuri WLM utilizzando l' AWS CLI API Amazon Redshift o uno degli SDK, usa AWS il resto di questa sezione per scoprire come costruire la struttura JSON per il parametro. `wlm_json_configuration`

## Note

Se si configura la WLM utilizzando la console Amazon Redshift, non è necessario conoscere la formattazione JSON, in quanto la console fornisce un modo semplice per aggiungere code e configurarne le proprietà. Per ulteriori informazioni sulla configurazione di WLM mediante la console, consultare [Modifica di un gruppo di parametri](#).

## Esempio

L'esempio seguente è la configurazione WLM predefinita, che definisce una coda con un WLM automatico.

```
{
  "auto_wlm": true
}
```

## Esempio

L'esempio seguente è una configurazione WLM personalizzata, che definisce una coda WLM manuale con un livello di simultaneità (slot di query) pari a 5.

```
{
  "query_concurrency": 5
}
```

## Sintassi

La configurazione WLM predefinita è molto semplice, con una sola coda e una sola proprietà. Puoi aggiungere altre code e configurare molteplici proprietà per ogni coda nella struttura JSON. La sintassi seguente rappresenta la struttura JSON che utilizzi per configurare molteplici code con molteplici proprietà:

```
[
  {
    "ParameterName": "wlm_json_configuration", "ParameterValue":
      "[
        {
          "q1_first_property_name": "q1_first_property_value",
          "q1_second_property_name": "q1_second_property_value",
          ...
        },
        {
          "q2_first_property_name": "q2_first_property_value",
          "q2_second_property_name": "q2_second_property_value",
          ...
        }
      ]"
  }
]
```

Nell'esempio precedente, le proprietà rappresentative che iniziano con q1 sono oggetti in una matrice per la prima coda. Ognuno di questi oggetti è una coppia nome/valore; name e value insieme impostano le proprietà WLM della prima coda. Le proprietà rappresentative che iniziano con q2 sono oggetti in una matrice per la seconda coda. Se sono necessarie altre code, è necessario aggiungere un altro array per ogni coda supplementare e impostare le proprietà per ogni oggetto.

Quando si modifica la configurazione della gestione del carico di lavoro, è necessario includere l'intera struttura per le code, anche se si intende modificare soltanto una proprietà in una coda. Questo perché l'intera struttura JSON viene passata in forma di stringa come valore del parametro `wlm_json_configuration`.

## Formattazione del comando AWS CLI

Il parametro `wlm_json_configuration` richiede uno specifico formato quando utilizzi l'AWS CLI. Il formato utilizzato dipende dal sistema operativo del cliente. Poiché i sistemi operativi dispongono di più modi per racchiudere la struttura JSON, questa viene passata correttamente dalla riga di

comando. Per dettagli su come creare il comando appropriato nei sistemi operativi Linux, Mac OS X e Windows, vedi le sezioni seguenti. [Per ulteriori informazioni sulle differenze nell'inclusione delle strutture di dati JSON in generale, consulta Quoting strings AWS CLI in the User Guide.AWS Command Line Interface](#)

## Examples (Esempi)

L'esempio di comando seguente configura WLM manuale per un gruppo di parametri denominato `example-parameter-group`. La configurazione abilita l'accelerazione di query brevi con un tempo di esecuzione massimo per tali query impostato su 0; questo valore comporta l'impostazione dinamica del valore da parte di WLM. L'impostazione `ApplyType` è `dynamic`. Questa impostazione comporta l'applicazione immediata di eventuali modifiche apportate alle proprietà dinamiche nel parametro, a meno che altre modifiche statiche non siano state apportate alla configurazione. La configurazione definisce tre code con quanto segue:

- La prima coda consente agli utenti di specificare `report` come etichetta (come specificato nella proprietà `query_group`) nelle loro query per facilitare l'instradamento delle query a quella coda. Le ricerche con caratteri jolly sono abilitate per l'etichetta `report*`, quindi questa non deve essere esatta affinché le query siano instradate alla coda. Ad esempio, `reports` e `reporting` corrispondono entrambe a questo gruppo di query. La coda utilizza il 25% della memoria totale allocata per tutte le code e può eseguire fino a quattro query contemporaneamente. Le query sono limitate a un tempo massimo di 20000 millisecondi (ms). La modalità è impostata su `auto`, quindi quando gli slot della query della coda sono completi, le query idonee vengono inviate a un cluster di dimensionamento.
- La seconda coda consente agli utenti che sono membri dei gruppi `admin` e `dba` nel database di instradare le loro query alla coda per l'elaborazione. Le ricerche con caratteri jolly sono disabilitate per i gruppi di utenti, quindi gli utenti devono corrispondere esattamente ai gruppi nel database affinché le loro query siano instradate alla coda. La coda utilizza il 40% della memoria totale allocata per tutte le code e può eseguire fino a cinque query contemporaneamente. La modalità è impostata su `off`, quindi tutte le query inviate dai membri dell'`admin` o di gruppi `dba` vengono eseguite nel cluster principale.
- L'ultima coda nella configurazione è la coda predefinita. Questa coda utilizza il 35% della memoria totale allocata per tutte le code e può elaborare fino a cinque query contemporaneamente. La modalità è impostata su `auto`.

**Note**

L'esempio è mostrato su più linee per scopi dimostrativi. I comandi effettivi non comportano interruzioni di riga.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name example-parameter-group
--parameters
'[
  {
    "query_concurrency": 4,
    "max_execution_time": 20000,
    "memory_percent_to_use": 25,
    "query_group": ["report"],
    "query_group_wild_card": 1,
    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "memory_percent_to_use": 40,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [
      "admin",
      "dba"
    ],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "off",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "query_group": [],
    "query_group_wild_card": 0,
```

```

    "user_group": [],
    "user_group_wild_card": 0,
    "user_role": [],
    "user_role_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {"short_query_queue": true}
]'

```

Quanto segue è un esempio di configurazione delle regole di monitoraggio di query WLM per una configurazione WLM automatico. L'esempio crea un gruppo di parametri denominato `example-monitoring-rules`. La configurazione definisce le stesse tre code dell'esempio precedente, ma `query_concurrency` e `memory_percent_to_use` non sono più specificati. La configurazione aggiunge anche le seguenti regole e priorità di query:

- La prima coda definisce una regola denominata `rule_1`. La regola ha due predicati: `query_cpu_time > 10000000` e `query_blocks_read > 1000`. L'operazione della regola è `log`. La priorità di questa coda è `Normal`.
- La seconda coda definisce una regola denominata `rule_2`. La regola ha due predicati: `query_execution_time > 600000000` e `scan_row_count > 1000000000`. L'operazione della regola è `abort`. La priorità di questa coda è `Highest`.
- L'ultima coda nella configurazione è la coda predefinita. La priorità di questa coda è `Low`.

### Note

L'esempio è mostrato su più linee per scopi dimostrativi. I comandi effettivi non comportano interruzioni di riga.

```

aws redshift modify-cluster-parameter-group
--parameter-group-name example-monitoring-rules
--parameters
'[ {
  "query_group" : [ "report" ],
  "query_group_wild_card" : 1,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],

```

```

"user_role_wild_card": 0,
"concurrency_scaling" : "auto",
"rules" : [{
  "rule_name": "rule_1",
  "predicate": [{
    "metric_name": "query_cpu_time",
    "operator": ">",
    "value": 1000000 },
    { "metric_name": "query_blocks_read",
    "operator": ">",
    "value": 1000
  } ],
  "action" : "log"
} ],
"priority": "normal",
"queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ "admin", "dba" ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,
  "concurrency_scaling" : "off",
  "rules" : [ {
    "rule_name": "rule_2",
    "predicate": [
      {"metric_name": "query_execution_time",
      "operator": ">",
      "value": 6000000000},
      {"metric_name": "scan_row_count",
      "operator": ">",
      "value": 1000000000}],
    "action": "abort"}],
  "priority": "high",
  "queue_type": "auto"
}, {
  "query_group" : [ ],
  "query_group_wild_card" : 0,
  "user_group" : [ ],
  "user_group_wild_card" : 0,
  "user_role": [ ],
  "user_role_wild_card": 0,

```

```
"concurrency_scaling" : "auto",
"priority": "low",
"queue_type": "auto",
"auto_wlm": true
}, {
  "short_query_queue" : true
} ]'
```

## Configurazione di WLM utilizzando la riga di comando con un file AWS CLI JSON

È possibile modificare il `wlm_json_configuration` parametro utilizzando AWS CLI e passare il valore dell'argomento `parameters` come file JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name
myclusterparametergroup --parameters file://modify_pg.json
```

Gli argomenti per `--parameters` sono memorizzati nel file `modify_pg.json`. La posizione del file è specificata nel formato del tuo sistema operativo. Per ulteriori informazioni, consultare la sezione relativa al [caricamento di parametri da un file](#). Di seguito vengono mostrati degli esempi del contenuto del file JSON `modify_pg.json`.

```
[
  {
    "ParameterName": "wlm_json_configuration",
    "ParameterValue": "[{\\"user_group\\":\\"example_user_group1\\",\\"query_group\\":
\\"example_query_group1\\", \\"query_concurrency\\":7},{\\"query_concurrency\\":5}]"
  }
]
```

```
[
  {
    "ParameterName": "wlm_json_configuration",
    "ParameterValue": "[{\\"query_group\\":[\\"reports\\"],\\"query_group_wild_card\\":0,
\\"query_concurrency\\":4,\\"max_execution_time\\":20000,\\"memory_percent_to_use\\":25},
{\\"user_group\\":[\\"admin\\",\\"dba\\"],\\"user_group_wild_card\\":1,\\"query_concurrency\\":5,
\\"memory_percent_to_use\\":40},{\\"query_concurrency\\":5,\\"memory_percent_to_use\\":35},
{\\"short_query_queue\\": true, \\"max_execution_time\\": 5000 }]",
    "ApplyType": "dynamic"
  }
]
```

]

## Regole per la configurazione di WLM utilizzando la AWS CLI riga di comando sui sistemi operativi Linux e macOS X

Segui queste regole per eseguire un AWS CLI comando con parametri su una riga:

- L'intera struttura JSON deve essere racchiusa tra virgolette singole (') e un set di parentesi quadre ([ ]).
- Tutti i nomi e i valori di parametro devono essere racchiusi tra virgolette doppie (").
- Nel valore `ParameterValue`, è necessario racchiudere l'intera struttura nidificata tra virgolette doppie (") e parentesi quadre ([ ]).
- Nella struttura nidificata, ogni proprietà e valore di ogni coda deve essere racchiuso tra parentesi graffe ({ }).
- Nella struttura nidificata, è necessario utilizzare la barra rovesciata (\) come carattere di escape prima delle virgolette doppie (").
- Per le coppie nome/valore, ogni proprietà deve essere separata dal relativo valore con i due punti (:).
- Ogni coppia nome/valore è separata da un'altra coppia con una virgola (,).
- Le code sono separate da una virgola (,) tra la parentesi graffa finale (}) di una coda e la parentesi graffa iniziale ({) della coda successiva.

## Regole per la configurazione di WLM utilizzando Windows su sistemi operativi PowerShell Microsoft Windows AWS CLI

Segui queste regole per eseguire un AWS CLI comando con parametri su una riga:

- L'intera struttura JSON deve essere racchiusa tra virgolette singole (') e un set di parentesi quadre ([ ]).
- Tutti i nomi e i valori di parametro devono essere racchiusi tra virgolette doppie (").
- Nel valore `ParameterValue`, è necessario racchiudere l'intera struttura nidificata tra virgolette doppie (") e parentesi quadre ([ ]).
- Nella struttura nidificata, ogni proprietà e valore di ogni coda deve essere racchiuso tra parentesi graffe ({ }).

- Nella struttura nidificata, è necessario utilizzare il carattere di escape (\) prima delle virgolette doppie (") e del relativo carattere di escape (\). Ciò significa che dovrai utilizzare tre barre rovesciate e le virgolette doppie affinché le proprietà siano passate correttamente (\\").
- Per le coppie nome/valore, ogni proprietà deve essere separata dal relativo valore con i due punti (:).
- Ogni coppia nome/valore è separata da un'altra coppia con una virgola (,).
- Le code sono separate da una virgola (,) tra la parentesi graffa finale (}) di una coda e la parentesi graffa iniziale ({) della coda successiva.

Regole per la configurazione di WLM mediante il prompt dei comandi su sistemi operativi Windows

Segui queste regole per eseguire un AWS CLI comando con parametri su una riga:

- L'intera struttura JSON deve essere racchiusa tra virgolette doppie (") e un set di parentesi quadre ([ ]).
- Tutti i nomi e i valori di parametro devono essere racchiusi tra virgolette doppie (").
- Nel valore `ParameterValue`, è necessario racchiudere l'intera struttura nidificata tra virgolette doppie (") e parentesi quadre ([ ]).
- Nella struttura nidificata, ogni proprietà e valore di ogni coda deve essere racchiuso tra parentesi graffe ({ }).
- Nella struttura nidificata, è necessario utilizzare il carattere di escape (\) prima delle virgolette doppie (") e del relativo carattere di escape (\). Ciò significa che dovrai utilizzare tre barre rovesciate e le virgolette doppie affinché le proprietà siano passate correttamente (\\").
- Per le coppie nome/valore, ogni proprietà deve essere separata dal relativo valore con i due punti (:).
- Ogni coppia nome/valore è separata da un'altra coppia con una virgola (,).
- Le code sono separate da una virgola (,) tra la parentesi graffa finale (}) di una coda e la parentesi graffa iniziale ({) della coda successiva.

## Gestione di gruppi di parametri mediante la console

È possibile visualizzare, creare, modificare ed eliminare gruppi di parametri nella console Amazon Redshift.

Puoi visualizzare uno qualsiasi dei tuoi gruppi di parametri per vedere un riepilogo dei valori dei parametri e della configurazione WLM (Workload Management, gestione del carico di lavoro). I gruppi di parametri sono mostrati nella scheda Parameters (Parametri) mentre le Workload queues (Code dei carichi di lavoro) sono visualizzate nella scheda Workload Management (Gestione dei carichi di lavoro).

## Creazione di un gruppo di parametri

Se intendi impostare dei valori differenti da quelli del gruppo di parametri predefinito, puoi creare il tuo gruppo di parametri personale.

Per creare un gruppo di parametri

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione scegliere Configurations (Configurazioni), quindi scegliere Workload management (Gestione carichi di lavoro) per visualizzare la pagina Workload management Gestione carichi di lavoro).
3. Scegli Create (Crea) per visualizzare la finestra Create parameter group (Crea gruppo di parametri).
4. Inserisci un valore per le voci Parameter group name (Nome gruppo parametri) and Description (Descrizione).
5. Per creare il gruppo di parametri, scegli Create (Crea).

## Modifica di un gruppo di parametri

In un gruppo di parametri, puoi modificare le impostazioni dei parametri e le proprietà della configurazione WLM.

### Note

Non è consentito modificare il gruppo di parametri predefinito.

Per modificare un gruppo di parametri

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione scegliere Configurations (Configurazioni), quindi scegliere Workload management (Gestione carichi di lavoro) per visualizzare la pagina Workload management Gestione carichi di lavoro).
3. Scegli il gruppo di parametri che intendi modificare per visualizzare la pagina dei dettagli, contenente le schede Parameters (Parametri) e Workload management (Gestione workload).
4. Scegli la scheda Parameters (Parametri) per visualizzare le impostazioni dei parametri correnti.
5. Scegli Edit parameters (Modifica parametri) per abilitare la modifica delle impostazioni di questi parametri:
  - auto\_analyze
  - auto\_mv
  - datestyle
  - enable\_case\_sensitive\_identifier
  - enable\_user\_activity\_logging
  - extra\_float\_digits
  - max\_concurrency\_scaling\_clusters
  - max\_cursor\_result\_set\_size
  - query\_group
  - require\_ssl
  - search\_path
  - statement\_timeout
  - use\_fips\_ssl

Per ulteriori informazioni su questi parametri, consultare [Gruppi di parametri di Amazon Redshift.](#)

6. Inserisci le modifiche e scegli Save (Salva) per aggiornare il gruppo di parametri.

Per modificare la configurazione WLM in un gruppo di parametri

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione scegliere Configurations (Configurazioni), quindi scegliere Workload management (Gestione carichi di lavoro) per visualizzare la pagina Workload management Gestione carichi di lavoro).
3. Scegli il gruppo di parametri che intendi modificare per visualizzare la pagina dei dettagli, contenente le schede Parameters (Parametri) e Workload management (Gestione dei carichi di lavoro).
4. Scegli la scheda Workload management (Gestione dei carichi di lavoro) per visualizzare la configurazione WLM attuale.
5. Scegli Edit workload queues (Modifica code dei carichi di lavoro) per modificare la configurazione del WLM,
6. (Facoltativo) Per abilitare la funzionalità SQA (Short Query Acceleration, accelerazione di query brevi), seleziona Enable short query acceleration (Abilita accelerazione di query brevi).

Quando abiliti la funzionalità SQA, per impostazione predefinita l'opzione Maximum run time for short queries (1 to 20 seconds) (Tempo di esecuzione massimo per query brevi (da 1 a 20 secondi)) viene impostata su Dynamic (Dinamico). Per impostare il runtime massimo su un valore fisso, scegliere un valore compreso tra 1 e 20.

7. Eseguire una o più delle seguenti operazioni per modificare la configurazione relativa alle code:
  - Scegli Switch WLM mode (Cambia modalità WLM) per scegliere tra Automatic WLM (WLM automatico) e Manual WLM (WLM manuale).

Con WLM automatico, i valori Memoria e Simultaneità su principale sono impostati su auto.

- Per creare una coda, scegli Edit workload queues (Modifica code dei carichi di lavoro), quindi scegli Add Queue (Aggiungi coda).
- Per modificare una coda, modifica i valori di proprietà nella tabella. A seconda del tipo di coda, le proprietà possono includere quanto segue:
  - Il Queue name (Nome della coda) può essere modificato.
  - Memoria (%)
  - Concurrency on main cluster (simultaneità nel cluster principale)
  - La Concurrency Scaling mode (Modalità dimensionamento della simultaneità) può essere off (disattivata) o auto (automatica)
  - Timeout (ms)
  - Gruppi di utenti
  - Gruppi di query

- Ruoli utente

Per ulteriori informazioni su queste proprietà, consultare [Proprietà del parametro wlm\\_json\\_configuration](#).

#### Important

Se modifichi il nome di una coda, cambia anche il valore della QueueName dimensione delle metriche della coda WLM (ad esempio, WLM, WLMQueueLength, WLMQueueWaitTime, WLM QueriesCompletedPerSecond e così via QueryDuration). RunningQueries Pertanto, se si modifica il nome di una coda, potrebbe essere necessario modificare gli allarmi impostati. CloudWatch

- Per modificare l'ordine delle code, utilizza i pulsanti freccia Up (Su) e Down (Giù).
  - Per eliminare una coda, scegli Delete (Elimina) nella riga della coda nella tabella.
8. (Facoltativo) Per applicare le modifiche ai cluster dopo il riavvio degli stessi, seleziona Defer dynamic changes until reboot (Rinvia modifiche dinamiche fino al riavvio).

#### Note

Alcune modifiche richiedono il riavvio dei cluster indipendentemente dalla selezione o meno di questa impostazione. Per ulteriori informazioni, consultare [Proprietà WLM dinamiche e statiche](#).

9. Seleziona Save (Salva).

## Creazione o modifica di una regola di monitoraggio di query mediante la console

È possibile utilizzare la console Amazon Redshift per creare e modificare le regole di monitoraggio delle query di WLM. Le regole di monitoraggio di query fanno parte del parametro di configurazione WLM di un gruppo di parametri. Se si modifica una regola di monitoraggio delle query (QMR), la modifica viene eseguita automaticamente senza la necessità di modificare il cluster. Per ulteriori informazioni, consultare [Regole di monitoraggio delle query WLM](#).

Quando crei una regola, definisci il nome della stessa, uno o più predicati e un'operazione.

Quando salvi una configurazione WLM che include una regola, puoi visualizzare il codice JSON della definizione della regola nel codice JSON del parametro di configurazione WLM.

Per creare una regola di monitoraggio di query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Configurations (Configurazioni), quindi scegliere Workload management (Gestione carichi di lavoro) per visualizzare la pagina Workload management Gestione carichi di lavoro).
3. Scegli il gruppo di parametri che intendi modificare per visualizzare la pagina dei dettagli, contenente le schede Parameters (Parametri) e Workload management (Gestione dei carichi di lavoro).
4. Per modificare la configurazione del WLM, scegli Workload management (Gestione dei carichi di lavoro) e quindi Edit workload queues (Modifica code dei carichi di lavoro).
5. Aggiungi una nuova regola utilizzando un modello predefinito o partendo da zero.

Per utilizzare un modello predefinito, procedi come segue:

1. Scegli Add rule from template (Aggiungi regola da modello nel gruppo Query monitoring rules (Regole di monitoraggio delle query). Viene visualizzato l'elenco dei modelli di regola.
2. Scegliere uno o più modelli di regole. Quando scegli Save (Salva), WLM crea una regola per ogni modello scelto.
3. Inserisci o conferma i calcoli per la regole, inclusi Rule names (Nomi delle regole), Predicates (Predicati) e Actions (Operazioni).
4. Selezionare Salva.

Per aggiungere una nuova regola da zero, procedi come segue:

1. Per aggiungere ulteriori predicati, scegli Add predicate (Aggiungi predicato). Possono essere aggiunti fino a tre predicati per ogni regola. Se tutti i predicati sono soddisfatti, WLM attiva l'operazione associata.
2. Scegli un'operazione in Action (Operazione). A ogni regola, è necessario associare un'operazione.
3. Selezionare Salva.

Amazon Redshift genera il parametro di configurazione WLM in formato JSON e lo visualizza nella sezione JSON.

## Eliminazione di un gruppo di parametri

Puoi eliminare un gruppo di parametri se questo non è più necessario e non è associato ad alcun cluster. È consentito eliminare soltanto gruppi di parametri personalizzati.

Per eliminare un gruppo di parametri

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Configurations (Configurazioni), quindi scegliere Workload management (Gestione carichi di lavoro) per visualizzare la pagina Workload management Gestione carichi di lavoro).
3. In Parameter groups (Gruppi di parametri), scegli il gruppo di parametri da modificare.

### Note

Non è possibile eliminare il gruppo di parametri predefinito.

4. Scegli Delete (Elimina) e conferma di voler eliminare il gruppo di parametri.

## Associazione di un gruppo di parametri a un cluster

Quando si avvia un cluster, è necessario associarlo a un gruppo di parametri. Se intendi cambiare il gruppo di parametri successivamente, puoi modificare il cluster e scegliere un gruppo di parametri differente.

## Gestione dei gruppi di parametri utilizzando AWS CLI l'API Amazon Redshift

Puoi utilizzare le seguenti operazioni di Amazon Redshift AWS CLI per gestire i gruppi di parametri.

- [create-cluster-parameter-group](#)
- [delete-cluster-parameter-group](#)
- [describe-cluster-parameters](#)

- [describe-cluster-parameter-groups](#)
- [describe-default-cluster-parameters](#)
- [modify-cluster-parameter-group](#)
- [reset-cluster-parameter-group](#)

Per gestire i gruppi di parametri, è possibile usare le seguenti operazioni API di Amazon Redshift.

- [CreateClusterParameterGroup](#)
- [DeleteClusterParameterGroup](#)
- [DescribeClusterParametri](#)
- [DescribeClusterParameterGroups](#)
- [DescribeDefaultClusterParameters](#)
- [ModifyClusterParameterGroup](#)
- [ResetClusterParameterGroup](#)

# Integrazione di Amazon Redshift con un partner AWS

Lavorando con Amazon Redshift, puoi effettuare l'integrazione con AWS i partner dalla pagina dei dettagli del cluster sulla console Amazon Redshift. Dalla pagina dei dettagli del cluster, puoi velocizzare l'onboarding dei dati nel tuo data warehouse AWS Amazon Redshift con le applicazioni dei partner. È inoltre possibile unire e analizzare i dati provenienti da origini diverse insieme ai dati esistenti nel cluster. Prima di completare l'integrazione con Informatica, è necessario aggiungere gli indirizzi IP del partner all'elenco del traffico in entrata consentito. I seguenti AWS partner possono integrarsi con Amazon Redshift:

- [Datacoral](#)
- [Etleap](#)
- [Fivetran](#)
- [SnapLogic](#)
- [Stitch](#)
- [Upsolver](#)
- [Matillion \(anteprima\)](#)
- [Sisense \(anteprima\)](#)
- [ThoughtSpot](#)

AWS I partner possono integrarsi con Amazon Redshift utilizzando le operazioni API AWS CLI di Amazon Redshift. Per ulteriori informazioni, consultare Riferimenti dei comandi della AWS CLI o la Documentazione di riferimento dell'API Amazon Redshift.

## Integrazione con un AWS partner tramite la console Amazon Redshift

Utilizza la seguente procedura per integrare un cluster con un AWS partner.

Per integrare un cluster Amazon Redshift con un partner AWS

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster).

3. Scegliere il cluster che si desidera integrare.
4. Scegliere Aggiungi integrazione con i partner. Si apre la pagina Scegli un partner con i dettagli sui AWS partner disponibili.
5. Scegli un AWS partner, quindi scegli Avanti.

Vengono visualizzati ulteriori dettagli sul AWS partner scelto, insieme a dettagli sul cluster che stai integrando. La sezione dei dettagli del cluster include informazioni fornite sul sito Web del AWS partner, come l'identificatore del cluster, l'endpoint, il nome del database e il nome utente (che è un nome utente del database). Queste informazioni vengono inviate al partner scelto.

6. Scegli Aggiungi partner per aprire il sito Web del AWS partner.
7. Configurare l'integrazione con il cluster Amazon Redshift sul sito Web del partner. Sul sito Web del partner, è possibile selezionare e configurare le origini dati caricate nel cluster Amazon Redshift. È inoltre possibile definire ulteriori trasformazioni di estrazione, caricamento e trasformazione (ELT) per elaborare i dati aziendali, unirli ad altri set di dati e creare viste consolidate per l'analisi e la creazione di report.

Puoi visualizzare e gestire le integrazioni dei AWS partner dalla scheda Proprietà dei dettagli del cluster. La sezione Integrazioni elenca il nome del partner che è possibile utilizzare per collegarsi al sito Web del AWS partner, lo stato dell'integrazione, il database che riceve i dati e l'ultima connessione riuscita che potrebbe aver aggiornato il cluster.

I valori di stato possibili sono i seguenti:

- Attivo: il AWS partner può connettersi al cluster e completare le attività configurate.
- Inattivo: l'integrazione AWS con i partner non esiste.
- Errore di runtime: il AWS partner può connettersi al cluster ma non può completare le attività configurate.
- Errore di connessione: il AWS partner non può connettersi al cluster.

Dopo aver eliminato un'integrazione AWS Partner da Amazon Redshift, i dati continuano a fluire nel cluster. Completare l'eliminazione sul sito Web del partner.

## Caricamento dei dati con i partner AWS

Oltre a eseguire l'integrazione di un partner con un cluster Amazon Redshift, puoi anche trasferire dati da oltre 30 origini nel tuo cluster utilizzando gli strumenti di caricamento dei dati del nostro

partner. Prima di procedere, devi aggiungere gli indirizzi IP del partner (che trovi di seguito) all'elenco consentito di regole in entrata. Per ulteriori informazioni sull'aggiunta di regole a un gruppo di sicurezza Amazon EC2, consulta [Authorizing Inbound Traffic for Your Instances nella Amazon EC2 User Guide](#). Tieni presente che, sebbene lo strumento di caricamento dei dati di Informatica sia gratuito, potrebbero essere applicati costi di ingresso dei dati a seconda delle origini dati e degli obiettivi scelti.

È possibile caricare dati dai seguenti partner:

- [Informatica: indirizzi IP](#)

Come integrare un cluster Amazon Redshift con Informatica

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel menu di navigazione, scegli l'integrazione con i AWS partner, quindi scegli il partner con cui desideri integrare il cluster.
3. Scegli Complete <partner-name> integration (Completa integrazione con <nome partner>). Si aprirà il sito di integrazione del partner.
4. Inserisci i dettagli necessari sul sito del partner e completa l'integrazione.

# Acquisto di nodi riservati di Amazon Redshift

## Panoramica

Nel AWS, i costi addebitati per l'utilizzo di Amazon Redshift si basano sui nodi di calcolo. Ogni nodo di calcolo viene fatturato in base a una tariffa oraria. La tariffa oraria varia in base a fattori come la regione, il tipo di nodo e a seconda che il nodo specifico riceva i prezzi dei nodi on demand o i prezzi dei nodi riservati.

Il prezzo dei nodi on demand rappresenta l'opzione più costosa ma più flessibile in Amazon Redshift. Con le tariffe on demand, vengono addebitati i costi solo per i nodi di calcolo presenti in un cluster in esecuzione. Se arresti o elimini un cluster, i costi per i nodi di calcolo presenti nel cluster smettono di essere addebitati. Vengono fatturati solo i nodi di calcolo usati e nient'altro. La tariffa oraria addebitata per ogni nodo di calcolo varia a seconda di fattori come la regione e il tipo di nodo.

Il prezzo dei nodi riservati è inferiore rispetto al prezzo on demand perché i nodi di calcolo vengono fatturati in base a tariffe orarie scontate. Per ottenere queste tariffe scontate, tuttavia, è necessario acquistare le offerte di nodi riservati. Quando acquisti un'offerta, fai una prenotazione. La prenotazione dà diritto a una tariffa scontata per ogni nodo che prenoti, per la durata della prenotazione. La tariffa scontata in un'offerta varia a seconda di fattori come la regione, il tipo di nodo, la durata e l'opzione di pagamento.

Puoi designare un nodo come nodo riservato chiamando l'API `PurchaseReservedNodeOffering` o scegliendo `Purchase reserved nodes` (Acquista nodi riservati) sulla console Amazon Redshift. Quando acquisti un nodo riservato, devi specificare una AWS regione, un tipo di nodo, la durata, la quantità di nodi e il tipo di offerta per il tipo di nodo riservato applicabile. Il nodo riservato può essere utilizzato solo nella AWS regione designata.

In questo argomento vengono descritte le offerte di nodi riservati e viene illustrato come acquistarle per ridurre il costo di esecuzione dei cluster Amazon Redshift. Vengono inoltre descritte in termini generali le tariffe on demand o scontate, per aiutarti a comprendere i concetti relativi ai prezzi e come i prezzi influiscono sulla fatturazione. Per ulteriori informazioni sulle tariffe specifiche, consultare [Prezzi di Amazon Redshift](#).

## Informazioni sulle offerte di nodi riservati

Se si prevede che il cluster Amazon Redshift rimanga in esecuzione continuamente per un periodo prolungato di tempo, prendere in considerazione l'acquisto di offerte di nodi riservati. Queste offerte

permettono risparmi significativi rispetto ai prezzi on demand, ma richiedono la prenotazione dei nodi di calcolo e un impegno al pagamento di tali nodi per un periodo di uno o tre anni.

I nodi riservati sono un concetto di fatturazione usato esclusivamente per determinare la tariffa in base a cui tali nodi vengono addebitati. La prenotazione di un nodo non implica l'effettiva creazione di nodi per te. I costi per i nodi riservati vengono addebitati indipendentemente dall'uso, ovvero devi pagare per ogni nodo che prenoti per la durata della prenotazione, indipendentemente dalla presenza di nodi in un cluster in esecuzione a cui si applica la tariffa scontata.

Nella fase di valutazione di un progetto o di sviluppo di un proof of concept, i prezzi on demand offrono un'opzione di pagamento flessibile in base al consumo, che permette di pagare in base all'uso effettivo e di smettere di pagare in qualsiasi momento arrestando o eliminando i cluster. Dopo avere determinato le esigenze dell'ambiente di produzione e avere avviato la fase di implementazione, valuta se prenotare nodi di calcolo acquistando una o più offerte.

Un'offerta può essere applicabile a uno o più nodi di calcolo. Puoi specificare il numero di nodi di calcolo che vuoi prenotare al momento dell'acquisto dell'offerta. Puoi scegliere di acquistare un'offerta per più nodi di calcolo oppure di acquistare più offerte e specificare un determinato numero di nodi di calcolo per ognuna.

Di seguito sono illustrati alcuni esempi di metodi validi di acquisto di un'offerta per tre nodi di calcolo:

- Acquistare un'offerta e specificare tre nodi di calcolo.
- Acquistare due offerte e specificare un nodo di calcolo per la prima offerta e due nodi di calcolo per la seconda offerta.
- Acquistare tre offerte e specificare un nodo di calcolo per ognuna.

## Confronto tra i prezzi delle offerte di nodi riservati

Amazon Redshift permette di scegliere tra diverse opzioni di pagamento per le offerte. L'opzione di pagamento scelta influisce sul piano di pagamento e sulla tariffa scontata addebitata per la prenotazione. Maggiore è il pagamento anticipato per la prenotazione, maggiore sarà il risparmio globale.

Per le offerte sono disponibili le opzioni di pagamento seguenti. Le offerte sono elencate in ordine crescente di risparmio rispetto alle tariffe on demand.

**Note**

Viene addebitata la tariffa oraria applicabile per ogni ora per la durata della prenotazione specificata, indipendentemente dall'uso del nodo riservato. L'opzione di pagamento determina la frequenza dei pagamenti e lo sconto applicato. Per ulteriori informazioni, consultare [Informazioni sulle offerte di nodi riservati](#).

## Confronto tra offerte di nodi riservati

Opzione di pagamento	Piano di pagamento	Risparmi comparativi	Durata	Costi anticipati	Costi mensili ricorrenti
Nessun pagamento anticipato	Rate mensili per la durata della prenotazione. Nessun pagamento anticipato.	Circa il 20% di sconto sulle tariffe on demand.	Periodo di un anno o di tre anni	Nessuno	Sì
Pagamento anticipato parziale	Pagamento anticipato o parziale e rate mensili per la durata della prenotazione.	Sconto fino al 41-73% a seconda della durata.	Periodo di un anno o di tre anni	Sì	Sì
Pagamento anticipato intero o costo	Pagamento anticipato o dell'importo totale per la prenotazione. Nessun costo mensile.	Sconto fino al 42-76% a seconda della durata.	Periodo di un anno o di tre anni	Sì	Nessuno

Le opzioni e le durate specifiche sono soggette a disponibilità.

**Note**

Se in precedenza sono state acquistate offerte per utilizzo pesante per Amazon Redshift, l'offerta paragonabile è quella con pagamento anticipato parziale.

## Modalità di funzionamento dei nodi riservati

Con le offerte di nodi riservati, paghi in base alle condizioni di pagamento descritte nella sezione precedente. Il pagamento avviene secondo questa modalità indipendentemente dal fatto che il cluster sia già in esecuzione o che venga avviato dopo la prenotazione.

Quando acquisti un'offerta, la prenotazione ha lo stato `payment-pending` (pagamento in attesa), fino a quando non viene elaborata. In caso di errore nell'elaborazione della prenotazione, lo stato viene indicato come `payment-failed` (pagamento non riuscito) e puoi provare a eseguire di nuovo l'elaborazione. Una volta completata l'elaborazione della prenotazione, lo stato cambia in `active` (attivo). La tariffa scontata applicabile nella prenotazione non viene addebitata in fattura fino a quando lo stato non cambia in `active` (attivo). Allo scadere della prenotazione, lo stato cambia in `retired` (ritirato), ma puoi continuare ad accedere alle informazioni sulla prenotazione a scopo di riferimento cronologico. Quando una prenotazione si trova nello stato `retired` (ritirato), i cluster rimangono in esecuzione ma potrebbe venire addebitata la tariffa `on demand`, a meno che non sia presente un'altra prenotazione in base a cui vengono applicati prezzi scontati ai nodi.

I nodi riservati sono specifici della regione in cui acquisti l'offerta. Se acquisti un'offerta utilizzando la console Amazon Redshift, seleziona la AWS regione in cui desideri acquistare un'offerta, quindi completa la procedura di prenotazione. Se si acquista un'offerta a livello di programmazione, la regione viene determinata dall'endpoint Amazon Redshift a cui ci si connette. Per ulteriori informazioni sulle regioni di Amazon Redshift, consulta [Regioni ed endpoint](#) in Riferimenti generali di Amazon Web Services.

Per assicurarti che venga applicata la tariffa scontata a tutti i nodi quando avvii un cluster, verifica che la regione, il tipo di nodo e il numero di nodi selezionati corrispondano a una o più prenotazioni attive. In caso contrario, verranno addebitate le tariffe `on demand` per i nodi che non corrispondono a una prenotazione attiva.

In un cluster in esecuzione, se superi il numero di nodi che hai prenotato, i costi per i nodi aggiuntivi vengono addebitati in base alla tariffa `on demand`. Ciò significa che è possibile che vengano addebitate tariffe diverse per i nodi nello stesso cluster, a seconda del numero di nodi riservati. Puoi acquistare un'altra offerta per coprire i nodi aggiuntivi e, in tal caso, una volta che lo stato della prenotazione diventa `active` (attivo), la tariffa scontata viene applicata a tali nodi per il resto della durata.

Se ridimensioni il cluster scegliendo un tipo di nodo diverso e non hai nodi riservati di tale tipo, verrà addebitata la tariffa `on demand`. Se desideri ricevere le tariffe scontate per il cluster ridimensionato, puoi acquistare un'altra offerta con il nuovo tipo di nodi. Tuttavia, continuerai a pagare anche la

prenotazione originale, fino alla sua scadenza. Se è necessario modificare le prenotazioni prima della scadenza, creare un caso di supporto usando la [Console AWS](#).

## Nodi riservati e fatturazione consolidata

I vantaggi in termini di prezzi dei nodi riservati sono condivisi quando l'account di acquisto fa parte di un insieme di account fatturati in un unico account pagamento con fatturazione consolidata. L'utilizzo orario in tutti gli account secondari viene aggregato mensilmente nell'account di pagamento. In genere, questa modalità è utile per le aziende con diversi team o gruppi funzionali. Successivamente, viene applicata la normale logica per i nodi riservati per calcolare la fattura. Per ulteriori informazioni, consulta la pagina [Fatturazione consolidata nella Guida](#) per l' AWS Billing utente.

## Esempi di nodi riservati

Gli scenari in questa sezione illustrano in che modo vengono accumulati i costi per i nodi in base alle tariffe on demand e scontate con i dettagli di prenotazione seguenti:

- Regione: Stati Uniti occidentali (Oregon)
- Tipo di nodo: ra3.xlplus
- Opzione di pagamento: nessun pagamento anticipato
- Durata: un anno
- Numero di nodi riservati: 16

### Esempio 1

Hai un cluster nella regione degli Stati Uniti occidentali (Oregon) con 20 nodi.

In questo scenario, per 16 nodi viene applicata la tariffa scontata in base alla prenotazione, mentre i 4 nodi aggiuntivi nel cluster vengono fatturati in base alla tariffa on demand.

### Esempio 2

Hai un cluster nella regione Stati Uniti occidentali (Oregon) con 12 nodi.

In questo scenario, per tutti e 12 i nodi nel cluster viene applicata la tariffa scontata in base alla prenotazione. Tuttavia, paghi anche la tariffa per i nodi riservati rimanenti, anche se al momento non c'è alcun cluster in esecuzione in cui vengono usati.

## Esempio 3

Hai un cluster nella regione Stati Uniti occidentali (Oregon) con 12 nodi. Esegui il cluster per alcuni mesi con questa configurazione e quindi devi aggiungere nodi al cluster. Ridimensioni il cluster scegliendo lo stesso tipo di nodo e specificando un totale di 16 nodi.

In questo scenario viene fatturata la tariffa scontata per 16 nodi. Le spese rimangono costanti per tutto l'anno perché il numero di nodi presenti nel cluster equivale al numero di nodi riservati.

## Esempio 4

Hai un cluster nella regione Stati Uniti occidentali (Oregon) con 16 nodi. Esegui il cluster per alcuni mesi con questa configurazione e quindi devi aggiungere nodi. Ridimensioni il cluster scegliendo lo stesso tipo di nodo e specificando un totale di 20 nodi.

In questo scenario, prima del ridimensionamento viene fatturata la tariffa scontata per tutti i nodi. Dopo il ridimensionamento, viene fatturata la tariffa scontata per 16 nodi per il resto dell'anno e viene fatturata la tariffa on demand per i 4 nodi aggiunti al cluster.

## Esempio 5

Hai due cluster nella regione Stati Uniti occidentali (Oregon). Uno dei cluster ha 6 nodi e l'altro ha 10 nodi.

In questo scenario, viene fatturata la tariffa scontata per tutti i nodi, perché il numero totale dei nodi presenti nei due cluster equivale al numero di nodi riservati.

## Esempio 6

Hai due cluster nella regione Stati Uniti occidentali (Oregon). Uno dei cluster ha 4 nodi e l'altro ha 6 nodi.

In questo scenario, viene fatturata la tariffa scontata per i 10 nodi in esecuzione nei cluster e paghi anche la tariffa scontata per i 6 nodi aggiuntivi che hai prenotato, anche se al momento non c'è alcun cluster in esecuzione in cui vengono usati.

# Acquisto di un'offerta di nodi riservati con la console Amazon Redshift

È possibile usare la pagina Nodi riservati nella console Amazon Redshift per acquistare offerte di nodi riservati e per visualizzare le prenotazioni correnti e passate.

Dopo aver acquistato un'offerta, nell'elenco Reserved Node (Nodi riservati) vengono visualizzate le prenotazioni con i relativi dettagli, ad esempio tipo di nodo, numero di nodi e stato della prenotazione. Per ulteriori informazioni sui dettagli della prenotazione, consultare [Modalità di funzionamento dei nodi riservati](#).

Per acquistare un nodo riservato

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere Reserved nodes (Nodi riservati) per visualizzare un elenco dei nodi riservati.
3. Scegli Purchase reserved nodes (Acquista nodi riservati) per visualizzare la pagina nella quale scegliere le proprietà del nodo che desideri acquistare.
4. Inserisci le proprietà del nodo, quindi scegli Purchase reserved nodes (Acquista nodi riservati).

Per aggiornare un nodo riservato utilizzare l' AWS CLI.

Non è possibile convertire tutti i tipi di nodo in nodi riservati ed è possibile che un nodo riservato esistente non sia disponibile per il rinnovo. Ciò potrebbe essere causato dall'indisponibilità del tipo di nodo. Contatta il supporto clienti per rinnovare un tipo di nodo non disponibile.

## Aggiornamento dei nodi riservati con AWS CLI

Per aggiornare una prenotazione di nodi riservati con AWS CLI

1. Ottieni un elenco di ReservedNodeOffering ID per le offerte che soddisfano i tuoi requisiti in termini di tipo di pagamento, durata e addebiti. L'esempio seguente illustra questa fase.

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
{
  "ReservedNodeOfferings": [
    {
      "Duration": 31536000,
      "ReservedNodeOfferingId": "yyyyyyyy-yy-yy-yy-yy-yyy",
      "UsagePrice": 0.0,
      "NodeType": "dc2.large",
      "RecurringCharges": [
```

```

        {
            "RecurringChargeFrequency": "Hourly",
            "RecurringChargeAmount": 0.2
        }
    ],
    "CurrencyCode": "USD",
    "OfferingType": "No Upfront",
    "ReservedNodeOfferingType": "Regular",
    "FixedPrice": 0.0
}
]
}

```

2. Chiama `accept-reserved-node-exchange` e fornisci l'ID per il nodo riservato DC1 che desideri scambiare insieme all' `ReservedNodeOfferingID` ottenuto nel passaggio precedente.

L'esempio seguente illustra questa fase.

```

aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy
{
  "ExchangedReservedNode": {
    "UsagePrice": 0.0,
    "OfferingType": "No Upfront",
    "State": "exchanging",
    "FixedPrice": 0.0,
    "CurrencyCode": "USD",
    "ReservedNodeId": "zzzzzzzz-zzzz-zzzz-zzzz-zzzzzzzzzzzzz",
    "NodeType": "dc2.large",
    "NodeCount": 1,
    "RecurringCharges": [
      {
        "RecurringChargeFrequency": "Hourly",
        "RecurringChargeAmount": 0.2
      }
    ],
    "ReservedNodeOfferingType": "Regular",
    "StartTime": "2018-06-27T18:02:58Z",
    "ReservedNodeOfferingId": "yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy",
    "Duration": 31536000
  }
}

```

```
}
```

Puoi confermare che lo scambio è completo chiamando [describe-reserved-nodese](#) controllando il valore di `Node type`.

## Acquisto di un'offerta di nodi riservati tramite la AWS CLI e l'API Amazon Redshift

Per l'acquisto delle offerte, è possibile utilizzare le operazioni AWS CLI descritte di seguito.

- [purchase-reserved-node-offering](#)
- [describe-reserved-node-offerings](#)
- [describe-orderable-cluster-options](#)

Per l'acquisto delle offerte di nodi riservati, è possibile utilizzare le operazioni API di Amazon Redshift descritte di seguito.

- [PurchaseReservedNodeOffering](#)
- [DescribeReservedNodeOfferings](#)
- [DescribeOrderableClusterOptions](#)

Non è possibile convertire tutti i tipi di nodo in nodi riservati ed è possibile che un nodo riservato esistente non sia disponibile per il rinnovo. Ciò potrebbe essere causato dall'indisponibilità del tipo di nodo.

# Sicurezza di Amazon Redshift

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. L'efficacia della nostra sicurezza è regolarmente testata e verificata da revisori di terze parti come parte dei [programmi di conformità AWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano ad Amazon Redshift, consultare [Servizi AWS coperti dal programma di conformità](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. L'utente è anche responsabile per altri fattori, tra cui la riservatezza dei dati, i requisiti dell'azienda, nonché le leggi e le normative applicabili.

L'accesso alle risorse Amazon Redshift è controllato a quattro livelli:

- Gestione dei cluster: la capacità di creare, configurare ed eliminare i cluster è controllata dalle autorizzazioni fornite all'utente o all'account associato alle credenziali di sicurezza AWS. Gli utenti con le autorizzazioni appropriate possono usare la AWS Management Console, l'AWS Command Line Interface (CLI) o l'interfaccia di programmazione dell'applicazione (API) di Amazon Redshift per gestire i cluster. Questo accesso viene gestito usando policy IAM.

## Important

Amazon Redshift contiene una raccolta di best practice per la gestione di autorizzazioni, identità e accesso sicuri. Consigliamo di acquisire familiarità con tali best practice quando si inizia a usare Amazon Redshift. Per ulteriori informazioni, consulta [Identity and Access Management in Amazon Redshift](#).

- Connettività del cluster: i gruppi di sicurezza di Amazon Redshift specificano le istanze AWS autorizzate a connettersi a un cluster Amazon Redshift in formato CIDR (Classless Inter-Domain Routing). Per informazioni sulla creazione di gruppi di sicurezza di Amazon Redshift, Amazon EC2

e Amazon VPC e sulla relativa associazione ai cluster, consultare [Gruppi di sicurezza dei cluster Amazon Redshift](#).

- **Accesso al database:** la capacità di accedere agli oggetti del database, come tabelle e viste, è controllata dagli account utente nel database Amazon Redshift. Gli utenti possono accedere solo alle risorse nel database per cui i propri account utente hanno ricevuto l'autorizzazione di accesso necessaria. È possibile creare questi account utente Amazon Redshift e gestire le rispettive autorizzazioni usando le istruzioni [CREATE USER](#), [CREATE GROUP](#), [GRANT](#) e [REVOKE](#). Per ulteriori informazioni, consultare [Gestione della sicurezza dei database](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- **Credenziali di database temporanee e Single Sign-On:** oltre a creare e gestire utenti del database tramite comandi SQL, come `CREATE USER` e `ALTER USER`, è possibile configurare il client SQL con driver JDBC o ODBC di Amazon Redshift personalizzati. Questi driver gestiscono il processo di creazione degli utenti del database e delle password temporanee come parte del processo di accesso al database.

I driver autenticano gli utenti del database in base all'autenticazione AWS Identity and Access Management (IAM). Se alcune identità utente vengono gestite al di fuori di AWS, è possibile utilizzare un provider di identità (IdP) conforme allo standard SAML 2.0 per gestire l'accesso alle risorse Amazon Redshift. È possibile utilizzare un ruolo IAM per configurare l'IdP e AWS per consentire agli utenti federati di generare credenziali temporanee di database e di accedere ai database di Amazon Redshift. Per ulteriori informazioni, consultare [Utilizzo dell'autenticazione IAM per generare credenziali utente di database](#).

Questa documentazione aiuta a comprendere come applicare il modello di responsabilità condivisa quando si utilizza Amazon Redshift. Gli argomenti seguenti descrivono come configurare Amazon Redshift per soddisfare gli obiettivi di sicurezza e conformità. Vengono inoltre fornite informazioni su come utilizzare altri servizi AWS che consentono di monitorare e proteggere le risorse di Amazon Redshift.

## Argomenti

- [Protezione dei dati in Amazon Redshift](#)
- [Identity and Access Management in Amazon Redshift](#)
- [Gestione delle password di amministrazione di Amazon Redshift tramite AWS Secrets Manager](#)
- [Registrazione e monitoraggio in Amazon Redshift](#)
- [Convalida della conformità per Amazon Redshift](#)

- [Resilienza in Amazon Redshift](#)
- [Sicurezza dell'infrastruttura in Amazon Redshift](#)
- [Analisi della configurazione e delle vulnerabilità in Amazon Redshift](#)

## Protezione dei dati in Amazon Redshift

Il [modello di responsabilità condivisa](#) di AWS si applica alla protezione dei dati in Amazon Redshift. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Questo include l'utilizzo di Amazon Redshift o altri Servizi AWS tramite la console, l'API, l'AWS CLI o gli SDK AWS. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti

suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

## Crittografia dei dati

La protezione dei dati ha lo scopo di proteggere i dati sia in transito (durante la trasmissione verso e da Amazon Redshift), sia quando sono inattivi (ovvero quando sono archiviati su disco nei data center Amazon Redshift). I dati in transito possono essere protetti tramite SSL o utilizzando la crittografia lato client. Per la protezione dei dati a riposo in Amazon Redshift sono disponibili le opzioni riportate di seguito.

- Utilizza crittografia lato server: si richiede ad Amazon Redshift di crittografare i dati prima di salvarli su disco nei relativi data center e di decrittarli al momento del download degli oggetti.
- Utilizza crittografia lato client: è possibile crittografare i dati lato client e caricare i dati crittografati in Amazon Redshift. In questo caso, è l'utente a gestire la procedura di crittografia, nonché le chiavi e gli strumenti correlati.

## Crittografia dei dati inattivi

La crittografia lato server esegue la crittografia dei dati a riposo, vale a dire che Amazon Redshift consente di crittografare i dati durante la scrittura nei data center e ne esegue la decrittografia quando avviene l'accesso. Se la richiesta è autenticata e sono disponibili le autorizzazioni per l'accesso, non c'è differenza nelle modalità di accesso ai dati, crittografati o meno.

Amazon Redshift protegge i dati a riposo mediante la crittografia. In alternativa, è possibile proteggere tutti i dati archiviati sui dischi all'interno di un cluster e tutti i backup in Amazon S3 con Advanced Encryption Standard AES-256.

Per gestire le chiavi utilizzate per crittografare e decrittografare le risorse Amazon Redshift, utilizzare [AWS Key Management Service \(AWS KMS\)](#). AWS KMS combina hardware e software sicuri e a disponibilità elevata per offrire un sistema di gestione delle chiavi a misura di cloud. AWS KMS consente di creare chiavi di crittografia e definire le policy che controllano il modo in cui queste chiavi possono essere utilizzate. AWS KMS supporta AWS CloudTrail, pertanto è possibile verificare che le chiavi vengano utilizzate in modo appropriato. È possibile utilizzare le proprie chiavi AWS KMS in combinazione con Amazon Redshift e i servizi AWS supportati. Per un elenco dei servizi che supportano AWS KMS, consultare [Come i servizi AWS utilizzano AWS KMS](#) nella Guida per gli sviluppatori di AWS Key Management Service.

Se scegli di gestire la password di amministratore del cluster con provisioning o dello spazio dei nomi serverless utilizzando AWS Secrets Manager, Amazon Redshift accetta anche una chiave AWS KMS aggiuntiva che viene utilizzata per crittografare le credenziali AWS Secrets Manager. Questa chiave aggiuntiva può essere una chiave generata automaticamente da AWS Secrets Manager o una chiave personalizzata fornita da te.

Amazon Redshift query editor v2 memorizza in modo sicuro le informazioni inserite nell'editor di query come segue:

- ARN (Amazon Resource Name) della chiave KMS usato per crittografare i dati query editor v2.
- Informazioni sulla connessione al database.
- Nomi e contenuti di file e cartelle.

Amazon Redshift query editor v2 crittografa le informazioni utilizzando la crittografia a livello di blocco con la chiave KMS o la chiave KMS dell'account di servizio. La crittografia dei dati Amazon Redshift è controllata dalle proprietà del cluster Amazon Redshift.

## Argomenti

- [Crittografia dei database di Amazon Redshift](#)

## Crittografia dei database di Amazon Redshift

In Amazon Redshift è possibile abilitare la crittografia del database per i cluster per proteggere ulteriormente i dati a riposo. Quando abiliti la crittografia per un cluster, i blocchi di dati e i metadati di sistema vengono crittografati per il cluster e i relativi snapshot.

È possibile abilitare la crittografia all'avvio del cluster oppure modificare un cluster non crittografato per utilizzare la crittografia AWS Key Management Service (AWS KMS). A tale scopo, è possibile utilizzare una chiave AWS gestita o una chiave gestita dal cliente. Quando si modifica il cluster per abilitare la crittografia AWS KMS, Amazon Redshift migra automaticamente i dati a un nuovo cluster crittografato. Anche le snapshot create dal cluster crittografato sono crittografate. Puoi anche eseguire la migrazione di un cluster crittografato in un cluster non crittografato modificando il cluster e l'opzione Encrypt database (Crittografia database). Per ulteriori informazioni, consultare [Modifica della crittografia del cluster](#).

Anche se la crittografia è un'impostazione facoltativa in Amazon Redshift, consigliamo di abilitarla per i cluster che contengono dati sensibili. Inoltre, potresti dover usare la crittografia in base a linee guida o normative che regolano i tuoi dati. Ad esempio, il Payment Card Industry Data Security

Standard (PCI DSS), il Sarbanes-Oxley Act (SOX), l'Health Insurance Portability and Accountability Act (HIPAA) e altre normative simili forniscono linee guida per la gestione di tipi specifici di dati.

Amazon Redshift usa una gerarchia di chiavi di crittografia per crittografare il database. Puoi utilizzare AWS Key Management Service (AWS KMS) o un modulo di sicurezza hardware (HSM) per gestire le chiavi di crittografia di primo livello in questa gerarchia. Il processo utilizzato da Amazon Redshift per la crittografia è diverso a seconda del modo in cui vengono gestite le chiavi. Amazon Redshift si integra automaticamente con un HSM AWS KMS, ma non con un HSM di terze parti. Quando si utilizza un modulo di sicurezza hardware (HSM), è necessario usare certificati client e server per configurare una connessione attendibile tra Amazon Redshift e il modulo di sicurezza hardware (HSM).

Miglioramenti del processo di crittografia per migliori prestazioni e disponibilità

### Crittografia con nodi RA3

Gli aggiornamenti al processo di crittografia per i nodi RA3 hanno migliorato notevolmente l'esperienza. Durante il processo possono essere eseguite sia le query di lettura che quelle di scrittura con un minore impatto sulle prestazioni dovuto alla crittografia. Inoltre, la crittografia termina molto più rapidamente. Le fasi del processo aggiornate includono un'operazione di ripristino e la migrazione dei metadati del cluster su un cluster di destinazione. L'esperienza migliorata si applica ai tipi di crittografia come AWS KMS, ad esempio. Quando si dispone di volumi di dati nell'ordine di petabyte, l'operazione è stata ridotta da settimane a giorni.

Prima di crittografare il cluster, se prevedi di continuare a eseguire i carichi di lavoro del database, puoi migliorare le prestazioni e accelerare il processo aggiungendo nodi con ridimensionamento elastico. Non puoi usare il ridimensionamento elastico quando la crittografia è in corso, quindi effettua questa operazione prima della crittografia. Tieni presente che l'aggiunta di nodi comporta in genere un costo più elevato.

### Crittografia con altri tipi di nodo

Quando si crittografa un cluster con nodi DC2, non è possibile eseguire query di scrittura, come con i nodi RA3. Puoi eseguire solo query di lettura.

### Note di utilizzo per la crittografia con nodi RA3

I seguenti approfondimenti e risorse aiutano a prepararsi alla crittografia e a monitorare il processo.

- Esecuzione delle query dopo l'avvio della crittografia: dopo l'avvio della crittografia, le operazioni di lettura e scrittura sono disponibili entro circa quindici minuti. Il tempo necessario per completare

l'intero processo di crittografia dipende dalla quantità di dati nel cluster e dai livelli del carico di lavoro.

- Quanto tempo richiede la crittografia? - Il tempo necessario per crittografare i dati dipende da diversi fattori: tra cui il numero di carichi di lavoro in esecuzione, le risorse di calcolo utilizzate, il numero e il tipo di nodi. Consigliamo di eseguire inizialmente la crittografia in un ambiente di test. Come regola generale, se lavori con volumi di dati in petabyte, possono essere necessari 1-3 giorni per il completamento della crittografia.
- Come faccio a sapere se la crittografia è terminata? — Dopo aver abilitato la crittografia, il completamento della prima istantanea conferma che la crittografia è stata completata.
- Rollback della crittografia: se devi eseguire il rollback dell'operazione di crittografia, il modo migliore per farlo è ripristinare il backup più recente eseguito prima dell'avvio della crittografia. Dovrai riapplicare tutti i nuovi aggiornamenti (aggiornamenti/eliminazioni/inserimenti) dopo l'ultimo backup.
- Esecuzione del ripristino di una tabella: tieni presente che non puoi ripristinare una tabella da un cluster non crittografato a un cluster crittografato.
- Crittografia di un cluster a nodo singolo: la crittografia di un cluster a nodo singolo presenta limiti di prestazioni. Richiede più tempo della crittografia per un cluster multinodo.
- Creazione di un backup dopo la crittografia: quando si crittografano i dati nel cluster, non viene creato un backup finché il cluster non è completamente crittografato. Il tempo necessario per questa operazione è variabile. Il tempo necessario per il backup può variare da ore a giorni, a seconda delle dimensioni del cluster. Una volta completata la crittografia, può verificarsi un ritardo prima di poter creare un backup.

Si noti che, poiché un' backup-and-restore operazione viene eseguita durante il processo di crittografia, le tabelle o le viste materializzate create con `BACKUP NO` non vengono conservate. Per ulteriori informazioni, consulta [CREATE TABLE](#) o [CREATE MATERIALIZED VIEW](#).

## Argomenti

- [Crittografia dei database per Amazon Redshift tramite AWS KMS](#)
- [Crittografia per Amazon Redshift tramite moduli di sicurezza hardware \(HSM\)](#)
- [Rotazione delle chiavi di crittografia in Amazon Redshift](#)
- [Modifica della crittografia del cluster](#)
- [Configurazione della crittografia di database mediante la console](#)
- [Configurazione della crittografia di database con l'API di Amazon Redshift e la CLI AWS CLI](#)

## Crittografia dei database per Amazon Redshift tramite AWS KMS

Quando scegli AWS KMS la gestione delle chiavi con Amazon Redshift, esiste una gerarchia di chiavi di crittografia a quattro livelli. Queste chiavi, in ordine gerarchico, sono la chiave root, una chiave di crittografia del cluster, una chiave di crittografia del database e le chiavi di crittografia dei dati.

Quando avvii il cluster, Amazon Redshift restituisce un elenco di quelli AWS KMS keys che il tuo AWS account ha creato o in cui è autorizzato a utilizzare. AWS KMS Devi selezionare una chiave KMS del cliente da usare come chiave root nella gerarchia di crittografia.

Per impostazione predefinita, Amazon Redshift seleziona la chiave predefinita come chiave root. La tua chiave predefinita è una chiave AWS gestita creata per il tuo AWS account da utilizzare in Amazon Redshift. AWS KMS crea questa chiave la prima volta che avvii un cluster crittografato in una AWS regione e scegli la chiave predefinita.

Se non desideri utilizzare la chiave predefinita, devi disporre (o creare) separatamente una chiave KMS gestita dal cliente AWS KMS prima di avviare il cluster in Amazon Redshift. Le chiavi gestite dal cliente ti offrono maggiore flessibilità, inclusa la possibilità di creare, ruotare, disabilitare, definire il controllo degli accessi per e controllare le chiavi di crittografia per proteggere i dati. Per ulteriori informazioni sulla creazione di chiavi KMS, consultare [Creazione di chiavi](#) nella Guida per gli sviluppatori di AWS Key Management Service .

Se desideri utilizzare una AWS KMS chiave di un altro AWS account, devi disporre dell'autorizzazione a utilizzare la chiave e specificarne il nome Amazon Resource Name (ARN) in Amazon Redshift. Per ulteriori informazioni sull'accesso alle chiavi in AWS KMS, consulta [Controlling Access to Your Keys](#) nella AWS Key Management Service Developer Guide.

Dopo aver scelto una chiave radice, Amazon Redshift richiede che AWS KMS generino una chiave dati e la crittografino utilizzando la chiave radice selezionata. Questa chiave di dati viene utilizzata come chiave CEK in Amazon Redshift. AWS KMS esporta la chiave CEK crittografata in Amazon Redshift, in cui viene archiviata internamente su disco in una rete separata dal cluster insieme all'autorizzazione per la chiave KMS e il contesto di crittografia per la chiave CEK. Solo la chiave CEK crittografata viene esportata in Amazon Redshift; la KMS rimane in AWS KMS. Amazon Redshift passa la chiave CEK crittografata anche al cluster attraverso un canale sicuro e la carica in memoria. Quindi, Amazon Redshift chiama AWS KMS per decrittografare il CEK e carica il CEK decrittografato in memoria. [Per ulteriori informazioni sulle sovvenzioni, sul contesto di crittografia e su altri concetti AWS KMS correlati, consulta Concepts nella Developer Guide.AWS Key Management Service](#)

Amazon Redshift genera quindi casualmente una chiave da usare come chiave di crittografia del database e la carica in memoria nel cluster. La chiave CEK decrittata viene usata per crittografare la

chiave DEK, che viene quindi passata attraverso un canale sicuro dal cluster per essere archiviata internamente da Amazon Redshift su disco in una rete separata dal cluster. Come per la chiave di crittografia del cluster, la versione crittografata e quella decrittografata della chiave di crittografia del database vengono caricate in memoria nel cluster. La versione decrittografata della chiave di crittografia del database viene quindi usata per crittografare le singole chiavi di crittografia generate casualmente per ogni blocco di dati nel database.

Al riavvio del cluster, Amazon Redshift inizia con le versioni crittografate e archiviate internamente di CEK e DEK, le ricarica in memoria e quindi AWS KMS chiama nuovamente per decrittografare il CEK con la chiave KMS in modo che possa essere caricato in memoria. La chiave di crittografia del cluster decrittografata viene quindi usata per decrittografare di nuovo la chiave di crittografia del database e questa chiave decrittografata viene caricata in memoria e quindi usata per crittografare e decrittografare le chiavi dei blocchi di dati in base alle esigenze.

Per ulteriori informazioni sulla creazione di cluster Amazon Redshift crittografati con chiavi AWS KMS, consultare [Creazione di un cluster](#) e [Gestione dei cluster utilizzando l'API AWS CLI Amazon Redshift](#).

### Copia di istantanee crittografate in un'altra regione AWS KMSAWS

AWS KMS le chiavi sono specifiche di una regione. AWS Se abiliti la copia degli snapshot di Amazon Redshift in AWS un'altra regione e il cluster di origine e i relativi snapshot sono crittografati utilizzando una chiave radice AWS KMS da, devi configurare una concessione per Amazon Redshift per utilizzare una chiave radice nella regione di destinazione. AWS Questa concessione consente ad Amazon Redshift di crittografare le istantanee nella regione di destinazione. AWS Per ulteriori informazioni sulla copia di snapshot tra regioni, consultare [Copia di snapshot in un'altra regione AWS](#).

#### Note

Se abiliti la copia di istantanee da un cluster crittografato e la utilizzi AWS KMS come chiave principale, non puoi rinominare il cluster perché il nome del cluster fa parte del contesto di crittografia. Se è necessario rinominare il cluster, è possibile disabilitare la copia delle istantanee nella AWS regione di origine, rinominare il cluster e quindi configurare e abilitare nuovamente la copia delle istantanee.

Il processo di configurazione dell'autorizzazione per la copia degli snapshot viene descritto di seguito.

1. Nella AWS regione di destinazione, crea una concessione per la copia delle istantanee effettuando le seguenti operazioni:
  - Se non hai già una AWS KMS chiave da usare, creane una. Per ulteriori informazioni sulla creazione di AWS KMS chiavi, consulta [Creating Keys](#) nella AWS Key Management Service Developer Guide.
  - Specificare un nome per l'autorizzazione di copia degli snapshot. Questo nome deve essere univoco in quella AWS regione per il tuo AWS account.
  - Specificate l'ID della AWS KMS chiave per cui state creando la sovvenzione. Se non si specifica un ID chiave, l'autorizzazione viene applicata alla chiave predefinita.
2. Nella AWS regione di origine, abilitate la copia delle istantanee e specificate il nome della concessione per la copia delle istantanee che avete creato nella regione di destinazione. AWS

Questo processo precedente è necessario solo se abiliti la copia di istantanee utilizzando l' AWS CLI API Amazon Redshift o gli SDK. Se si utilizza la console, Amazon Redshift fornisce il flusso di lavoro appropriato per configurare l'autorizzazione quando si abilita la copia di snapshot tra regioni. Per ulteriori informazioni sulla configurazione della copia di snapshot tra regioni per cluster crittografati con AWS KMS utilizzando la console, consultare [Configura una copia delle istantanee tra regioni per un cluster crittografato AWS KMS](#).

Prima che lo snapshot venga copiato AWS nella regione di destinazione, Amazon Redshift decripta lo snapshot utilizzando la chiave radice nella regione di AWS origine e lo cripta nuovamente temporaneamente utilizzando una chiave RSA generata casualmente che Amazon Redshift gestisce internamente. Amazon Redshift copia quindi lo snapshot su un canale sicuro AWS nella regione di destinazione, decripta lo snapshot utilizzando la chiave RSA gestita internamente e quindi cripta nuovamente lo snapshot utilizzando la chiave radice nella regione di destinazione. AWS

Per ulteriori informazioni sulla configurazione delle concessioni di copie istantanee per cluster crittografati, consulta. AWS KMS [Configurazione di Amazon Redshift per l'utilizzo delle chiavi di crittografia AWS KMS con l'API di Amazon Redshift e AWS CLI](#)

Crittografia per Amazon Redshift tramite moduli di sicurezza hardware (HSM)

Se non lo utilizzi AWS KMS per la gestione delle chiavi, puoi utilizzare un modulo di sicurezza hardware (HSM) per la gestione delle chiavi con Amazon Redshift.

**⚠ Important**

La crittografia tramite un modulo di sicurezza hardware non è supportata per tipi di nodo DC2 ed RA3.

I moduli di sicurezza hardware sono dispositivi che forniscono il controllo diretto sulla generazione e sulla gestione delle chiavi. Forniscono una sicurezza maggiore separando la gestione delle chiavi dai livelli applicazione e database. Amazon Redshift supporta AWS CloudHSM Classic per la gestione delle chiavi. Il processo di crittografia è diverso quando usi un modulo di sicurezza hardware per gestire le chiavi di crittografia invece di AWS KMS.

**⚠ Important**

Amazon Redshift supporta solo AWS CloudHSM la versione Classic. Il servizio AWS CloudHSM più recente non è supportato.

AWS CloudHSM Classic è chiuso ai nuovi clienti. Per ulteriori informazioni, consulta la pagina dei prezzi di [CloudHSM Classic](#). AWS CloudHSM La versione classica non è disponibile in tutte le AWS regioni. Per ulteriori informazioni sulle AWS regioni disponibili, consulta la [tabella delle AWS regioni](#).

Quando si configura il cluster per l'uso di un modulo di sicurezza hardware (HSM), Amazon Redshift invia una richiesta al modulo di sicurezza hardware per generare e archiviare una chiave da usare come chiave di crittografia del cluster. Tuttavia AWS KMS, a differenza di HSM, non esporta il CEK in Amazon Redshift. Amazon Redshift genera invece casualmente la chiave DEK nel cluster e la passa al modulo di sicurezza hardware (HSM) perché venga crittografata dalla chiave di crittografia del cluster. Il modulo di sicurezza hardware (HSM) restituisce la chiave DEK crittografata ad Amazon Redshift, in cui viene ulteriormente crittografata con una chiave root interna generata casualmente e archiviata internamente su disco in una rete separata dal cluster. Amazon Redshift inoltre carica la versione decrittata della chiave DEK nella memoria nel cluster in modo che la chiave possa essere utilizzata per crittografare e decrittare le singole chiavi per i blocchi di dati.

Se il cluster viene riavviato, Amazon Redshift decrittata la chiave DEK doppiamente crittografata e archiviata internamente usando la chiave root interna per riportare la chiave DEK archiviata internamente allo stato di crittografia tramite la chiave CEK. La chiave DEK crittografata con la chiave CEK viene passata al modulo di sicurezza hardware (HSM) perché venga decrittata e quindi passata

di nuovo ad Amazon Redshift, in cui può essere caricata di nuovo in memoria per l'uso con le singole chiavi dei blocchi di dati.

## Configurazione di una connessione attendibile tra Amazon Redshift e un modulo di sicurezza hardware (HSM)

Se si decide di usare un modulo di sicurezza hardware (HSM) per la gestione della chiave del cluster, è necessario configurare un collegamento di rete attendibile tra Amazon Redshift e il modulo di sicurezza hardware. A questo scopo, devi configurare certificati client e server. La connessione attendibile viene usata per passare le chiavi di crittografia tra il modulo di sicurezza hardware e Amazon Redshift durante le operazioni di crittografia e decrittografia.

Amazon Redshift crea un certificato client pubblico da una coppia di chiavi privata e pubblica generata casualmente. Queste chiavi vengono crittografate e archiviate internamente. Devi scaricare e registrare il certificato client pubblico nel modulo di sicurezza hardware e quindi assegnarlo alla partizione del modulo di sicurezza hardware appropriata.

Fornire ad Amazon Redshift l'indirizzo IP dell'HSM, il nome e la password della partizione HSM e un certificato server HSM pubblico, che viene crittografato con una chiave root interna. Amazon Redshift completa il processo di configurazione e verifica se riesce a connettersi a HSM. In caso contrario, il cluster passa allo stato `INCOMPATIBLE_HSM` (`HSM_INCOMPATIBILE`) e non viene creato. In questo caso, devi eliminare il cluster incompleto e riprovare.

### Important

Quando si modifica il cluster per l'uso di una partizione del modulo di sicurezza hardware diversa, Amazon Redshift verifica di riuscire a connettersi alla nuova partizione, ma non verifica la presenza di una chiave di crittografia valida. Prima di usare la nuova partizione, devi replicarvi le chiavi. Se il cluster viene riavviato e Amazon Redshift non riesce a trovare una chiave valida, il riavvio non riesce. Per ulteriori informazioni, consultare la pagina relativa alla [replica di chiavi tra moduli di sicurezza hardware](#).

Se dopo la configurazione iniziale Amazon Redshift non riesce a connettersi al modulo di sicurezza hardware (HSM), viene registrato un evento. Per ulteriori informazioni su questi eventi, consultare [Notifiche di eventi di Amazon Redshift](#).

## Rotazione delle chiavi di crittografia in Amazon Redshift

In Amazon Redshift è possibile eseguire la rotazione delle chiavi di crittografia per i cluster crittografati. All'inizio del processo di rotazione delle chiavi, Amazon Redshift esegue la rotazione della chiave CEK per il cluster specificato e per qualsiasi snapshot automatico o manuale del cluster. Amazon Redshift esegue la rotazione anche della chiave DEK per il cluster specificato, ma non può ruotare la chiave DEK per gli snapshot mentre questi sono archiviati internamente in Amazon Simple Storage Service (Amazon S3) e crittografati con la chiave DEK esistente.

Durante la rotazione, il cluster passa allo stato `ROTATING_KEYS` fino al completamento, quindi torna allo stato `AVAILABLE`. Amazon Redshift gestisce la decrittografia e la nuova crittografia durante il processo di rotazione delle chiavi.

### Note

Non puoi eseguire la rotazione delle chiavi per snapshot senza un cluster di origine. Prima di eliminare un cluster, valuta se gli snapshot associati usano la rotazione delle chiavi.

Poiché il cluster è momentaneamente non disponibile durante il processo di rotazione delle chiavi, devi ruotare le chiavi solo in base alla frequenza determinata dalle esigenze relative ai dati o quando sospetti che le chiavi siano state compromesse. Come best practice, devi esaminare il tipo di dati archiviati e determinare la frequenza della rotazione delle chiavi che crittografano i dati. La frequenza per la rotazione delle chiavi varia a seconda delle policy aziendali in materia di sicurezza dei dati e di qualsiasi standard del settore relativo ai dati sensibili e alla conformità alle normative. Assicurati che il tuo piano garantisca un giusto equilibrio tra esigenze di sicurezza e considerazioni sulla disponibilità per il cluster.

Per ulteriori informazioni sulla rotazione delle chiavi, consultare [Rotazione delle chiavi di crittografia utilizzando la console di Amazon Redshift](#) e [Rotazione delle chiavi di crittografia con l'API di Amazon Redshift e la AWS CLI](#).

## Modifica della crittografia del cluster

Puoi modificare un cluster non crittografato per utilizzare la crittografia AWS Key Management Service (AWS KMS), utilizzando una chiave gestita o una chiave AWS gestita dal cliente. Quando modifichi il cluster per abilitare la AWS KMS crittografia, Amazon Redshift migra automaticamente i dati in un nuovo cluster crittografato. È anche possibile ripristinare un cluster non crittografato in un cluster crittografato modificando il cluster.

Durante l'operazione di migrazione, il cluster rimane disponibile in sola lettura e lo stato visualizzato sarà `resizing` (ridimensionamento).

Se il cluster è configurato per abilitare la copia di istantanee tra AWS regioni, è necessario disabilitarlo prima di modificare la crittografia. Per ulteriori informazioni, consultare [Copia di snapshot in un'altra regione AWS](#) e [Configura una copia delle istantanee tra regioni per un cluster crittografato AWS KMS](#). Non puoi abilitare la crittografia con il modulo di sicurezza hardware (HSM) modificando il cluster. Devi invece creare un nuovo cluster crittografato con HSM ed eseguire la migrazione dei dati al nuovo cluster. Per ulteriori informazioni, consulta [Migrazione a un cluster crittografato con HSM](#).

Per modificare la crittografia del database su un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster di cui si desidera modificare la crittografia.
3. Scegli Properties (Proprietà).
4. Nella sezione Configurazioni di database, scegliere Modifica, quindi Modifica crittografia.
5. Scegliere una delle opzioni di crittografia e selezionare Salva modifiche.

Per cambiare la crittografia del cluster con l'interfaccia a riga di comando

Per modificare il cluster non crittografato da utilizzare AWS KMS, `modify-cluster` esegui il comando CLI e `--encrypted` specifica, come illustrato di seguito. Per impostazione predefinita viene utilizzata la chiave KMS predefinita. Per specificare una chiave gestita dal cliente, includi l'opzione `--kms-key-id`.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id <value>
```

Per rimuovere la crittografia dal cluster, esegui questo comando della CLI.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

## Migrazione a un cluster crittografato con HSM

Per eseguire la migrazione di un cluster non crittografato a un cluster crittografato con un modulo di sicurezza hardware (HSM), crea un nuovo cluster crittografato e sposta i dati nel nuovo cluster. Non puoi eseguire la migrazione a un cluster crittografato con HSM modificando il cluster.

Per eseguire la migrazione da un cluster non crittografato a un cluster crittografato con HSM, devi prima scaricare i dati dal cluster di origine esistente. Ricarica quindi i dati in un nuovo cluster di destinazione con l'impostazione di crittografia scelta. Per ulteriori informazioni sull'avvio di un cluster crittografato, consultare [Crittografia dei database di Amazon Redshift](#).

Durante il processo di migrazione, il cluster di origine è disponibile per query di sola lettura fino all'ultima fase. L'ultima fase consiste nel rinominare i cluster di destinazione e di origine, scambiando gli endpoint in modo che il traffico venga instradato al nuovo cluster di destinazione. Il cluster di destinazione non è disponibile fino al riavvio successivo alla ridenominazione. Durante il trasferimento dei dati, sospendi qualsiasi caricamento dei dati e altre operazioni di scrittura nel cluster di origine.

### Preparativi per la migrazione

1. Identificare tutti i sistemi dipendenti che interagiscono con Amazon Redshift, ad esempio gli strumenti di business intelligence (BI) e i sistemi di estrazione, trasformazione e caricamento (ETL).
2. Identificare le query di convalida per testare la migrazione.

Ad esempio, è possibile usare la query seguente per trovare il numero di tabelle definite dall'utente.

```
select count(*)
from pg_table_def
where schemaname != 'pg_catalog';
```

La query seguente restituisce un elenco di tutte le tabelle definite dall'utente e il numero di righe in ogni tabella.

```
select "table", tbl_rows
from svv_table_info;
```

3. Scegliere un buon momento per la migrazione. Per trovare un momento in cui l'utilizzo del cluster è minimo, monitorare i parametri del cluster, come utilizzo della CPU e numero di connessioni al database. Per ulteriori informazioni, consultare [Visualizzazione di dati di prestazioni dei cluster](#).
4. Rimuovere le tabelle inutilizzate.

Per creare un elenco di tabelle che indichi anche il numero di volte in cui sono state eseguite query su ogni tabella, eseguire la query seguente.

```
select database,
schema,
table_id,
"table",
round(size::float/(1024*1024)::float,2) as size,
sortkey1,
nvl(s.num_qs,0) num_qs
from svv_table_info t
left join (select tbl,
perm_table_name,
count(distinct query) num_qs
from stl_scan s
where s.userid > 1
and s.perm_table_name not in ('Internal worktable','S3')
group by tbl,
perm_table_name) s on s.tbl = t.table_id
where t."schema" not in ('pg_internal');
```

5. Avviare un nuovo cluster crittografato.

Usare lo stesso numero di porta del cluster di destinazione come cluster di origine. Per ulteriori informazioni sull'avvio di un cluster crittografato, consultare [Crittografia dei database di Amazon Redshift](#).

6. Configurare il processo di scaricamento e caricamento.

Puoi utilizzare l'[utilità di scaricamento/copia di Amazon Redshift](#) per semplificare la migrazione di dati tra cluster. L'utilità esporta dati dal cluster di origine a una posizione in Amazon S3. I dati vengono crittografati con AWS KMS. L'utilità importa quindi automaticamente i dati nella destinazione. Facoltativamente, è possibile usare l'utilità per eseguire la pulizia di Amazon S3 al termine della migrazione.

7. Eseguire un test per verificare il processo e determinare il periodo di tempo per cui sospendere le operazioni di scrittura.

Durante le operazioni di scaricamento e caricamento dei dati, mantenere la coerenza dei dati sospendendo il caricamento dei dati e altre operazioni di scrittura. Usando una delle tabelle di dimensioni maggiori, eseguire il processo di scaricamento e caricamento per stimare i tempi.

8. Creare oggetti di database, come schemi, viste e tabelle. Per aiutarti a generare le istruzioni DDL (Data Definition Language) necessarie, puoi utilizzare gli script presenti [AdminViews](#) nel AWS GitHub repository.

Per eseguire la migrazione del cluster

1. Arrestare tutti i processi ETL nel cluster di origine.

Per verificare che non vi siano operazioni di scrittura in corso, usare la Console di gestione di Amazon Redshift per monitorare gli IOPS di scrittura. Per ulteriori informazioni, consultare [Visualizzazione di dati di prestazioni dei cluster](#).

2. Eseguire le query di convalida identificate in precedenza per raccogliere informazioni sul cluster di origine non crittografato prima della migrazione.
3. Facoltativo: creare una coda di gestione dei carichi di lavoro per usare il numero massimo di risorse disponibili sia nel cluster di origine sia nel cluster di destinazione. Ad esempio, creare una coda denominata `data_migrate` e configurarla con memoria al 95% e simultaneità 4. Per ulteriori informazioni, consultare [Routing di query su code basate su gruppi di utenti e gruppi di query](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
4. Utilizzando la `data_migrate` coda, esegui il `UnloadCopyUtility`

Monitorare i processi UNLOAD e COPY tramite la console Amazon Redshift.

5. Eseguire di nuovo le query di convalida e verificare che i risultati corrispondano a quelli del cluster di origine.
6. Rinominare i cluster di origine e di destinazione per scambiare gli endpoint. Per evitare interruzioni, eseguire questa operazione al di fuori dell'orario di ufficio.
7. Verificare di potersi connettere al cluster di destinazione usando tutti i client SQL, tra cui gli strumenti ETL e di creazione di report.
8. Arrestare il cluster di origine non crittografato.

## Configurazione della crittografia di database mediante la console

È possibile utilizzare la console Amazon Redshift per configurare Amazon Redshift per l'utilizzo di un modulo HSM e per ruotare le chiavi di crittografia. Per informazioni su come creare cluster utilizzando chiavi di AWS KMS crittografia, vedere [Creazione di un cluster](#) e [Gestione dei cluster utilizzando l'API AWS CLI Amazon Redshift](#).

Per modificare la crittografia del database su un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster per il quale spostare gli snapshot.
3. Alla voce Actions (Operazioni), scegli Modify (Modifica) per visualizzare la pagina di configurazione.
4. Nella sezione Database configuration (Configurazione database), scegli le impostazioni per la voce Encryption (Crittografia), quindi scegli Modify cluster (Modifica cluster).

## Rotazione delle chiavi di crittografia utilizzando la console di Amazon Redshift

Per ruotare le chiavi di crittografia utilizzando la console Amazon Redshift, procedere nel modo illustrato di seguito.

Per ruotare le chiavi crittografiche per un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster di cui aggiornare le chiavi di crittografia.
3. Alla voce Actions (Operazioni), scegli Rotate encryption (Ruota cifratura) per visualizzare la pagina Rotate encryption keys (Rotazione delle chiavi crittografiche).
4. Nella pagina Rotate encryption keys (Rotazione delle chiavi crittografiche), scegli Rotate encryption keys (Ruota chiavi crittografiche).

## Configurazione della crittografia di database con l'API di Amazon Redshift e la CLI AWS CLI

Utilizzare l'API Amazon Redshift e l'AWS Command Line Interface (AWS CLI) per configurare le opzioni delle chiavi di crittografia per i database Amazon Redshift. Per ulteriori informazioni sulla crittografia di database, consultare [Crittografia dei database di Amazon Redshift](#).

Configurazione di Amazon Redshift per l'utilizzo delle chiavi di crittografia AWS KMS con l'API di Amazon Redshift e AWS CLI

È possibile utilizzare le operazioni API di Amazon Redshift per configurare Amazon Redshift in modo da utilizzare le chiavi di crittografia di AWS KMS.

- [CreateCluster](#)
- [CreateSnapshotCopyGrant](#)
- [DescribeSnapshotCopyGrants](#)
- [DeleteSnapshotCopyGrant](#)
- [DisableSnapshotCopy](#)
- [EnableSnapshotCopy](#)

È possibile utilizzare le seguenti operazioni della CLI di Amazon Redshift per configurare Amazon Redshift in modo da utilizzare le chiavi di crittografia di AWS KMS.

- [create-cluster](#)
- [create-snapshot-copy-grant](#)
- [describe-snapshot-copy-grants](#)
- [delete-snapshot-copy-grant](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)

Configurazione di Amazon Redshift per l'utilizzo di un HSM con l'API di Amazon Redshift e AWS CLI

È possibile utilizzare le seguenti operazioni API di Amazon Redshift per gestire i moduli di sicurezza hardware (HSM).

- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)

- [DeleteHsmClientCertificate](#)
- [DeleteHsmConfiguration](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

Puoi utilizzare le seguenti operazioni dell'AWS CLI per gestire i moduli di protezione hardware.

- [create-hsm-client-certificate](#)
- [create-hsm-configuration](#)
- [delete-hsm-client-certificate](#)
- [delete-hsm-configuration](#)
- [describe-hsm-client-certificates](#)
- [describe-hsm-configurations](#)

Rotazione delle chiavi di crittografia con l'API di Amazon Redshift e la AWS CLI

È possibile utilizzare le seguenti operazioni API di Amazon Redshift per eseguire la rotazione delle chiavi di crittografia.

- [RotateEncryptionKey](#)

Puoi utilizzare le seguenti operazioni dell'AWS CLI per eseguire la rotazione delle chiavi di crittografia.

- [rotate-encryption-key](#)

## Crittografia in transito

Puoi configurare l'ambiente per proteggere la riservatezza e l'integrità dei dati in transito.

La crittografia dei dati in transito tra un cluster Amazon Redshift e i client SQL tramite JDBC/ODBC:

- È possibile connettersi ai cluster Amazon Redshift dagli strumenti del client SQL tramite le connessioni Java Database Connectivity (JDBC) e Open Database Connectivity (ODBC).
- Amazon Redshift supporta le connessioni Secure Sockets Layer (SSL) per crittografare i dati e i certificati server per convalidare il certificato del server a cui si connette il client. Il client si

connette al nodo principale di un cluster Amazon Redshift. Per ulteriori informazioni, consultare [Configurazione delle opzioni di sicurezza per le connessioni](#).

- Per supportare le connessioni SSL, Amazon Redshift crea e installa certificati emessi da AWS Certificate Manager (ACM) su ciascun cluster. Per ulteriori informazioni, consultare [Passaggio ai certificati ACM per connessioni SSL](#).
- Per proteggere i dati in transito all'interno di AWS Cloud, Amazon Redshift utilizza la tecnologia SSL accelerata via hardware per comunicare con Amazon S3 o Amazon DynamoDB per COPY, UNLOAD e le operazioni di backup e ripristino.

Crittografia dei dati in transito tra un cluster Amazon Redshift e Amazon S3 o DynamoDB:

- Amazon Redshift utilizza la tecnologia SSL accelerata via hardware per comunicare con Amazon S3 o DynamoDB per le operazioni COPY, UNLOAD, di backup e di ripristino.
- Redshift Spectrum supporta la crittografia lato server (SSE) di Amazon S3 utilizzando la chiave predefinita dell'account gestita da AWS Key Management Service (KMS).
- Crittografare i carichi di Amazon Redshift con Amazon S3 e AWS KMS. Per ulteriori informazioni, consultare [Crittografia dei carichi Amazon Redshift con Amazon S3 e AWS KMS](#).

La crittografia e la firma dei dati in transito tra la AWS CLI, SDK o client API ed endpoint Amazon Redshift:

- Amazon Redshift fornisce endpoint HTTPS per la crittografia dei dati in transito.
- Per proteggere l'integrità delle richieste API ad Amazon Redshift, le chiamate API devono essere firmate dal chiamante. Le chiamate sono firmate da un certificato X.509 o dalla chiave di accesso segreta AWS del cliente secondo il processo di firma di Signature Version 4 (Sigv4). Per ulteriori informazioni, consulta [Processo di firma Signature Version 4](#) in Riferimenti generali di AWS.
- Utilizzare la AWS CLI o uno degli SDK AWS per effettuare richieste ad AWS. Questi strumenti firmano automaticamente le tue richieste con la chiave di accesso specificata al momento della configurazione.

Crittografia dei dati in transito tra i cluster Amazon Redshift e il query editor v2 di Amazon Redshift

- I dati vengono trasmessi tra il query editor v2 e i cluster Amazon Redshift su un canale crittografato TLS.

## Gestione delle chiavi

Puoi configurare il tuo ambiente per proteggere i dati con le chiavi.

- Amazon Redshift si integra automaticamente con AWS Key Management Service (AWS KMS) per la gestione delle chiavi. AWS KMS utilizza la crittografia envelope. Per ulteriori informazioni, consultare [Crittografia envelope](#).
- Quando le chiavi di crittografia vengono gestite in AWS KMS, Amazon Redshift utilizza un'architettura basata su chiavi, a quattro livelli per la crittografia. L'architettura consiste in chiavi di crittografia dei dati AES-256 generate casualmente, una chiave di database, una chiave del cluster e una chiave root. Per ulteriori informazioni, consultare [Come Amazon Redshift utilizza AWS KMS](#).
- È possibile creare la propria chiave gestita dal cliente in AWS KMS. Per ulteriori informazioni, consultare [Creazione di chiavi](#).
- Puoi anche importare il tuo materiale sulla chiave per le nuove AWS KMS keys. Per ulteriori informazioni, consultare [Importazione del materiale della chiave in AWS Key Management Service \(AWS KMS\)](#).
- Amazon Redshift supporta la gestione delle chiavi di crittografia nei moduli di sicurezza hardware (HSM). L'HSM può essere on-premise o AWS CloudHSM. Quando si utilizza un modulo di sicurezza hardware (HSM), è necessario usare certificati client e server per configurare una connessione attendibile tra Amazon Redshift e il modulo di sicurezza hardware (HSM). Amazon Redshift supporta solo AWS CloudHSM Classic per la gestione delle chiavi. Per ulteriori informazioni, consulta [Crittografia per Amazon Redshift tramite moduli di sicurezza hardware \(HSM\)](#). Per informazioni su AWS CloudHSM, consultare [Che cos'è AWS CloudHSM?](#).
- Puoi eseguire la rotazione delle chiavi di crittografia per cluster crittografati. Per ulteriori informazioni, consultare [Rotazione delle chiavi di crittografia in Amazon Redshift](#).

## Tokenizzazione dei dati

La tokenizzazione è il processo di sostituzione dei valori effettivi con valori opachi per scopi di sicurezza dei dati. Le applicazioni sensibili alla sicurezza utilizzano la tokenizzazione per sostituire i dati sensibili come le informazioni personali (PII) o i dati sanitari protetti (PHI) con token per ridurre i rischi per la sicurezza. La detokenizzazione ri-sostituisce i token con valori effettivi per gli utenti autorizzati con policy di sicurezza appropriati.

Per l'integrazione con servizi di tokenizzazione di terze parti, è possibile utilizzare le funzioni definite dall'utente (UDF) di Amazon Redshift create utilizzando [AWS Lambda](#). Per ulteriori informazioni,

consultare [Funzioni Lambda definite dall'utente](#) nella Guida per gli sviluppatori di Amazon Redshift. Ad esempio, consultare [Protezione](#).

Amazon Redshift invia richieste di tokenizzazione a un server di tokenizzazione a cui si accede tramite un'API REST o un endpoint predefinito. Due o più funzioni Lambda gratuite elaborano le richieste di tokenizzazione e detokenizzazione. Per questa elaborazione, è possibile utilizzare le funzioni Lambda fornite da un provider di tokenizzazione di terze parti. È possibile utilizzare anche le funzioni Lambda che vengono registrate come funzioni Lambda definite dall'utente in Amazon Redshift.

Si supponga, ad esempio, che venga inviata una query che richiami una funzione definita dall'utente di tokenizzazione o detokenizzazione in una colonna. Il cluster Amazon Redshift esegue lo spool delle righe di argomenti applicabili e invia tali righe in batch alla funzione Lambda in parallelo. I dati vengono trasferiti tra i nodi di calcolo Amazon Redshift e Lambda in una connessione di rete isolata separata che non è accessibile ai client. La funzione Lambda passa i dati all'endpoint del server di tokenizzazione. Il server di tokenizzazione tokenizza o detokenizza i dati, se necessario, e li restituisce. Le funzioni Lambda quindi trasmettono i risultati al cluster Amazon Redshift per ulteriori elaborazioni, se necessario, e poi restituiscono i risultati della query.

## Riservatezza del traffico Internet

Per instradare il traffico tra Amazon Redshift e i client e le applicazioni su una rete aziendale:

- Configurare una connessione privata tra il cloud privato virtuale (VPC, Virtual Private Cloud) e la rete aziendale. Configurare una connessione VPN IPsec su Internet oppure una connessione fisica privata che utilizza una connessione AWS Direct Connect. AWS Direct Connect consente di stabilire un'interfaccia privata virtuale tra la rete on-premise direttamente su Amazon VPC, creando una connessione di rete privata e ad elevata larghezza di banda tra la rete e il VPC. Grazie all'utilizzo di diverse interfacce virtuali, puoi anche stabilire una connessione privata tra diversi cloud privati virtuali conservando l'isolamento di rete. Per ulteriori informazioni, consultare [Che cos'è AWS Site-to-Site VPN?](#) e [Che cos'è AWS Direct Connect?](#)

Per instradare il traffico tra un cluster Amazon Redshift in un VPC e i bucket Amazon S3 nella stessa regione AWS:

- Configurare un endpoint VPC privato Amazon S3 per accedere ai dati Amazon S3 in forma privata da un comando load o unload ETL. Per ulteriori informazioni, consultare [Endpoint per Amazon S3](#).

- Abilitare "Routing VPC avanzato" per un cluster Amazon Redshift, specificando un endpoint VPC di Amazon S3 di destinazione. Il traffico generato mediante i comandi COPY, UNLOAD o CREATE LIBRARY di Amazon Redshift viene quindi instradato tramite endpoint privato. Per ulteriori informazioni, consultare [Routing VPC avanzato](#).

## Identity and Access Management in Amazon Redshift

L'accesso ad Amazon Redshift richiede credenziali che AWS possono essere utilizzate per autenticare le tue richieste. Tali credenziali devono disporre delle autorizzazioni per accedere a AWS risorse, come un cluster Amazon Redshift. Nelle sezioni seguenti vengono fornite informazioni su come utilizzare [AWS Identity and Access Management \(IAM\)](#) ed Amazon Redshift per proteggere le risorse tramite il controllo degli accessi:

- [Autenticazione con identità](#)
- [Controllo accessi](#)

### Important

Questo argomento contiene una raccolta di best practice per la gestione di autorizzazioni, identità e accesso sicuri. Si consiglia di acquisire familiarità con le best practice per l'utilizzo di IAM con Amazon Redshift. Queste includono l'utilizzo dei ruoli IAM per l'applicazione delle autorizzazioni. Una buona conoscenza di queste sezioni aiuterà a mantenere un data warehouse Amazon Redshift più sicuro.

## 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 principale. 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.

## Controllo accessi

Per autenticare le richieste, è necessario disporre di credenziali valide, ma a meno che non si disponga delle autorizzazioni non è possibile creare o accedere a risorse Amazon Redshift. Ad esempio, devi avere le autorizzazioni necessarie per la creazione di un cluster Amazon Redshift, la creazione di uno snapshot, l'aggiunta della sottoscrizione di un evento e così via.

Nelle sezioni seguenti viene descritto come gestire le autorizzazioni per Amazon Redshift. Consigliamo di leggere prima la panoramica.

- [Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Redshift](#)
- [Utilizzo di policy basate su identità \(policy IAM\) per Amazon Redshift](#)

## Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Redshift

Ogni AWS risorsa è di proprietà di un AWS account e le autorizzazioni per creare o accedere alle risorse sono regolate da politiche di autorizzazione. Un amministratore di account può allegare politiche di autorizzazione alle identità IAM (ovvero utenti, gruppi e ruoli) e alcuni servizi (come AWS Lambda) supportano anche l'associazione di politiche di autorizzazione alle risorse.

### Note

Un amministratore account (o un utente amministratore) è un utente con privilegi di amministratore. Per ulteriori informazioni, consultare la sezione [best practice IAM](#) nella Guida per l'utente IAM.

Nel concedere le autorizzazioni, devi stabilire chi ottiene le autorizzazioni, per quali risorse concedere le autorizzazioni e le operazioni specifiche che vuoi permettere su tali risorse.

## Risorse e operazioni di Amazon Redshift

Amazon Redshift fornisce operazioni e chiavi di contesto della condizione specifiche del servizio per l'utilizzo in policy delle autorizzazioni IAM.

## Autorizzazioni di accesso per Amazon Redshift, Amazon Redshift Serverless, l'API dati di Amazon Redshift e l'Editor di query Amazon Redshift v2

Quando si configura [Controllo accessi](#), si scrivono policy di autorizzazione che è possibile collegare a un'identità IAM (policy basate sull'identità). Per ulteriori informazioni, consultare gli argomenti seguenti nella Referenza sull'autorizzazione del servizio:

- Per Amazon Redshift consulta [Operazioni, risorse e chiavi di condizione per Amazon Redshift](#) che utilizzano il prefisso `redshift:`.
- Per Amazon Redshift serverless consulta [Operazioni, risorse e chiavi di condizione per Amazon Redshift serverless](#) che utilizzano il prefisso `redshift-serverless:`.
- Per l'API dati di Amazon Redshift consulta [Operazioni, risorse e chiavi di condizione per l'API dati di Amazon Redshift](#) che utilizzano il prefisso `redshift-data:`.
- Per l'editor di query di Amazon Redshift v2, consulta [Azioni, risorse e chiavi di condizione per AWS SQL Workbench \(Amazon Redshift query editor v2\)](#) che utilizzano il prefisso `sqlworkbench:`.

L'editor di query v2 include operazioni di sola autorizzazione che non corrispondono direttamente a un'operazione API. Queste operazioni sono indicate nella Guida di riferimento per l'autorizzazione al servizio con `[permission only]`.

La Guida di riferimento per l'autorizzazione al servizio contiene informazioni su quali operazioni API possono essere utilizzate in una policy IAM. Include anche la AWS risorsa per la quale puoi concedere le autorizzazioni e le chiavi di condizione che puoi includere per un controllo granulare degli accessi. Per ulteriori informazioni sulle condizioni, consulta [Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi](#).

Le operazioni, il valore della risorsa e le condizioni vengono specificati rispettivamente nei campi `Action`, `Resource` e `Condition` della policy. Per specificare un'operazione per Amazon Redshift, utilizza il prefisso `redshift:` seguito dal nome dell'operazione API (ad esempio, `redshift:CreateCluster`).

## Informazioni sulla proprietà delle risorse

Il proprietario della risorsa è l'AWS account che ha creato una risorsa. Cioè, il proprietario della risorsa è l'AWS account dell'entità principale (l'account root, un utente IAM o un ruolo IAM) che autentica la richiesta che crea la risorsa. Negli esempi seguenti viene illustrato il funzionamento:

- Se utilizzi le credenziali dell'account root del tuo AWS account per creare un cluster DB, l' AWS account è il proprietario della risorsa Amazon Redshift.
- Se crei un ruolo IAM nel tuo AWS account con le autorizzazioni per creare risorse Amazon Redshift, chiunque possa assumere il ruolo può creare risorse Amazon Redshift. L'account AWS a cui appartiene il ruolo è il proprietario delle risorse Amazon Redshift.
- Se crei un utente IAM nel tuo AWS account e concedi le autorizzazioni per creare risorse Amazon Redshift a quell'utente, l'utente può creare risorse Amazon Redshift. Tuttavia, il tuo AWS account, a cui appartiene l'utente, possiede le risorse di Amazon Redshift. Nella maggior parte dei casi questo metodo non è consigliato. Ti suggeriamo di creare un ruolo IAM, collegare le autorizzazioni al ruolo e quindi assegnare il ruolo a un utente.

## Gestione dell'accesso alle risorse

Una policy di autorizzazioni descrive chi ha accesso a cosa. Nella sezione seguente vengono descritte le opzioni disponibili per la creazione di policy relative alle autorizzazioni.

### Note

In questa sezione viene descritto IAM nel contesto di Amazon Redshift. Non vengono fornite informazioni dettagliate sul servizio IAM. Per la documentazione di IAM completa, consulta la pagina [Che cos'è IAM?](#) nella Guida per l'utente di IAM. Per informazioni sulla sintassi delle policy IAM e le rispettive descrizioni, consultare [Riferimento alle policy IAM di AWS](#) nella Guida per l'utente di IAM.

Le policy collegate a un'identità IAM vengono definite policy basate su identità (policy IAM), mentre quelle collegate a una risorsa vengono definite policy basate su risorse. Amazon Redshift supporta solo policy basate su identità (policy IAM).

### Policy basate su identità (policy IAM)

Puoi assegnare le autorizzazioni collegando le policy a un ruolo IAM e quindi assegnando il ruolo a un utente o un gruppo. Di seguito è riportato un esempio di policy contenente le autorizzazioni per creare, eliminare, modificare e riavviare i cluster Amazon Redshift per il tuo account. AWS

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

```
{
  "Sid": "AllowManageClusters",
  "Effect": "Allow",
  "Action": [
    "redshift:CreateCluster",
    "redshift>DeleteCluster",
    "redshift:ModifyCluster",
    "redshift:RebootCluster"
  ],
  "Resource": "*"
}
```

Per ulteriori informazioni sull'uso di policy basate su identità con Amazon Redshift, consultare [Utilizzo di policy basate su identità \(policy IAM\) per Amazon Redshift](#). Per ulteriori informazioni su utenti, gruppi, ruoli e autorizzazioni, consultare [Identità \(utenti, gruppi e ruoli\)](#) nella Guida per l'utente di IAM.

## Policy basate su risorse

Anche altri servizi, ad esempio Amazon S3, supportano policy di autorizzazioni basate su risorse. Ad esempio, è possibile associare una policy a un bucket S3 per gestire le autorizzazioni di accesso a quel bucket. Amazon Redshift non supporta le policy basate su risorse.

## Specifica degli elementi delle policy: operazioni, effetti, risorse ed entità

Per ogni risorsa Amazon Redshift (consultare [Risorse e operazioni di Amazon Redshift](#)), il servizio definisce un insieme di operazioni API (consultare [Operazioni](#)). Per concedere le autorizzazioni per queste operazioni API, Amazon Redshift definisce un set di operazioni che possono essere specificate in una policy. L'esecuzione di un'operazione API può richiedere le autorizzazioni per più di un'operazione.

Di seguito sono elencati gli elementi di base di una policy:

- **Risorsa:** in una policy si utilizza il nome della risorsa Amazon (ARN) per identificare la risorsa a cui si applica la policy stessa. Per ulteriori informazioni, consulta [Risorse e operazioni di Amazon Redshift](#).
- **Operazione:** utilizzi le parole chiave per identificare le operazioni sulla risorsa da permettere o rifiutare. Ad esempio, l'autorizzazione `redshift:DescribeClusters` concede all'utente le autorizzazioni per eseguire l'operazione `DescribeClusters` di Amazon Redshift.

- **Effetto:** l'effetto prodotto quando l'utente richiede l'operazione specifica, ovvero un'autorizzazione o un rifiuto. USe non concedi esplicitamente (consenti) l'accesso a una risorsa, l'accesso viene implicitamente rifiutato. Puoi anche rifiutare esplicitamente l'accesso a una risorsa per garantire che un utente non possa accedervi, anche se l'accesso viene concesso da un'altra policy.
- **Principale -** Nelle policy basate su identità (policy IAM), l'utente a cui la policy è collegata è il principale implicito. Per policy basate su risorse, specifichi l'utente, l'account, il servizio o un'altra entità che desideri riceva le autorizzazioni (si applica solo alle policy basate su risorse). Amazon Redshift non supporta le policy basate su risorse.

Per ulteriori informazioni sulla sintassi e le descrizioni delle policy IAM, consultare [AWS Riferimento alle policy IAM](#) nella Guida per l'utente di IAM.

Per una tabella che mostra tutte le operazioni API Amazon Redshift e le risorse a cui si applicano, consultare [Autorizzazioni di accesso per Amazon Redshift, Amazon Redshift Serverless, l'API dati di Amazon Redshift e l'Editor di query Amazon Redshift v2](#).

## Specifiche delle condizioni in una policy

Quando concedi le autorizzazioni, puoi utilizzare la sintassi della policy di accesso per specificare le condizioni in base a cui la policy deve essere applicata. Ad esempio, potresti decidere che una policy venga applicata solo dopo una data specifica. Per ulteriori informazioni su come specificare le condizioni nella sintassi della/e policy di accesso, consultare [Elementi delle policy JSON IAM: Condizione](#) nella Guida per l'utente di IAM.

Per identificare le condizioni in cui viene applicata una policy di autorizzazioni, includi un elemento `Condition` nella policy di autorizzazioni IAM. Ad esempio, puoi creare una policy che permette a un utente di creare un cluster tramite l'operazione `redshift:CreateCluster` e puoi aggiungere un elemento `Condition` per limitare la creazione del cluster da parte dell'utente a una sola regione specifica. Per informazioni dettagliate, vedi [Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi](#). Per un elenco che mostra tutti i valori delle chiavi di condizione e le operazioni e le risorse di Amazon Redshift a cui si applicano, consultare [Autorizzazioni di accesso per Amazon Redshift, Amazon Redshift Serverless, l'API dati di Amazon Redshift e l'Editor di query Amazon Redshift v2](#).

### Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi

In Amazon Redshift puoi usare chiavi di condizione per limitare l'accesso alle risorse in base ai tag per queste risorse. Di seguito sono riportate le chiavi di condizione di Amazon Redshift più comuni.

Chiave di condizione	Descrizione
<code>aws:RequestTag</code>	Richiede che gli utenti includano la chiave (nome) e il valore di un tag ogni volta che creano una risorsa. Per ulteriori informazioni, consulta <a href="#">aws: RequestTag</a> nella IAM User Guide.
<code>aws:ResourceTag</code>	Limita l'accesso utente alle risorse in base a chiavi e valori di tag specifici . Per ulteriori informazioni, consulta <a href="#">aws: ResourceTag</a> nella Guida per l'utente IAM.
<code>aws:TagKeys</code>	Utilizzare questa chiave per confrontare le chiavi dei tag in una richiesta con quelle specificate nella policy. Per ulteriori informazioni, consulta <a href="#">aws: TagKeys</a> nella Guida per l'utente IAM.

Per informazioni sui tag, consultare [Panoramica del tagging](#).

Per un elenco di operazioni API che supportano le chiavi di condizione `redshift:RequestTag` e `redshift:ResourceTag`, consultare [Autorizzazioni di accesso per Amazon Redshift, Amazon Redshift Serverless, l'API dati di Amazon Redshift e l'Editor di query Amazon Redshift v2](#).

Le seguenti chiavi di condizione possono essere utilizzate con l'azione Amazon Redshift `GetClusterCredentials`.

Chiave di condizione	Descrizione
<code>redshift:DurationSeconds</code>	Limita il numero di secondi che possono essere specificati per la durata.
<code>redshift:DbName</code>	Limita i nomi di database che possono essere specificati.
<code>redshift:DbUser</code>	Limita i nomi degli utenti del database che possono essere specificati.

Esempio 1: limitazione dell'accesso utilizzando la chiave `aws:condition ResourceTag`

Utilizza la seguente policy IAM per consentire a un utente di modificare un cluster Amazon Redshift solo per un AWS account specifico nella `us-west-2` regione con un tag denominato `environment` con un valore di tag di `test`

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowModifyTestCluster",
    "Effect": "Allow",
    "Action": "redshift:ModifyCluster",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:cluster:*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/environment": "test"
      }
    }
  }
}
```

## Esempio 2: limitazione dell'accesso utilizzando la chiave aws: condition RequestTag

Utilizza la policy IAM seguente per permettere a un utente di creare un cluster Amazon Redshift solo se il comando per creare il cluster include un tag denominato usage con un valore di tag production. La condizione con `aws:TagKeys` e il modificatore `ForAllValues` specifica che solo le chiavi `costcenter` e `usage` possono essere specificate nella richiesta.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "AllowCreateProductionCluster",
    "Effect": "Allow",
    "Action": [
      "redshift:CreateCluster",
      "redshift:CreateTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/usage": "production"
      },
      "ForAllValues:StringEquals": {
        "aws:TagKeys": [
          "costcenter",
          "usage"
        ]
      }
    }
  }
}
```

```

    }
  }
}

```

## Utilizzo di policy basate su identità (policy IAM) per Amazon Redshift

In questo argomento vengono forniti esempi di policy basate su identità in cui un amministratore account può collegare policy di autorizzazione a identità IAM, ovvero utenti, gruppi e ruoli.

### Important

In primo luogo, è consigliabile esaminare gli argomenti introduttivi in cui vengono spiegati i concetti di base e le opzioni disponibili per gestire l'accesso alle risorse di Amazon Redshift. Per ulteriori informazioni, consulta [Panoramica della gestione delle autorizzazioni di accesso alle risorse di Amazon Redshift](#).

Di seguito viene illustrato un esempio di policy di autorizzazione. La policy consente a un utente di creare, eliminare, modificare e riavviare tutti i cluster, quindi nega l'autorizzazione a eliminare o modificare tutti i cluster in cui l'identificatore del cluster inizia con and. production Regione AWS us-west-2 Account AWS 123456789012

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "DenyDeleteModifyProtected",
      "Action": [

```

```
        "redshift:DeleteCluster",
        "redshift:ModifyCluster"
    ],
    "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:production*"
    ],
    "Effect": "Deny"
}
]
```

La policy include due dichiarazioni:

- La prima istruzione concede le autorizzazioni a un utente per la creazione, l'eliminazione, la modifica e il riavvio di cluster. L'istruzione specifica un carattere jolly (\*) come Resource valore in modo che la policy si applichi a tutte le risorse Amazon Redshift di proprietà dell'account root. AWS
- La seconda istruzione nega l'autorizzazione per l'eliminazione o la modifica di un cluster. L'istruzione specifica per il valore Resource l'Amazon Resource Name (ARN) di un cluster che include un carattere jolly (\*). Di conseguenza, questa dichiarazione si applica a tutti i cluster Amazon Redshift di proprietà dell' AWS account root da cui inizia l'identificatore del cluster. production

## AWS politiche gestite per Amazon Redshift

AWS affronta molti casi d'uso comuni fornendo politiche IAM autonome create e amministrare da. AWS Le policy gestite concedono le autorizzazioni necessarie per i casi di utilizzo comune in modo da non dover cercare quali sono le autorizzazioni richieste. Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Puoi anche creare policy IAM personalizzate per concedere autorizzazioni per risorse e operazioni API Amazon Redshift. Puoi collegare queste policy personalizzate ai ruoli o ai gruppi IAM che richiedono le autorizzazioni.

Le seguenti sezioni descrivono le politiche AWS gestite, che puoi allegare agli utenti del tuo account e sono specifiche per Amazon Redshift.

### AmazonRedshiftReadOnlyAccesso

Garantisce l'accesso in sola lettura a tutte le risorse Amazon Redshift per un account. AWS

Puoi trovare la policy di [AmazonRedshiftReadOnlyaccesso](#) sulla console IAM e [AmazonRedshiftReadOnlyAccess](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftFullAccess

Garantisce l'accesso completo a tutte le risorse Amazon Redshift per AWS un account. Inoltre, questa policy consente l'accesso completo a tutte le risorse di Amazon Redshift Serverless.

Puoi trovare la [AmazonRedshiftFullAccess](#) policy sulla console IAM e [AmazonRedshiftFullAccess](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftQueryEditor

Concede l'accesso completo all'editor di query nella console Amazon Redshift.

Puoi trovare la [AmazonRedshiftQueryEditor](#) policy sulla console IAM e [AmazonRedshiftQueryEditor](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftDataFullAccesso

Garantisce l'accesso completo alle operazioni e alle risorse dell'Amazon Redshift Data API per AWS un account.

Puoi trovare la policy di [AmazonRedshiftDataFullaccesso](#) sulla console IAM e [AmazonRedshiftDataFullAccess](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftQueryEditorV2 FullAccess

Consente l'accesso completo alle operazioni e alle risorse dell'editor di query v2 di Amazon Redshift. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti.

Puoi trovare la FullAccess policy [AmazonRedshiftQueryEditorV2](#) sulla console IAM e la [AmazonRedshiftQueryEditorV2 FullAccess](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftQueryEditorV2 NoSharing

Concede la possibilità di lavorare con l'editor di query v2 di Amazon Redshift senza condividere le risorse. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Il principale che utilizza questa policy non può taggare le sue risorse (ad esempio le query) per condividerle con altre entità nello stesso Account AWS.

Puoi trovare la NoSharing policy [AmazonRedshiftQueryEditorV2](#) sulla console IAM e la [AmazonRedshiftQueryEditorV2 NoSharing](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftQueryEditorV2 ReadSharing

Concede la possibilità di lavorare con l'editor di query v2 di Amazon Redshift con una condivisione limitata di risorse. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Il principale che utilizza questa policy può taggare le sue risorse (come le query) per condividerle con altri principali nello stesso Account AWS. Il principale concesso può leggere le risorse condivise con il suo team ma non può aggiornarle.

Puoi trovare la ReadSharing policy [AmazonRedshiftQueryEditorV2](#) sulla console IAM e la [AmazonRedshiftQueryEditorV2 ReadSharing](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftQueryEditorCondivisione V2 ReadWrite

Concede la possibilità di lavorare con l'editor di query v2 di Amazon Redshift condividendo le risorse. Questa policy inoltre garantisce l'accesso ad altri servizi richiesti. Il principale che utilizza questa policy può taggare le sue risorse (come le query) per condividerle con altri principali nello stesso Account AWS. Il principale concesso può leggere e aggiornare le risorse condivise con il suo team.

Puoi trovare la policy di [ReadWritecondivisione AmazonRedshift QueryEditor V2](#) sulla console IAM e la condivisione [AmazonRedshiftQueryEditorV2 nella AWS Managed Policy ReadWrite Reference Guide](#).

## AmazonRedshiftServiceLinkedRolePolicy

Non puoi collegarti AmazonRedshiftServiceLinkedRolePolicy alle tue entità IAM. Questa policy è allegata a un ruolo collegato al servizio che consente ad Amazon Redshift di accedere alle risorse dell'account. Per ulteriori informazioni, consultare [Utilizzo di ruoli collegati ai servizi per Amazon Redshift](#).

Puoi trovare la [AmazonRedshiftServiceLinkedRolePolicy](#) policy sulla console IAM e [AmazonRedshiftServiceLinkedRolePolicy](#) nella AWS Managed Policy Reference Guide.

## AmazonRedshiftAllCommandsFullAccess

Consente di utilizzare il ruolo IAM creato dalla console Amazon Redshift e impostarlo come predefinito per far eseguire al cluster la COPIA tramite i comandi di Amazon S3, SCARICARE, CREA FUNZIONE ESTERNA, CREA TABELLA ESTERNA, CREA SCHEMA ESTERNO e CREA MODELLO. La policy concede inoltre le autorizzazioni per eseguire istruzioni SELECT per servizi correlati, come Amazon S3, CloudWatch Logs, Amazon o. SageMaker AWS Glue

Puoi trovare la [AmazonRedshiftAllCommandsFullAccess](#) policy sulla console IAM e [AmazonRedshiftAllCommandsFullAccess](#) nella AWS Managed Policy Reference Guide.

Puoi anche creare policy IAM personalizzate per concedere autorizzazioni per risorse e operazioni API Amazon Redshift. Puoi collegare queste policy personalizzate ai ruoli o ai gruppi IAM che richiedono le autorizzazioni.

## Amazon Redshift si aggiorna alle AWS politiche gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Redshift da quando questo servizio ha iniziato a tracciare queste modifiche. Per gli avvisi automatici sulle modifiche apportate a questa pagina, sottoscrivere il feed RSS nella pagina della cronologia dei documenti di Amazon Redshift.

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 FullAccess</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>redshift-serverless:ListNamespaces</code> e <code>redshift-serverless:ListWorkgroups</code> viene aggiunta alla policy gestita. La loro aggiunta consente di elencare namespace e gruppi di lavoro serverless nel data warehouse di Amazon Redshift.	21 febbraio 2024
<a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>redshift-serverless:ListNamespaces</code> e <code>redshift-serverless:ListWorkgroups</code> viene aggiunta alla policy gestita. La loro	21 febbraio 2024

Modifica	Descrizione	Data
	aggiunta consente di elencare namespace e gruppi di lavoro serverless nel data warehouse di Amazon Redshift.	
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>redshift-serverless:ListNamespaces</code> e <code>redshift-serverless:ListWorkgroups</code> viene aggiunta alla policy gestita. La loro aggiunta consente di elencare namespace e gruppi di lavoro serverless nel data warehouse di Amazon Redshift.	21 febbraio 2024
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>redshift-serverless:ListNamespaces</code> e <code>redshift-serverless:ListWorkgroups</code> viene aggiunta alla policy gestita. La loro aggiunta consente di elencare namespace e gruppi di lavoro serverless nel data warehouse di Amazon Redshift.	21 febbraio 2024

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftReadOnlyAccess</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>redshift:ListRecommendations</code> viene aggiunta alla policy gestita. Ciò concede l'autorizzazione a elencare i consigli di Amazon Redshift Advisor.	7 febbraio 2024
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>ec2:AssignIpv6Addresses</code> e <code>ec2:UnassignIpv6Addresses</code> viene aggiunta alla policy gestita. L'aggiunta di tali operazioni consente di assegnare e annullare l'assegnazione degli indirizzi IP.	31 ottobre 2023
<a href="#">AmazonRedshiftQueryEditorV2NoSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>sqlworkbench:GetAutocompletionMetadata</code> e <code>sqlworkbench:GetAutocompletionResource</code> viene aggiunta alla policy gestita. La loro aggiunta concede l'autorizzazione a generare e recuperare le informazioni del database per il completamento automatico di SQL durante la modifica delle query.	16 agosto 2023

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>sqlworkbench:GetAutocompletionMetadata</code> e <code>sqlworkbench:GetAutocompletionResource</code> viene aggiunta alla policy gestita. La loro aggiunta concede l'autorizzazione a generare e recuperare le informazioni del database per il completamento automatico di SQL durante la modifica delle query.	16 agosto 2023
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	L'autorizzazione per le operazioni <code>sqlworkbench:GetAutocompletionMetadata</code> e <code>sqlworkbench:GetAutocompletionResource</code> viene aggiunta alla policy gestita. La loro aggiunta concede l'autorizzazione a generare e recuperare le informazioni del database per il completamento automatico di SQL durante la modifica delle query.	16 agosto 2023

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	<p>Le autorizzazioni per le azioni volte AWS Secrets Manager a creare e gestire i segreti vengono aggiunte alla policy gestita. Le autorizzazioni aggiunte sono le seguenti:</p> <ul style="list-style-type: none"><li>• <code>secretsmanager:GetRandomPassword</code></li><li>• <code>secretsmanager:DescribeSecret</code></li><li>• <code>secretsmanager:PutSecretValue</code></li><li>• <code>secretsmanager:UpdateSecret</code></li><li>• <code>secretsmanager:UpdateSecretVersionStage</code></li><li>• <code>secretsmanager:RotateSecret</code></li><li>• <code>secretsmanager&gt;DeleteSecret</code></li></ul>	14 agosto 2023

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	<p>Le autorizzazioni per le operazioni su Amazon EC2 per la creazione e la gestione delle regole dei gruppi di sicurezza e di instradamento vengono rimosse dalla policy gestita. Queste autorizzazioni riguardavano la creazione di sottoreti e VPC. Le autorizzazioni rimosse sono le seguenti:</p> <ul style="list-style-type: none"><li>• <code>ec2:AuthorizeSecurityGroupEgress</code></li><li>• <code>ec2:AuthorizeSecurityGroupIngress</code></li><li>• <code>ec2:UpdateSecurityGroupRuleDescriptionsEgress</code></li><li>• <code>ec2:ReplaceRouteTableAssociation</code></li><li>• <code>ec2:CreateRouteTable</code></li><li>• <code>ec2:AttachInternetGateway</code></li><li>• <code>ec2:UpdateSecurityGroupRuleDescriptionsIngress</code></li><li>• <code>ec2:AssociateRouteTable</code></li><li>• <code>ec2:RevokeSecurityGroupIngress</code></li><li>• <code>ec2:CreateRoute</code></li></ul>	8 maggio 2023

Modifica	Descrizione	Data
	<ul style="list-style-type: none"><li>• ec2:CreateSecurityGroup</li><li>• ec2:RevokeSecurityGroupEgress</li><li>• ec2:ModifyVpcAttribute</li><li>• ec2:CreateSubnet</li><li>• ec2:CreateInternetGateway</li><li>• ec2:CreateVpc</li></ul> <p>Queste erano associate al tag Purpose: RedshiftMigrateToVpc resource. Il tag limita l'ambito delle autorizzazioni a specifiche attività di migrazione e da Amazon EC2 Classic ad Amazon EC2 VPC. Per ulteriori informazioni sui tag di risorsa, consultare <a href="#">Controllo dell'accesso alle risorse AWS mediante i tag delle risorse</a>.</p>	

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftData FullAccesso</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>redshift:GetClusterCredentialsWithIAM</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione per ottenere credenziali temporanee avanzate per accedere a un database Amazon Redshift con l'Account AWS specificato.	7 aprile 2023
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	Le autorizzazioni per le operazioni su Amazon EC2 per la creazione e la gestione delle regole dei gruppi di sicurezza vengono aggiunte alla policy gestita. Queste regole e gruppi di sicurezza sono specificamente associati al tag delle risorse <code>aws:RequestTag/Redshift</code> di Amazon Redshift. Ciò limita l'ambito delle autorizzazioni a risorse specifiche di Amazon Redshift.	6 aprile 2023
<a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:GetSchemaInference</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione per ottenere le colonne e i tipi di dati dedotti da un file.	21 marzo 2023

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:GetSchemaInference</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione per ottenere le colonne e i tipi di dati dedotti da un file.	21 marzo 2023
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:GetSchemaInference</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione per ottenere le colonne e i tipi di dati dedotti da un file.	21 marzo 2023
<a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:AssociateNotebookWithTab</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione a creare e aggiornare le schede collegate al notebook di un utente.	2 febbraio 2023

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:AssociateNotebookWithTab</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione a creare e aggiornare le schede collegate al notebook di un utente o a un notebook condiviso.	2 febbraio 2023
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:AssociateNotebookWithTab</code> viene aggiunta alla policy gestita. La sua aggiunta concede l'autorizzazione a creare e aggiornare le schede collegate al notebook di un utente o a un notebook condiviso.	2 febbraio 2023

Modifica	Descrizione	Data
<p><a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a>: aggiornamento a una policy esistente</p>	<p>Per concedere l'autorizzazione all'uso dei notebook, Amazon Redshift ha aggiunto l'autorizzazione per le seguenti azioni:</p> <ul style="list-style-type: none"><li>• <code>sqlworkbench:ListNotebooks</code></li><li>• <code>sqlworkbench:CreateNotebook</code></li><li>• <code>sqlworkbench:DuplicateNotebook</code></li><li>• <code>sqlworkbench:CreateNotebookFromVersion</code></li><li>• <code>sqlworkbench:ImportNotebook</code></li><li>• <code>sqlworkbench:GetNotebook</code></li><li>• <code>sqlworkbench:UpdateNotebook</code></li><li>• <code>sqlworkbench&gt;DeleteNotebook</code></li><li>• <code>sqlworkbench:CreateNotebookCell</code></li><li>• <code>sqlworkbench&gt;DeleteNotebookCell</code></li><li>• <code>sqlworkbench:UpdateNotebookCellContent</code></li><li>• <code>sqlworkbench:UpdateNotebookCellLayout</code></li></ul>	<p>17 ottobre 2022</p>

Modifica	Descrizione	Data
	<ul style="list-style-type: none"><li>• <code>sqlworkbench:BatchGetNotebookCell</code></li><li>• <code>sqlworkbench:ListNotebookVersions</code></li><li>• <code>sqlworkbench:CreateNotebookVersion</code></li><li>• <code>sqlworkbench:GetNotebookVersion</code></li><li>• <code>sqlworkbench&gt;DeleteNotebookVersion</code></li><li>• <code>sqlworkbench:RestoreNotebookVersion</code></li><li>• <code>sqlworkbench:ExportNotebook</code></li></ul>	

Modifica	Descrizione	Data
<p><a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a>: aggiornamento a una policy esistente</p>	<p>Per concedere l'autorizzazione all'uso dei notebook, Amazon Redshift ha aggiunto l'autorizzazione per le seguenti azioni:</p> <ul style="list-style-type: none"> <li>• sqlworkbench:ListNotebooks</li> <li>• sqlworkbench:CreateNotebook</li> <li>• sqlworkbench:DuplicateNotebook</li> <li>• sqlworkbench:CreateNotebookFromVersion</li> <li>• sqlworkbench:ImportNotebook</li> <li>• sqlworkbench:GetNotebook</li> <li>• sqlworkbench:UpdateNotebook</li> <li>• sqlworkbench&gt;DeleteNotebook</li> <li>• sqlworkbench:CreateNotebookCell</li> <li>• sqlworkbench&gt;DeleteNotebookCell</li> <li>• sqlworkbench:UpdateNotebookCellContent</li> <li>• sqlworkbench:UpdateNotebookCellLayout</li> </ul>	<p>17 ottobre 2022</p>

Modifica	Descrizione	Data
	<ul style="list-style-type: none"><li>• <code>sqlworkbench:BatchGetNotebookCell</code></li><li>• <code>sqlworkbench:ListNotebookVersions</code></li><li>• <code>sqlworkbench:CreateNotebookVersion</code></li><li>• <code>sqlworkbench:GetNotebookVersion</code></li><li>• <code>sqlworkbench&gt;DeleteNotebookVersion</code></li><li>• <code>sqlworkbench:RestoreNotebookVersion</code></li><li>• <code>sqlworkbench:ExportNotebook</code></li></ul>	

Modifica	Descrizione	Data
<p><a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a>: aggiornamento a una policy esistente</p>	<p>Per concedere l'autorizzazione all'uso dei notebook, Amazon Redshift ha aggiunto l'autorizzazione per le seguenti azioni:</p> <ul style="list-style-type: none"> <li>• sqlworkbench:ListNotebooks</li> <li>• sqlworkbench:CreateNotebook</li> <li>• sqlworkbench:DuplicateNotebook</li> <li>• sqlworkbench:CreateNotebookFromVersion</li> <li>• sqlworkbench:ImportNotebook</li> <li>• sqlworkbench:GetNotebook</li> <li>• sqlworkbench:UpdateNotebook</li> <li>• sqlworkbench&gt;DeleteNotebook</li> <li>• sqlworkbench:CreateNotebookCell</li> <li>• sqlworkbench&gt;DeleteNotebookCell</li> <li>• sqlworkbench:UpdateNotebookCellContent</li> <li>• sqlworkbench:UpdateNotebookCellLayout</li> </ul>	<p>17 ottobre 2022</p>

Modifica	Descrizione	Data
	<ul style="list-style-type: none"> <li>• <code>sqlworkbench:BatchGetNotebookCell</code></li> <li>• <code>sqlworkbench:ListNotebookVersions</code></li> <li>• <code>sqlworkbench:CreateNotebookVersion</code></li> <li>• <code>sqlworkbench:GetNotebookVersion</code></li> <li>• <code>sqlworkbench&gt;DeleteNotebookVersion</code></li> <li>• <code>sqlworkbench:RestoreNotebookVersion</code></li> <li>• <code>sqlworkbench:ExportNotebook</code></li> </ul>	
<p><a href="#">AmazonRedshiftServiceLinkedRolePolicy</a>: aggiornamento a una policy esistente</p>	<p>Amazon Redshift ha aggiunto lo spazio dei nomi <code>AWS/Redshift</code> per consentire la pubblicazione di metriche. <code>CloudWatch</code></p>	<p>7 settembre 2022</p>
<p><a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a>: aggiornamento a una policy esistente</p>	<p>Amazon Redshift ha aggiunto l'autorizzazione per le operazioni <code>sqlworkbench:ListQueryExecutionHistory</code> e <code>sqlworkbench:GetQueryExecutionHistory</code>. Ciò consente di concedere l'autorizzazione per visualizzare la cronologia delle query.</p>	<p>30 agosto 2022</p>

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto l'autorizzazione per le operazioni <code>sqlworkbench:ListQueryExecutionHistory</code> e <code>sqlworkbench:GetQueryExecutionHistory</code> . Ciò consente di concedere l'autorizzazione per visualizzare la cronologia delle query.	30 agosto 2022
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto l'autorizzazione per le operazioni <code>sqlworkbench:ListQueryExecutionHistory</code> e <code>sqlworkbench:GetQueryExecutionHistory</code> . Ciò consente di concedere l'autorizzazione per visualizzare la cronologia delle query.	30 agosto 2022
<a href="#">AmazonRedshiftFullAccess</a> : aggiornamento a una policy esistente	Le autorizzazioni per Amazon Redshift Serverless vengono aggiunte alla policy gestita esistente. <code>AmazonRedshiftFullAccess</code>	22 luglio 2022

Modifica	Descrizione	Data
<p><a href="#">AmazonRedshiftData FullAccesso</a>: aggiornamento a una policy esistente</p>	<p>Amazon Redshift ha aggiornato la condizione di ambito predefinita <code>redshift-serverless:GetCredentials</code> dell'autorizzazione del tag <code>aws:ResourceTag/RedshiftDataFullAccess</code> da <code>StringEquals</code> a <code>StringLike</code> per concedere l'accesso alle risorse taggate con la chiave di tag <code>RedshiftDataFullAccess</code> e qualsiasi valore di tag.</p>	<p>11 luglio 2022</p>
<p><a href="#">AmazonRedshiftData FullAccesso</a>: aggiornamento a una policy esistente</p>	<p>Amazon Redshift ha aggiunto nuove autorizzazioni per consentire l'operazione <code>redshift-serverless:GetCredentials</code> per le credenziali temporanee ad Amazon Redshift Serverless.</p>	<p>8 luglio 2022</p>
<p><a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a>: aggiornamento a una policy esistente</p>	<p>Amazon Redshift ha aggiunto l'autorizzazione per l'azione <code>sqlworkbench:GetAccountSettings</code>. Ciò concede l'autorizzazione per ottenere le impostazioni dell'account.</p>	<p>15 giugno 2022</p>

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto l'autorizzazione per l'azione <code>sqlworkbench:GetAccountSettings</code> . Ciò concede l'autorizzazione per ottenere le impostazioni dell'account.	15 giugno 2022
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto l'autorizzazione per l'azione <code>sqlworkbench:GetAccountSettings</code> . Ciò concede l'autorizzazione per ottenere le impostazioni dell'account.	15 giugno 2022
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	Per abilitare l'accesso pubblico ai nuovi endpoint Amazon Redshift Serverless, Amazon Redshift assegna e associa gli indirizzi IP elastici all'interfaccia di rete Elastic dell'endpoint VPC nell'account cliente. Lo fa tramite le autorizzazioni fornite attraverso il ruolo collegato al servizio. Per abilitare questo caso d'uso, le azioni per allocare e rilasciare un indirizzo IP elastico vengono aggiunte al ruolo collegato al servizio Amazon Redshift Serverless.	26 maggio 2022

Modifica	Descrizione	Data
<p><a href="#">AmazonRedshiftQueryEditorV2 FullAccess:</a> aggiornamento a una policy esistente</p>	<p>Autorizzazioni per l'operazione <code>sqlworkbench:ListTaggedResources</code>. È specifico per le risorse dell'editor di query v2 di Amazon Redshift. Questo aggiornamento delle policy dà il diritto di chiamare <code>tag:GetResources</code> solo tramite l'editor di query v2.</p>	<p>22 febbraio 2022</p>
<p><a href="#">AmazonRedshiftQueryEditorV2 NoSharing:</a> aggiornamento a una policy esistente</p>	<p>Autorizzazioni per l'operazione <code>sqlworkbench:ListTaggedResources</code>. È specifico per le risorse dell'editor di query v2 di Amazon Redshift. Questo aggiornamento delle policy dà il diritto di chiamare <code>tag:GetResources</code> solo tramite l'editor di query v2.</p>	<p>22 febbraio 2022</p>
<p><a href="#">AmazonRedshiftQueryEditorV2 ReadSharing:</a> aggiornamento a una policy esistente</p>	<p>Autorizzazioni per l'operazione <code>sqlworkbench:ListTaggedResources</code>. È specifico per le risorse dell'editor di query v2 di Amazon Redshift. Questo aggiornamento delle policy dà il diritto di chiamare <code>tag:GetResources</code> solo tramite l'editor di query v2.</p>	<p>22 febbraio 2022</p>

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : aggiornamento a una policy esistente	Autorizzazioni per l'operazione <code>sqlworkbench:ListTaggedResources</code> . È specifico per le risorse dell'editor di query v2 di Amazon Redshift. Questo aggiornamento delle policy dà il diritto di chiamare <code>tag:GetResources</code> solo tramite l'editor di query v2.	22 febbraio 2022
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : aggiornamento a una policy esistente	L'autorizzazione per l'operazione <code>sqlworkbench:AssociateQueryWithTab</code> viene aggiunta alla policy gestita. Tale aggiunta consente ai clienti di creare schede editor collegate a una query condivisa con loro.	22 febbraio 2022
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto le autorizzazioni per nuove azioni per consentire la gestione della rete Amazon Redshift e delle risorse VPC.	22 novembre 2021

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftAllCommandsFullAccess</a> : nuova policy	Amazon Redshift ha aggiunto una nuova policy per consentire l'utilizzo del ruolo IAM creato dalla console di Amazon Redshift e impostarlo come predefinito per far eseguire al cluster la COPIA tramite i comandi di Amazon S3, SCARICARE, CREA FUNZIONE ESTERNA, CREA TABELLA ESTERNA, CREA SCHEMA ESTERNO, CREA MODELLO o CREA LIBRERIA.	18 novembre 2021
<a href="#">AmazonRedshiftServiceLinkedRolePolicy</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto le autorizzazioni per nuove azioni per consentire la gestione dei gruppi di CloudWatch log e dei flussi di log di Amazon Redshift, inclusa l'esportazione dei log di audit.	15 novembre 2021
<a href="#">AmazonRedshiftFullAccess</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto nuove autorizzazioni per consentire la spiegabilità del modello, DynamoDB, Redshift Spectrum e la federazione Amazon RDS.	7 ottobre 2021

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftQueryEditorV2 FullAccess</a> : nuova policy	Amazon Redshift ha aggiunto una nuova policy per consentire l'accesso completo all'editor di query v2 di Amazon Redshift.	24 settembre 2021
<a href="#">AmazonRedshiftQueryEditorV2 NoSharing</a> : nuova policy	Amazon Redshift ha aggiunto una nuova policy per consentire l'utilizzo dell'editor di query v2 di Amazon Redshift senza condividere risorse.	24 settembre 2021
<a href="#">AmazonRedshiftQueryEditorV2 ReadSharing</a> : nuova policy	Amazon Redshift ha aggiunto una nuova policy per consentire la condivisione di lettura all'interno dell'editor di query v2 di Amazon Redshift.	24 settembre 2021
<a href="#">AmazonRedshiftQueryEditorCondivisione V2 ReadWrite</a> : nuova policy	Amazon Redshift ha aggiunto una nuova policy per consentire la condivisione di lettura e aggiornamento all'interno dell'editor di query v2 di Amazon Redshift.	24 settembre 2021
<a href="#">AmazonRedshiftFullAccess</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto nuove autorizzazioni per consentire <code>sagemaker:*Job*</code> .	18 agosto 2021
<a href="#">AmazonRedshiftDataFullAccesso</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto nuove autorizzazioni per consentire <code>AuthorizeDataShare</code> .	12 agosto 2021

Modifica	Descrizione	Data
<a href="#">AmazonRedshiftData FullAccesso</a> : aggiornamento a una policy esistente	Amazon Redshift ha aggiunto nuove autorizzazioni per consentire BatchExecuteStatement .	27 luglio 2021
Amazon Redshift ha iniziato a monitorare le modifiche	Amazon Redshift ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	27 luglio 2021

## Autorizzazioni richieste per utilizzare Redshift Spectrum

Amazon Redshift Spectrum richiede autorizzazioni per AWS altri servizi per accedere alle risorse. Per i dettagli delle autorizzazioni nelle policy IAM per Redshift Spectrum, consultare [Policy IAM per Amazon Redshift Spectrum](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Autorizzazioni richieste per utilizzare la console Amazon Redshift

Affinché un utente possa lavorare con la console Amazon Redshift, deve disporre di un set minimo di autorizzazioni che gli consentano di descrivere le risorse Amazon Redshift per il proprio account. AWS Queste autorizzazioni devono inoltre consentire all'utente di descrivere altre informazioni correlate, tra cui la sicurezza di Amazon EC2, Amazon, CloudWatch Amazon SNS e le informazioni di rete.

Se decidi di creare una policy IAM più restrittiva delle autorizzazioni minime richieste, la console non funzionerà come previsto per gli utenti con tale policy IAM. Per essere certi che gli utenti possano continuare a usare la console Amazon Redshift, collega anche la policy gestita da AmazonRedshiftReadOnlyAccess all'utente. Questa procedura è descritta in [AWS politiche gestite per Amazon Redshift](#).

Per informazioni su come consentire a un utente l'accesso all'editor di query nella console Amazon Redshift, consultare [Autorizzazioni richieste per utilizzare l'editor di query della console Amazon Redshift](#).

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso l' AWS CLI API di Amazon Redshift.

## Autorizzazioni richieste per utilizzare l'editor di query della console Amazon Redshift

Affinché un utente possa utilizzare l'editor di query Amazon Redshift, deve disporre di un set minimo di autorizzazioni per Amazon Redshift e le operazioni API dati di Amazon Redshift. Per connettersi a un database utilizzando un segreto, è necessario disporre anche delle autorizzazioni di Secrets Manager.

Per consentire a un utente di accedere all'editor di query sulla console Amazon Redshift, collega le policy `AmazonRedshiftQueryEditor` e le policy `AmazonRedshiftReadOnlyAccess` AWS gestite. La policy `AmazonRedshiftQueryEditor` concede all'utente l'autorizzazione per recuperare solo i risultati delle proprie istruzioni SQL. Ovvero, dichiarazioni inviate dallo stesso, `aws:userid` come illustrato in questa sezione della politica `AmazonRedshiftQueryEditor` AWS gestita.

```
{
  "Sid": "DataAPIIAMSessionPermissionsRestriction",
  "Action": [
    "redshift-data:GetStatementResult",
    "redshift-data:CancelStatement",
    "redshift-data:DescribeStatement",
    "redshift-data:ListStatements"
  ],
  "Effect": "Allow",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "redshift-data:statement-owner-iam-userid": "${aws:userid}"
    }
  }
}
```

Per consentire a un utente di recuperare i risultati delle istruzioni SQL di altri utenti nello stesso ruolo IAM, creare una policy personalizzata senza la condizione per limitare l'accesso all'utente corrente. Limitare anche l'accesso a un amministratore per modificare una policy.

## Autorizzazioni necessarie per utilizzare l'editor della query v2

Affinché un utente possa lavorare con l'editor di query di Amazon Redshift v2, deve disporre di un set minimo di autorizzazioni per Amazon Redshift, le operazioni dell'editor di query v2 e altri AWS servizi come il servizio di tagging. AWS Key Management Service AWS Secrets Manager

Per consentire a un utente l'accesso completo all'editor di query v2, allega la policy gestita. `AmazonRedshiftQueryEditorV2FullAccess` AWS La policy `AmazonRedshiftQueryEditorV2FullAccess` consente all'utente di condividere le risorse dell'editor di query v2, come le query, con altri membri dello stesso team. Per informazioni dettagliate su come viene controllato l'accesso alle risorse dell'editor di query v2, consultare la definizione della specifica policy gestita per l'editor di query v2 nella console IAM.

Alcune policy AWS gestite di Amazon Redshift Query Editor v2 utilizzano i AWS tag all'interno di condizioni per definire l'accesso alle risorse. Nell'editor di query v2, la condivisione delle query si basa sulla chiave e sul valore del tag `"aws:ResourceTag/sqlworkbench-team"`: `"${aws:PrincipalTag/sqlworkbench-team}"` nella policy IAM collegata al principale (il ruolo IAM). I responsabili dello stesso gruppo Account AWS con lo stesso valore di tag (ad esempio, `accounting-team`) fanno parte dello stesso team in Query Editor v2. Si può essere associati a un solo team alla volta. Un utente con autorizzazioni amministrative può configurare i team nella console IAM dando a tutti i membri del team lo stesso valore per il tag `sqlworkbench-team`. Se il valore del tag del `sqlworkbench-team` viene modificato per un utente o per un ruolo IAM, potrebbe esserci un ritardo fino a quando la modifica non si riflette nelle risorse condivise. Se il valore del tag di una risorsa (ad esempio una query) viene modificato, potrebbe esserci un ritardo fino a quando la modifica non viene riflessa. I membri del team devono avere anche il permesso `tag:GetResources` per condividere.

Esempio: per aggiungere il tag **accounting-team** per un ruolo IAM

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 riquadro di navigazione della console, scegliere Roles (Ruoli) e selezionare il nome del ruolo che si desidera modificare.
3. Scegliere la scheda Tag quindi scegliere Aggiungi tag.
4. Aggiungi il tag chiave `sqlworkbench team` e il valore `accounting-team`.
5. Seleziona Salvataggio delle modifiche.

Ora quando un principale IAM (con questo ruolo IAM allegato) condivide una query con il team, altri principal con lo stesso valore del tag `accounting-team` può visualizzare la query.

Per ulteriori informazioni su come collegare un tag a un principale, inclusi i ruoli e gli utenti IAM, consultare [Assegnazione di tag di risorse IAM](#) nella Guida per l'utente di IAM.

È inoltre possibile configurare team a livello di sessione utilizzando un Identity Provider (IdP). Ciò consente a più utenti che utilizzano lo stesso ruolo IAM di avere un team diverso. La policy di attendibilità del ruolo IAM deve consentire l'operazione `sts:TagSession`. Per ulteriori informazioni, consultare [Autorizzazioni necessarie per aggiungere tag di sessione](#) nella Guida per l'utente di IAM. Aggiungi l'attributo tag principale all'asserzione SAML fornita dal tuo IdP.

```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/PrincipalTag:sqlworkbench-team">
  <AttributeValue>accounting-team</AttributeValue>
</Attribute>
```

Segui le istruzioni per il tuo provider di identità (IdP) per popolare l'attributo SAML con il contenuto proveniente dalla tua directory. Per ulteriori informazioni sui provider di identità (IdPs) e Amazon Redshift, consulta [Utilizzo dell'autenticazione IAM per generare credenziali utente di database e Identity providers and federation](#) nella IAM User Guide.

`sqlworkbench:CreateNotebookVersion` concede l'autorizzazione per ottenere il contenuto corrente delle celle del notebook e creare una versione del notebook nel tuo account. Pertanto, al momento della creazione della versione, il contenuto corrente del notebook è lo stesso di quello della versione. Quando il notebook viene aggiornato, il contenuto delle celle della versione rimane lo stesso. `sqlworkbench:GetNotebookVersion` concede l'autorizzazione per ottenere una versione del notebook. Un utente che non dispone dell'autorizzazione `sqlworkbench:BatchGetNotebookCell`, ma ha le autorizzazioni `sqlworkbench:CreateNotebookVersion` e `sqlworkbench:GetNotebookVersion` su un notebook, ha accesso alle celle del notebook nella versione. Questo utente senza l'autorizzazione `sqlworkbench:BatchGetNotebookCell` è comunque in grado di recuperare il contenuto delle celle del notebook creando una versione e ottenendola.

## Autorizzazioni richieste per utilizzare il pianificatore Amazon Redshift

Quando utilizzi il pianificatore di Amazon Redshift, imposti un ruolo IAM con una relazione di attendibilità con il pianificatore Amazon Redshift (**`scheduler.redshift.amazonaws.com`**) per permettere al pianificatore di acquisire le autorizzazioni per tuo conto. Viene inoltre collegata una policy (autorizzazioni) al ruolo delle operazioni API di Amazon Redshift che desideri pianificare.

L'esempio seguente mostra il documento di policy in formato JSON per impostare una relazione di attendibilità con il pianificatore di Amazon Redshift e Amazon Redshift stesso.

```
{
```

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

Per ulteriori informazioni sulle entità fiduciarie, consulta [Creating a role to delegate permissions to an AWS service](#) nella IAM User Guide.

È necessario anche aggiungere le autorizzazioni per le operazioni Amazon Redshift che desideri pianificare.

Affinché lo strumento di pianificazione possa usare l'operazione `ResizeCluster`, aggiungi alla tua policy IAM un'autorizzazione sia simile alla seguente. A seconda dell'ambiente, potrebbe essere necessario rendere la policy maggiormente restrittiva.

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

Per i passaggi per creare un ruolo per lo scheduler di Amazon Redshift, consulta [Creating a role for an AWS service \(console\)](#) nella IAM User Guide. Durante la creazione di un ruolo nella console IAM, applica queste selezioni:

- Alla voce Choose the service that will use this role (Scegli il servizio che utilizzerà questo ruolo), scegli Redshift.

- Alla voce **Select your use case (Seleziona il tuo caso d'uso)**, scegli **Redshift - Scheduler**.
- Crea o collega una policy al ruolo che permetta a un'operazione di Amazon Redshift di essere pianificata. Scegli **Create policy (Crea policy)** o modifica il ruolo per collegare una policy. Inserisci la policy JSON per l'operazione che deve essere pianificata.
- Dopo aver creato il ruolo, modifica la **Trust Relationship (Relazione di trust)** del ruolo IAM per includere il servizio `redshift.amazonaws.com`.

Il ruolo IAM creato dispone delle entità `trusted` di `scheduler.redshift.amazonaws.com` e `redshift.amazonaws.com`. Possiede anche una policy collegata che permette un'operazione API di Amazon Redshift supportata, come per esempio `"redshift:ResizeCluster"`.

## Autorizzazioni necessarie per utilizzare lo scheduler di Amazon EventBridge

Quando utilizzi lo EventBridge scheduler Amazon, configuri un ruolo IAM con una relazione di fiducia con lo EventBridge scheduler (**events.amazonaws.com**) per consentire allo scheduler di assumere le autorizzazioni per tuo conto. Inoltre, alleghi una policy (autorizzazioni) al ruolo per le operazioni Amazon Redshift Data API che desideri pianificare e una policy per le operazioni Amazon EventBridge .

Utilizzi lo EventBridge scheduler quando crei query pianificate con l'editor di query di Amazon Redshift sulla console.

È possibile creare un ruolo IAM per eseguire query pianificate nella console IAM. In questo ruolo IAM, collegare `AmazonEventBridgeFullAccess` e `AmazonRedshiftDataFullAccess`.

L'esempio seguente mostra il documento di policy in formato JSON per impostare una relazione di fiducia con lo scheduler. EventBridge

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

```
]
}
```

Per ulteriori informazioni sulle entità di fiducia, consulta [Creazione di un ruolo per delegare le autorizzazioni a un AWS servizio nella Guida per l'utente IAM](#).

Per i passaggi per creare un ruolo per lo EventBridge scheduler, consulta [Creating a role for an AWS service \(console\)](#) nella IAM User Guide. Durante la creazione di un ruolo nella console IAM, applica queste selezioni:

- Per scegliere il servizio che utilizzerà questo ruolo: Scegli CloudWatch eventi.
- Per Seleziona il tuo caso d'uso: scegli CloudWatch Eventi.
- Collega le policy di autorizzazione AmazonEventBridgeFullAccess e AmazonRedshiftDataFullAccess.

Il ruolo IAM creato dispone delle entità attendibili di `events.amazonaws.com`. Possiede anche una policy collegata che permette un'operazione API dati di Amazon Redshift supportata, come per esempio `redshift-data:*`.

## Autorizzazioni necessarie per utilizzare il machine learning (ML) di Amazon Redshift

Di seguito, puoi trovare una descrizione delle autorizzazioni necessarie per utilizzare il machine learning (ML) di Amazon Redshift con Amazon SageMaker per diversi casi d'uso.

Per consentire ai tuoi utenti di utilizzare Amazon Redshift ML con Amazon SageMaker, crea un ruolo IAM con una politica più restrittiva rispetto a quella predefinita. Si può usare la seguente policy. È inoltre possibile modificare questa policy per soddisfare le esigenze specifiche.

La seguente politica mostra le autorizzazioni necessarie per eseguire SageMaker Autopilot con la spiegabilità del modello da Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
```

```

        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
    ],
    "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
        "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [

```

```

        "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": [
                "SageMaker",
                "/aws/sagemaker/Endpoints",
                "/aws/sagemaker/ProcessingJobs",
                "/aws/sagemaker/TrainingJobs",
                "/aws/sagemaker/TransformJobs"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ecr:BatchCheckLayerAvailability",
        "ecr:BatchGetImage",
        "ecr:GetAuthorizationToken",
        "ecr:GetDownloadUrlForLayer"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
    ],

```

```

    "Resource": [
      "arn:aws:s3:::redshift-downloads",
      "arn:aws:s3:::redshift-downloads/*",
      "arn:aws:s3:::*redshift*",
      "arn:aws:s3:::*redshift*/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetBucketAcl",
      "s3:GetBucketCors",
      "s3:GetEncryptionConfiguration",
      "s3:GetBucketLocation",
      "s3:ListBucket",
      "s3:ListAllMyBuckets",
      "s3:ListMultipartUploadParts",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject",
      "s3:PutBucketAcl",
      "s3:PutBucketCors",
      "s3:DeleteObject",
      "s3:AbortMultipartUpload",
      "s3:CreateBucket"
    ],
    "Resource": "*",
    "Condition": {
      "StringEqualsIgnoreCase": {
        "s3:ExistingObjectTag/Redshift": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "iam:PassRole"
    ],
    "Resource": "arn:aws:iam::*:role/*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": [
          "redshift.amazonaws.com",
          "sagemaker.amazonaws.com"
        ]
      }
    }
  }
}

```

```

    ]
  }
}
]
}
}

```

La seguente policy mostra le autorizzazioni minime complete per consentire l'accesso alla federazione Amazon DynamoDB, Redshift Spectrum e Amazon RDS.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker:CreateTrainingJob",
        "sagemaker:CreateAutoMLJob",
        "sagemaker:CreateCompilationJob",
        "sagemaker:CreateEndpoint",
        "sagemaker:DescribeAutoMLJob",
        "sagemaker:DescribeTrainingJob",
        "sagemaker:DescribeCompilationJob",
        "sagemaker:DescribeProcessingJob",
        "sagemaker:DescribeTransformJob",
        "sagemaker:ListCandidatesForAutoMLJob",
        "sagemaker:StopAutoMLJob",
        "sagemaker:StopCompilationJob",
        "sagemaker:StopTrainingJob",
        "sagemaker:DescribeEndpoint",
        "sagemaker:InvokeEndpoint",
        "sagemaker:StopProcessingJob",
        "sagemaker:CreateModel",
        "sagemaker:CreateProcessingJob"
      ],
      "Resource": [
        "arn:aws:sagemaker:*:*:model/*redshift*",
        "arn:aws:sagemaker:*:*:training-job/*redshift*",
        "arn:aws:sagemaker:*:*:automl-job/*redshift*",
        "arn:aws:sagemaker:*:*:compilation-job/*redshift*",
        "arn:aws:sagemaker:*:*:processing-job/*redshift*",
        "arn:aws:sagemaker:*:*:transform-job/*redshift*",
        "arn:aws:sagemaker:*:*:endpoint/*redshift*"
      ]
    }
  ]
}

```

```

    ],
  },
  {
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:CreateLogStream",
      "logs:DescribeLogStreams",
      "logs:PutLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/Endpoints/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/ProcessingJobs/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/TrainingJobs/*redshift*",
      "arn:aws:logs:*:*:log-group:/aws/sagemaker/TransformJobs/*redshift*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "cloudwatch:PutMetricData"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "cloudwatch:namespace": [
          "SageMaker",
          "/aws/sagemaker/Endpoints",
          "/aws/sagemaker/ProcessingJobs",
          "/aws/sagemaker/TrainingJobs",
          "/aws/sagemaker/TransformJobs"
        ]
      }
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ecr:BatchCheckLayerAvailability",
    "ecr:BatchGetImage",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer"
  ],
  "Resource": "*"
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",
        "s3:CreateBucket"
      ],
      "Resource": [
        "arn:aws:s3:::redshift-downloads",
        "arn:aws:s3:::redshift-downloads/*",
        "arn:aws:s3::*redshift*",
        "arn:aws:s3::*redshift/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetBucketAcl",
        "s3:GetBucketCors",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:ListMultipartUploadParts",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:PutBucketCors",
        "s3:DeleteObject",
        "s3:AbortMultipartUpload",

```

```

        "s3:CreateBucket"
    ],
    "Resource": "*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "s3:ExistingObjectTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "dynamodb:Scan",
        "dynamodb:DescribeTable",
        "dynamodb:Getitem"
    ],
    "Resource": [
        "arn:aws:dynamodb:*:*:table/*redshift*",
        "arn:aws:dynamodb:*:*:table/*redshift*/index/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "elasticmapreduce:ListInstances"
    ],
    "Resource": [
        "arn:aws:elasticmapreduce:*:*:cluster/*redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "elasticmapreduce:ListInstances"
    ],
    "Resource": "*",
    "Condition": {
        "StringEqualsIgnoreCase": {
            "elasticmapreduce:ResourceTag/Redshift": "true"
        }
    }
},
{
    "Effect": "Allow",

```

```

    "Action": [
      "lambda:InvokeFunction"
    ],
    "Resource": "arn:aws:lambda:*:*:function:*redshift*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue>DeleteDatabase",
      "glue:GetDatabase",
      "glue:GetDatabases",
      "glue:UpdateDatabase",
      "glue:CreateTable",
      "glue>DeleteTable",
      "glue:BatchDeleteTable",
      "glue:UpdateTable",
      "glue:GetTable",
      "glue:GetTables",
      "glue:BatchCreatePartition",
      "glue:CreatePartition",
      "glue>DeletePartition",
      "glue:BatchDeletePartition",
      "glue:UpdatePartition",
      "glue:GetPartition",
      "glue:GetPartitions",
      "glue:BatchGetPartition"
    ],
    "Resource": [
      "arn:aws:glue:*:*:table/*redshift*/*",
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/*redshift*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetResourcePolicy",
      "secretsmanager:GetSecretValue",
      "secretsmanager:DescribeSecret",
      "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:*redshift*"
    ]
  }

```

```

    ],
    {
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "secretsmanager:ResourceTag/Redshift": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": [
            "redshift.amazonaws.com",
            "glue.amazonaws.com",
            "sagemaker.amazonaws.com",
            "athena.amazonaws.com"
          ]
        }
      }
    }
  ]
}

```

Facoltativamente, per utilizzare una AWS KMS chiave per la crittografia, aggiungi le seguenti autorizzazioni alla policy.

```

{
  "Effect": "Allow",
  "Action": [
    "kms:CreateGrant",
    "kms:Decrypt",

```

```

    "kms:DescribeKey",
    "kms:Encrypt",
    "kms:GenerateDataKey*"
  ],
  "Resource": [
    "arn:aws:kms:<your-region>:<your-account-id>:key/<your-kms-key>"
  ]
}

```

Per consentire ad Amazon Redshift e SageMaker assumere il precedente ruolo IAM di interagire con altri servizi, aggiungi la seguente policy di fiducia al ruolo.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.amazonaws.com",
          "sagemaker.amazonaws.com",
          "forecast.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```

Nel precedente esempio, il bucket Amazon S3 `redshift-downloads/redshift-ml/` è la posizione in cui sono memorizzati i dati di esempio utilizzati per altre fasi ed esempi. È possibile rimuovere questo bucket se non è necessario caricare dati da Amazon S3. O sostituirlo con altri bucket Amazon S3 utilizzati per caricare i dati in Amazon Redshift.

I valori **your-account-id**, **your-role**, **eyour-s3-bucket** sono l'ID account, il ruolo e il bucket specificati nel comando CREAZIONE MODELLO.

Facoltativamente, puoi utilizzare la sezione AWS KMS keys della policy di esempio se specifichi una AWS KMS chiave da usare con Amazon Redshift ML. Il valore **your-kms-key** è la chiave che si utilizza come parte del comando CREATE MODEL.

Quando si specifica un cloud privato virtuale (VPC) privato per processo di ottimizzazione dell'iperparametro, aggiungere le seguenti autorizzazioni.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2>DeleteNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ]
}
```

Per utilizzare la spiegazione del modello, assicurati di disporre delle autorizzazioni per chiamare SageMaker le operazioni API. Ti consigliamo di utilizzare la policy gestita `AmazonSageMakerFullAccess`. Se si desidera creare un ruolo IAM con una policy più restrittiva, utilizzare la policy seguente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sagemaker::CreateEndpoint",
        "sagemaker::CreateEndpointConfig",
        "sagemaker::DeleteEndpoint",
        "sagemaker::DeleteEndpointConfig",
        "sagemaker::DescribeEndpoint",
        "sagemaker::DescribeEndpointConfig",
        "sagemaker::DescribeModel",
        "sagemaker::InvokeEndpoint",
        "sagemaker::ListTags"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Per ulteriori informazioni sulla policy `AmazonSageMakerFullAccess` gestita, consulta [AmazonSageMakerFullAccess](#) nella Amazon SageMaker Developer Guide.

Se desideri creare modelli di previsione, ti consigliamo di utilizzare la policy gestita `AmazonForecastFullAccess`. Se desideri utilizzare una policy maggiormente restrittiva, aggiungi la policy seguente al tuo ruolo IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "forecast:CreateAutoPredictor",
        "forecast:CreateDataset",
        "forecast:CreateDatasetGroup",
        "forecast:CreateDatasetImportJob",
        "forecast:CreateForecast",
        "forecast:CreateForecastExportJob",
        "forecast>DeleteResourceTree",
        "forecast:DescribeAutoPredictor",
        "forecast:DescribeDataset",
        "forecast:DescribeDatasetGroup",
        "forecast:DescribeDatasetImportJob",
        "forecast:DescribeForecast",
        "forecast:DescribeForecastExportJob",
        "forecast:StopResource",
        "forecast:TagResource",
        "forecast:UpdateDatasetGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

Per ulteriori informazioni su Amazon Redshift ML, consultare [Utilizzo di Machine Learning in Amazon Redshift](#) o [CREAZIONE DEL MODELLO](#).

## Autorizzazioni per l'importazione dati in streaming

L'importazione dati in streaming funziona con due servizi. Questi sono flusso di video Amazon Kinesis e Amazon MSK.

Autorizzazioni necessarie per utilizzare l'importazione dati in streaming con flusso di dati Amazon Kinesis

Una procedura con un esempio di policy gestita è disponibile in [Nozioni di base sull'importazione dati in streaming da flusso di dati Amazon Kinesis](#).

Autorizzazioni necessarie per utilizzare l'importazione dati in streaming con Amazon MSK

Una procedura con un esempio di policy gestita è disponibile in [Nozioni di base sull'importazione dati in streaming da flusso di dati Amazon Kinesis](#).

Autorizzazioni necessarie per utilizzare le operazioni dell'API di condivisione dei dati

Per controllare l'accesso alle operazioni API di condivisione dati, utilizzare le policy basate su azioni IAM. Per ulteriori informazioni sulla gestione e sulla creazione di policy IAM personalizzate, consultare [Gestione delle policy IAM](#) nella Guida per l'utente di IAM.

In particolare, si supponga che un amministratore del cluster producer debba utilizzare la chiamata `AuthorizeDataShare` per autorizzare l'uscita di una unità di condivisione dati all'esterno di un account Account AWS. In questo caso, si imposta una policy basata sulle azioni IAM per concedere questa autorizzazione. Utilizzare la chiamata `DeauthorizeDataShare` per revocare l'uscita.

Quando si utilizzano policy basate su operazioni IAM è inoltre possibile specificare una risorsa IAM nella policy, ad esempio `DataShareARN`. Di seguito vengono mostrati il formato e un esempio per `DataShareARN`.

```
arn:aws:redshift:region:account-id:datashare:namespace-guid/datashare-name
arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
SalesShare
```

È possibile limitare l'accesso `AuthorizeDataShare` a una unità di condivisione dati specificando il nome dell'unità nella policy IAM.

```
{
  "Statement": [
```

```

{
  "Action": [
    "redshift:AuthorizeDataShare",
  ],
  "Resource": [
    "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/SalesShare"
  ],
  "Effect": "Deny"
}
]
}

```

È inoltre possibile limitare la policy IAM a tutte le unità di condivisione dati di proprietà di un cluster producer specifico. Per effettuare questa operazione, sostituire il valore **datashare-name** nella policy con un carattere jolly o un asterisco. Mantieni il valore del cluster namespace-guid.

```

arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-e2e24359e9a8/
*

```

Di seguito è riportata una policy IAM che impedisce a un'entità di chiamare AuthorizeDataShare sulle unità di condivisione dati di proprietà di un cluster producer specifico.

```

{
  "Statement": [
    {
      "Action": [
        "redshift:AuthorizeDataShare",
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:555555555555:datashare:86b5169f-01dc-4a6f-9fbb-
e2e24359e9a8/*"
      ],
      "Effect": "Deny"
    }
  ]
}

```

DataShareARN limita l'accesso in base sia al nome dell'unità di condivisione dati che all'ID univoco globale (GUID) dello spazio dei nomi del cluster proprietario. Questa operazione viene effettuata specificando il nome come asterisco.

## Politiche relative alle risorse per GetClusterCredentials

Per connetterti al database di un cluster tramite una connessione JDBC o ODBC con credenziali di database IAM o per chiamare a livello di programmazione l'operazione `GetClusterCredentials`, devi disporre di un set minimo di autorizzazioni. Devi avere almeno l'autorizzazione per chiamare l'azione `redshift:GetClusterCredentials` con accesso a una risorsa `dbuser`.

Se usi una connessione JDBC o ODBC, invece di `server` e `port` puoi specificare `cluster_id` e `region`, ma a questo scopo la policy deve anche consentire l'operazione `redshift:DescribeClusters` con accesso alla risorsa `cluster`.

Se chiami `GetClusterCredentials` con i parametri facoltativi `Autocreate`, `DbGroups` e `DbName`, dovrai anche consentire le operazioni e permettere l'accesso alle risorse elencate nella tabella seguente:

GetClusterCredentials parametro	Azione	Risorsa
Autocreate	<code>redshift:CreateClusterUser</code>	<code>dbuser</code>
DbGroups	<code>redshift:JoinGroup</code>	<code>dbgroup</code>
DbName	N/A	<code>dbname</code>

Per ulteriori informazioni sulle risorse, consultare [Risorse e operazioni di Amazon Redshift](#).

Puoi anche includere le condizioni seguenti nella policy:

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

Per ulteriori informazioni sulle condizioni, consulta [Specifiche delle condizioni in una policy](#).

## Esempi di policy gestite dal cliente

Questa sezione include policy utente di esempio che concedono autorizzazioni per diverse operazioni Amazon Redshift. Queste policy funzionano quando utilizzi l'API Amazon Redshift, gli AWS SDK o il AWS CLI

### Note

Tutti gli esempi utilizzano la regione Stati Uniti occidentali (Oregon) (us-west-2) e contengono ID account fittizi.

Esempio 1: concessione di accesso utente completo a tutte le operazioni e risorse di Amazon Redshift

La policy seguente concede l'accesso a tutte le operazioni di Amazon Redshift su tutte le risorse.

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

Il valore `redshift:*` nell'elemento `Action` indica tutte le operazioni in Amazon Redshift.

Esempio 2: rifiuto dell'accesso utente a un set di operazioni Amazon Redshift

Per impostazione predefinita, vengono negate tutte le autorizzazioni. Tuttavia, a volte è necessario negare esplicitamente l'accesso a un'operazione specifica o un set di operazioni specifico. La policy seguente concede l'accesso a tutte le operazioni di Amazon Redshift e nega esplicitamente l'accesso a qualsiasi operazione Amazon Redshift il cui nome inizia con `Delete`. Questa policy si applica a tutte le risorse Amazon Redshift nella regione `us-west-2`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowUSWest2Region",
      "Action": [
        "redshift:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:redshift:us-west-2:*"
    },
    {
      "Sid": "DenyDeleteUSWest2Region",
      "Action": [
        "redshift:Delete*"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:redshift:us-west-2:*"
    }
  ]
}
```

### Esempio 3: Concessione a un utente dell'autorizzazione per la gestione dei cluster

La policy seguente permette a un utente di creare, eliminare, modificare e riavviare tutti i cluster e quindi nega l'autorizzazione per eliminare o modificare qualsiasi cluster il cui identificatore inizia con `protected`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowClusterManagement",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```

    },
    {
      "Sid": "DenyDeleteProtected",
      "Action": [
        "redshift:DeleteCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:cluster:protected*"
      ],
      "Effect": "Deny"
    }
  ]
}

```

Esempio 4: Concessione a un utente dell'autorizzazione per concedere o revocare l'accesso agli snapshot

La policy seguente permette a un utente, ad esempio all'utente A, di eseguire le operazioni seguenti:

- Autorizzare l'accesso a qualsiasi snapshot creato da un cluster denominato shared.
- Revocare l'accesso a qualsiasi snapshot creato dal cluster shared il cui nome di cluster inizia con revokable.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSharedSnapshots",
      "Action": [
        "redshift:AuthorizeSnapshotAccess"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:shared/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRevokableSnapshot",
      "Action": [
        "redshift:RevokeSnapshotAccess"
      ],
      "Resource": [

```

```

        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/revokable*"
    ],
    "Effect": "Allow"
}
]
}

```

Se l'utente A ha consentito all'utente B di accedere a uno snapshot, l'utente B deve avere una policy come la seguente per poter ripristinare un cluster dallo snapshot. La policy seguente permette all'utente B di descrivere gli snapshot ed eseguire operazioni di ripristino dagli snapshot, nonché di creare cluster. Il nome di questi cluster deve iniziare con `from-other-account`.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribeSnapshots",
      "Action": [
        "redshift:DescribeClusterSnapshots"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowUserRestoreFromSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/*",
        "arn:aws:redshift:us-west-2:444455556666:cluster:from-other-account*"
      ],
      "Effect": "Allow"
    }
  ]
}

```

Esempio 5: Concessione a un utente dell'autorizzazione per la copia di uno snapshot del cluster e per il ripristino di un cluster da uno snapshot

La policy seguente permette a un utente di copiare qualsiasi snapshot creato dal cluster denominato `big-cluster-1` e di ripristinare qualsiasi snapshot il cui nome inizia con `snapshot-for-restore`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCopyClusterSnapshot",
      "Action": [
        "redshift:CopyClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:big-cluster-1/*"
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowRestoreFromClusterSnapshot",
      "Action": [
        "redshift:RestoreFromClusterSnapshot"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:snapshot:*/snapshot-for-restore*",
        "arn:aws:redshift:us-west-2:123456789012:cluster:*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Esempio 6: concessione a un utente dell'accesso ad Amazon Redshift e alle operazioni e risorse comuni per i servizi AWS correlati

La seguente policy di esempio consente l'accesso a tutte le azioni e le risorse per Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) e Amazon CloudWatch. Consente anche operazioni specifiche su tutte le risorse Amazon EC2 correlate nell'account.

 Note

Le autorizzazioni a livello di risorsa non sono supportate per le operazioni Amazon EC2 specificate in questa policy di esempio.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshift",
      "Effect": "Allow",
      "Action": [
        "redshift:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowSNS",
      "Effect": "Allow",
      "Action": [
        "sns:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCloudWatch",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowEC2Actions",
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:AllocateAddress",
      "ec2:AssociateAddress",
      "ec2:AttachNetworkInterface",
      "ec2:DescribeAccountAttributes",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeInternetGateways",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs"
    ],
    "Resource": [
      "*"
    ]
  }
]
}

```

### Esempio 7: consentire a un utente di taggare le risorse con la console Amazon Redshift

La seguente policy di esempio consente a un utente di taggare le risorse con la console Amazon Redshift utilizzando AWS Resource Groups. Questa policy può essere collegata a un ruolo utente che richiama la console Amazon Redshift nuova o originale. Per ulteriori informazioni sul tagging, consultare [Assegnazione di tag alle risorse in Amazon Redshift nella ..](#)

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Tagging permissions",
      "Effect": "Allow",
      "Action": [
        "redshift:DeleteTags",
        "redshift:CreateTags",
        "redshift:DescribeTags",
        "tag:UntagResources",
        "tag:TagResources"
      ],
      "Resource": "*"
    }
  ]
}

```

}

## Esempio di politica per l'utilizzo GetClusterCredentials

La seguente policy utilizza questi valori di parametro di esempio:

- Regione: us-west-2
- AWS Account: 123456789012
- Nome del cluster: examplecluster

La seguente policy consente le operazioni GetCredentials, CreateClusterUser e JoinGroup. La policy utilizza i tasti condizionali per consentire le CreateClusterUser azioni GetClusterCredentials and solo quando l'ID AWS utente corrisponde "AIDI0DR4TAW7CSEXAMPLE:\${redshift:DbUser}@yourdomain.com". L'accesso IAM è richiesto solo per il database "testdb". La policy, inoltre, consente agli utenti di unirsi a un gruppo chiamato "common\_group".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AIDI0DR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "CreateClusterUserStatement",
```

```

    "Effect": "Allow",
    "Action": [
      "redshift:CreateClusterUser"
    ],
    "Resource": [
      "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
${redshift:DbUser}"
    ],
    "Condition": {
      "StringEquals": {
        "aws:userid": "AIDIO4R4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
      }
    }
  },
  {
    "Sid": "RedshiftJoinGroupStatement",
    "Effect": "Allow",
    "Action": [
      "redshift:JoinGroup"
    ],
    "Resource": [
      "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
    ]
  }
]
}

```

## Native identity provider (IdP) federation for Amazon Redshift (Federazione di provider di identità nativi (IdP) per Amazon Redshift)

La gestione delle identità e delle autorizzazioni per Amazon Redshift è semplificata con la federazione dei provider di identità nativi perché sfrutta il provider di identità esistente per semplificare l'autenticazione e la gestione delle autorizzazioni. Ciò consente di condividere i metadati di identità con Redshift dal proprio provider di identità. Per la prima iterazione di questa caratteristica, il provider di identità supportato è [Microsoft Azure Active Directory \(Azure AD\)](#).

Per configurare Amazon Redshift in modo che possa autenticare le identità dal provider di identità di terze parti, è necessario registrare il provider di identità con Amazon Redshift. Ciò consente a Redshift di autenticare utenti e ruoli definiti dal provider di identità. In questo modo è possibile evitare di eseguire una gestione granulare delle identità sia nel proprio provider di identità di terze parti che in Amazon Redshift, poiché le informazioni sull'identità sono condivise.

Per informazioni sull'utilizzo dei ruoli di sessione trasferiti dai gruppi di gestori dell'identità digitale, consulta [PG\\_GET\\_SESSION\\_ROLES](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Configurazione del provider di identità su Amazon Redshift

In questa sezione vengono illustrati i passaggi per configurare il provider di identità e Amazon Redshift per stabilire la comunicazione per la federazione dei provider di identità nativi. È necessario un account attivo con il proprio provider di identità. Prima di configurare Amazon Redshift, registrare Redshift come applicazione presso il proprio provider di identità, concedendo il consenso dell'amministratore.

Completare la seguente procedura in Amazon Redshift:

1. È possibile eseguire un'istruzione SQL per registrare il provider di identità, incluse le descrizioni dei metadati dell'applicazione Azure. Per creare il provider di identità in Amazon Redshift, eseguire il comando seguente dopo aver sostituito i valori dei parametri issuer, client\_id, client\_secret e audience. Questi parametri sono specifici di Microsoft Azure AD. Sostituire il nome del provider di identità con un nome a scelta e sostituire lo spazio dei nomi con un nome univoco per contenere utenti e ruoli dalla directory del provider di identità.

```
CREATE IDENTITY PROVIDER oauth_standard TYPE azure
NAMESPACE 'aad'
PARAMETERS '{
  "issuer": "https://sts.windows.net/2sdfdsf-d475-420d-b5ac-667adad7c702/",
  "client_id": "<client_id>",
  "client_secret": "BUAH~ewrqewrqwerUUY^%tHe1oNZShoiU7",
  "audience": ["https://analysis.windows.net/powerbi/connector/AmazonRedshift"]
}'
```

Il tipo `azure` indica che il provider facilita specificamente la comunicazione con Microsoft Azure AD. Questo è attualmente l'unico provider di identità di terze parti supportato.

- `issuer`: l'ID emittente da considerare attendibile quando viene ricevuto un token. L'identificatore univoco per `tenant_id` viene aggiunto all'emittente.
- `client_id`: l'identificativo pubblico univoco dell'applicazione registrata presso il provider di identità. Questo può essere indicato come ID dell'applicazione.
- `client_secret`: un identificatore segreto o password noto solo al provider di identità e all'applicazione registrata.

- **audience:** l'ID applicazione assegnato all'applicazione in Azure.

Invece di utilizzare un segreto client condiviso, è possibile impostare i parametri per specificare un certificato, una chiave privata e una password per chiave privata quando si crea il gestore dell'identità digitale.

```
CREATE IDENTITY PROVIDER example_idp TYPE azure
NAMESPACE 'example_aad'
PARAMETERS '{"issuer":"https://sts.windows.net/2sdfdsf-d475-420d-
b5ac-667adad7c702/",
"client_id":"<client_id>",
"audience":["https://analysis.windows.net/powerbi/connector/AmazonRedshift"],
"client_x5t":"<certificate thumbprint>",
"client_pk_base64":"<private key in base64 encoding>",
"client_pk_password":"test_password"}';
```

La password della chiave privata, `client_pk_password`, è facoltativa.

2. **Facoltativo:** eseguire comandi SQL in Amazon Redshift per creare in anticipo utenti e ruoli. Ciò facilita la concessione anticipata delle autorizzazioni. Il nome del ruolo in Amazon Redshift è simile al seguente: `<GroupName su Azure <Namespace>AD`. Ad esempio, quando si crea un gruppo in Microsoft Azure AD denominato `rsgroup` e uno spazio dei nomi denominato `aad`, il nome del ruolo è `aad:rsgroup`. Il nome dell'utente e del ruolo in Amazon Redshift sono definiti da questi nomi utente e appartenenze ai gruppi nello spazio dei nomi del gestore dell'identità digitale.

La mappatura per ruoli e utenti include la verifica del loro valore `external_id` per garantire che sia aggiornato. L'ID esterno viene mappato all'identificatore del gruppo o dell'utente nel provider di identità. Ad esempio, l'ID esterno di un ruolo viene mappato all'ID del gruppo Azure AD corrispondente. Allo stesso modo, l'ID esterno di ogni utente viene mappato al relativo ID nel provider di identità.

```
create role "aad:rsgroup";
```

3. Concedere le autorizzazioni pertinenti ai ruoli in base alle proprie esigenze. Ad esempio:

```
GRANT SELECT on all tables in schema public to role "aad:rsgroup";
```

4. È anche possibile concedere autorizzazioni a un utente specifico.

```
GRANT SELECT on table foo to aad:alice@example.com
```

Si noti che l'appartenenza ai ruoli di un utente esterno federato è disponibile solo nella sessione di quell'utente. Ciò ha implicazioni per la creazione di oggetti di database. Quando un utente esterno federato crea una visualizzazione o una procedura archiviata, ad esempio, lo stesso utente non può delegare l'autorizzazione di tali oggetti ad altri utenti e ruoli.

## Una spiegazione degli spazi dei nomi

Uno spazio dei nomi mappa un utente o un ruolo a un provider di identità specifico. Ad esempio, il prefisso per gli utenti creati in IAM è. `AWS iam:` Questo prefisso impedisce le collisioni tra nomi utente e rende possibile il supporto per più archivi di identità. Se accede un utente `alice@example.com` dall'origine di identità registrata con lo spazio dei nomi `aad`, in Redshift viene creato l'utente `aad:alice@example.com`, se non è già esistente. Si noti che uno spazio dei nomi di utente e ruolo ha una funzione diversa rispetto a uno spazio dei nomi di cluster di Amazon Redshift, che è un identificatore univoco associato a un cluster.

## Come funziona l'accesso con la federazione di provider di identità nativi (IdP)

Per completare la configurazione preliminare tra il provider di identità e Amazon Redshift, eseguire un paio di passaggi: innanzitutto, registrare Amazon Redshift come applicazione di terze parti presso il proprio provider di identità, richiedendo le autorizzazioni API necessarie. Quindi creare utenti e gruppi nel provider di identità. Infine, registrare il provider di identità con Amazon Redshift, utilizzando istruzioni SQL, che impostano parametri di autenticazione univoci per il provider di identità. Come parte della registrazione del provider di identità con Redshift, si assegna uno spazio dei nomi per assicurarsi che utenti e ruoli siano raggruppati correttamente.

Con il provider di identità registrato con Amazon Redshift, viene impostata la comunicazione tra Redshift e il provider di identità. Un client può quindi passare token e autenticarsi con Redshift come entità provider di identità. Amazon Redshift utilizza le informazioni sull'appartenenza al gruppo IdP per mappare i ruoli di Redshift. Se l'utente non esiste in precedenza in Redshift, viene creato. Vengono creati ruoli che mappano ai gruppi di provider di identità, se non esistono. L'amministratore di Amazon Redshift concede l'autorizzazione per i ruoli e gli utenti possono eseguire query e altre attività di database.

La procedura seguente illustra il funzionamento della federazione di provider di identità nativi quando un utente accede:

1. Quando un utente accede utilizzando l'opzione IdP nativi dal client, il token del provider di identità viene inviato dal client al driver.
2. L'utente è autenticato. Se l'utente non esiste già in Amazon Redshift, viene creato un nuovo utente. Redshift mappa i gruppi del provider di identità dell'utente ai ruoli Redshift.
3. Le autorizzazioni vengono assegnate in base ai ruoli Redshift dell'utente. Questi sono concessi agli utenti e ai ruoli da parte di un amministratore.
4. L'utente può eseguire query su Redshift.

## Connessione ad Amazon Redshift con gli strumenti client desktop

Per istruzioni su come utilizzare la federazione dei provider di identità nativi per connettersi ad Amazon Redshift con Power BI, consultare il post del blog [Integrate Amazon Redshift native IdP federation with Microsoft Azure Active Directory \(AD\) and Power BI](#) (Integrazione della federazione IdP nativi di Amazon Redshift con Microsoft Azure Active Directory (AD) e Power BI). Descrive un' step-by-step implementazione della configurazione IdP nativa di Amazon Redshift con Azure AD. Inoltre, descrive in dettaglio i passaggi per configurare la connessione client per Power BI Desktop o per il servizio Power BI. I passaggi includono la registrazione dell'applicazione, la configurazione delle autorizzazioni e la configurazione delle credenziali.

Per informazioni su come integrare la federazione IdP nativa di Amazon Redshift con Azure AD, utilizzando Power BI Desktop e JDBC Client-SQL Workbench/J, guarda il seguente video:

Per istruzioni su come utilizzare la federazione dei provider di identità nativi per connettersi ad Amazon Redshift con un client SQL, in particolare DBeaver o SQL Workbench/J, consultare il post del blog [Integrate Amazon Redshift native IdP federation with Microsoft Azure AD using a SQL client](#) (Integrazione della federazione IdP nativi di Amazon Redshift con Microsoft Azure AD utilizzando un client SQL).

## Connessione di Redshift al Centro identità IAM per offrire agli utenti un'esperienza di autenticazione unica

Puoi gestire l'accesso di utenti e gruppi ai data warehouse Amazon Redshift tramite la propagazione di identità affidabili. Funziona tramite una connessione tra Redshift e AWS IAM Identity Center, che offre agli utenti un'esperienza di accesso singolo. In questo modo puoi inserire utenti e gruppi dalla tua directory e assegnare loro direttamente le autorizzazioni. In secondo luogo, questa connessione supporta l'aggiunta di altri strumenti e servizi. Per illustrare un end-to-end caso, puoi utilizzare una Amazon QuickSight dashboard o l'editor di query Amazon Redshift v2 per accedere a Redshift.

L'accesso in questo caso si basa sui gruppi del Centro identità IAM. Redshift può determinare chi è un utente e la sua appartenenza ai gruppi. IAM Identity Center consente inoltre di connettere e gestire le identità tramite un provider di identità (IdP) di terze parti come Okta o PingOne

Dopo aver impostato la connessione tra Redshift e il Centro identità IAM, è possibile configurare un accesso granulare basato sui gruppi di gestori dell'identità digitale per autorizzare l'accesso degli utenti ai dati.

## I vantaggi dell'integrazione di Redshift con AWS IAM Identity Center

L'utilizzo del Centro identità IAM con Redshift può apportare vantaggi alla tua organizzazione nei seguenti modi:

- Gli autori di dashboard Amazon QuickSight possono connettersi alle fonti di dati Redshift senza dover reinserire le password o richiedere a un amministratore di configurare i ruoli IAM con autorizzazioni complesse.
- Il Centro identità IAM fornisce una posizione centrale per gli utenti della tua forza lavoro in AWS. Puoi creare utenti e gruppi direttamente in IAM Identity Center o connettere utenti e gruppi esistenti che gestisci in un provider di identità basato su standard come Okta PingOne o Microsoft Entra ID (Azure AD). Il Centro identità IAM indirizza l'autenticazione alla fonte di verità prescelta per gli utenti e i gruppi e mantiene un elenco di utenti e gruppi a cui Redshift può accedere. Per ulteriori informazioni, consulta [Manage your identity source](#) e [Supported identity providers](#) nella Guida per l'utente di Centro identitàAWS IAM.
- Puoi condividere un'istanza Centro identità IAM con più cluster e gruppi di lavoro Redshift con una semplice funzionalità di rilevamento automatico e connessione. In tal modo si accelera l'aggiunta dei cluster senza l'attività di configurazione della connessione del Centro identità IAM per ognuno di essi e si garantisce che tutti i cluster e i gruppi di lavoro abbiano una visione coerente degli utenti nonché dei relativi attributi e gruppi. Tieni presente che l'istanza Centro identità IAM dell'organizzazione deve trovarsi nella stessa regione di tutte le unità di condivisione dati Redshift a cui ti connetti.
- Con le identità degli utenti note e registrate insieme all'accesso ai dati, è più facile soddisfare le normative di conformità attraverso il controllo degli accessi degli utenti in AWS CloudTrail.

## Configurazione dell'integrazione del Centro identità IAM con Amazon Redshift

L'amministratore del cluster Amazon Redshift o l'amministratore di Amazon Redshift serverless deve eseguire diversi passaggi per configurare Redshift come applicazione abilitata per il Centro identità

IAM. In questo modo si consente a Redshift di rilevare e connettersi automaticamente al Centro identità IAM per ricevere i servizi di accesso e directory utente. Dopodiché, quando l'amministratore di Redshift crea un cluster o un gruppo di lavoro, può consentire al nuovo data warehouse di utilizzare il Centro identità IAM per gestire l'accesso al database.

Lo scopo dell'abilitazione di Redshift come applicazione gestita dal Centro identità IAM è controllare le autorizzazioni di utenti e gruppi dal Centro identità IAM o da un gestore dell'identità digitale di terze parti integrato. Quando gli utenti accedono a un database Redshift, ad esempio un analista o un data scientist, controlla i gruppi del Centro identità IAM che definiscono i nomi dei ruoli in Redshift. In questo modo, un gruppo che definisce il nome per un ruolo del database Redshift può accedere, ad esempio, a un set di tabelle per l'analisi delle vendite. Nelle seguenti sezioni viene mostrato come si configura.

## Prerequisiti

I prerequisiti per l'integrazione del Centro identità IAM con Amazon Redshift sono i seguenti:

- Configurazione dell'account: devi configurare IAM Identity Center nell'account di gestione della tua AWS organizzazione se prevedi di avere casi d'uso tra account o se utilizzi cluster Redshift in account diversi con la stessa istanza di IAM Identity Center. È inclusa la configurazione dell'origine di identità. Per ulteriori informazioni, consulta [Getting Started](#), [Workforce Identities](#) e [Supported identity providers](#) nella Guida per l'utente di Centro identità AWS IAM. Prima di poterli assegnare utenti e gruppi ai dati in Redshift, devi assicurarti di averli creati nel Centro identità IAM o di averli sincronizzati dall'origine di identità.

### Note

È possibile utilizzare un'istanza di account di IAM Identity Center, a condizione che Redshift e IAM Identity Center si trovino nello stesso account. Puoi creare questa istanza utilizzando un widget al momento della creazione e configurazione di un cluster o un gruppo di lavoro Redshift.

- Configurazione di un emittente di token attendibile: in alcuni casi, potrebbe essere necessario utilizzare un emittente di token attendibile, ovvero un'entità in grado di emettere e verificare token attendibili. Sono necessari alcuni passaggi prima che l'amministratore di Redshift che configura l'integrazione con il Centro identità IAM possa selezionare l'emittente di token attendibile e aggiungere gli attributi necessari per completare la configurazione. Uno di questi passaggi potrebbe essere la configurazione di un gestore dell'identità digitale esterno che funga da

emittente di token attendibile e l'aggiunta dei relativi attributi nella console Centro identità IAM. Per completare questi passaggi, consulta [Utilizzo di applicazioni con un emittente di token affidabile](#).

#### Note

La configurazione di un emittente di token attendibile non è richiesta per tutte le connessioni esterne. La connessione al database Redshift con l'Editor di query Amazon Redshift v2 non richiede la configurazione di un emittente di token attendibile. Può invece essere eseguita per applicazioni di terze parti come pannelli di controllo o applicazioni personalizzate che si autenticano con il tuo gestore dell'identità digitale.

- Configurazione di uno o più ruoli IAM: nelle sezioni che seguono sono indicate le autorizzazioni che devono essere configurate. Dovrai aggiungere le autorizzazioni seguendo le best practice IAM. Le autorizzazioni specifiche sono illustrate nelle procedure che seguono.

Per ulteriori informazioni, consulta [Getting Started with IAM Identity Center](#).

## Configurazione del gestore dell'identità digitale per utilizzare il Centro identità IAM

Il primo passaggio per controllare la gestione delle identità di utenti e gruppi consiste nel connettersi al Centro identità IAM e configurare il gestore dell'identità digitale. Puoi utilizzare lo stesso Centro identità IAM come gestore dell'identità digitale oppure puoi connettere un archivio di identità di terze parti, ad esempio Okta. Per ulteriori informazioni sulla configurazione della connessione e del gestore dell'identità digitale, consulta [Connect to an external identity provider](#) nella Guida per l'utente di Centro identità IAM. Alla fine di questo processo, assicurati di aggiungere una piccola raccolta di utenti e gruppi al Centro identità IAM, a scopo di test.

## Autorizzazioni di amministrazione

Autorizzazioni richieste per la gestione del ciclo di vita delle applicazioni Redshift/IAM Identity Center

È necessario creare un'identità IAM, che un amministratore di Redshift utilizza per configurare Redshift da utilizzare con IAM Identity Center. Nella maggior parte dei casi, è necessario creare un ruolo IAM con autorizzazioni e assegnarlo ad altre identità, se necessario. Deve disporre delle autorizzazioni elencate per eseguire le seguenti azioni.

## Creazione dell'applicazione Redshift/IAM Identity Center

- `sso:PutApplicationAssignmentConfiguration`: utilizzato per la sicurezza.
- `sso:CreateApplication`: utilizzato per creare un'applicazione Centro identità IAM.

- `sso:PutApplicationAuthenticationMethod`: fornisce l'accesso all'autenticazione Redshift.
- `sso:PutApplicationGrant`: utilizzato per modificare le informazioni sull'emittente di token attendibile.
- `sso:PutApplicationAccessScope`: utilizzato per la configurazione dell'applicazione Centro identità IAM per Redshift. Ciò include per AWS Lake Formation e per [Amazon S3 Access](#) Grants.
- `redshift:CreateRedshiftIdcApplication`: utilizzato per creare l'applicazione Centro identità Redshift.

### Descrizione dell'applicazione RedShift/IAM Identity Center

- `sso:GetApplicationGrant`: utilizzato per elencare informazioni sull'emittente di token attendibile.
- `sso:ListApplicationAccessScopes`— Per la configurazione dell'applicazione Redshift IAM Identity Center per elencare le integrazioni downstream, come for AWS Lake Formation e S3 Access Grants.
- `redshift:DescribeRedshiftIdcApplications`— Utilizzato per descrivere le applicazioni IAM Identity Center esistenti.

### Modifica dell'applicazione Redshift/IAM Identity Center

- `redshift:ModifyRedshiftIdcApplication`: utilizzato per modificare un'applicazione Redshift esistente.
- `sso:UpdateApplication`: utilizzato per aggiornare un'applicazione Centro identità IAM.
- `sso:GetApplicationGrant`— Ottiene le informazioni sull'emittente del token di fiducia.
- `sso:ListApplicationAccessScopes`: utilizzato per la configurazione dell'applicazione Centro identità IAM per Redshift.
- `sso>DeleteApplicationGrant`: elimina le informazioni sull'emittente di token attendibile.
- `sso:PutApplicationGrant`: utilizzato per modificare le informazioni sull'emittente di token attendibile.
- `sso:PutApplicationAccessScope`: utilizzato per la configurazione dell'applicazione Centro identità IAM per Redshift. Ciò include per AWS Lake Formation e per [Amazon S3 Access](#) Grants.
- `sso>DeleteApplicationAccessScope`— Per eliminare la configurazione dell'applicazione Redshift IAM Identity Center. Ciò include per AWS Lake Formation e per [Amazon S3 Access](#) Grants.

## Eliminazione dell'applicazione Redshift/IAM Identity Center

- `sso:DeleteApplication`: utilizzato per eliminare un'applicazione Centro identità IAM.
- `redshift:DeleteRedshiftIdcApplication`: offre la possibilità di eliminare un'applicazione Centro identità Redshift esistente.

## Autorizzazioni richieste per la gestione del ciclo di vita delle applicazioni RedShift/Query Editor v2

È necessario creare un'identità IAM, che un amministratore di Redshift utilizza per configurare Redshift da utilizzare con IAM Identity Center. Nella maggior parte dei casi, è necessario creare un ruolo IAM con autorizzazioni e assegnarlo ad altre identità, se necessario. Deve disporre delle autorizzazioni elencate per eseguire le seguenti azioni.

## Creazione dell'applicazione Query Editor v2

- `redshift:CreateQev2IdcApplication`— Utilizzato per creare l'applicazione QEV2.
- `sso:CreateApplication`— Offre la possibilità di creare un'applicazione IAM Identity Center.
- `sso:PutApplicationAuthenticationMethod`: fornisce l'accesso all'autenticazione Redshift.
- `sso:PutApplicationGrant`: utilizzato per modificare le informazioni sull'emittente di token attendibile.
- `sso:PutApplicationAccessScope`: utilizzato per la configurazione dell'applicazione Centro identità IAM per Redshift. È incluso l'editor di query v2.
- `sso:PutApplicationAssignmentConfiguration`: utilizzato per la sicurezza.

## Descrivi l'applicazione Query Editor v2

- `redshift:DescribeQev2IdcApplications`— Utilizzato per descrivere l'applicazione IAM Identity Center QEV2.

## Cambia l'applicazione Query Editor v2

- `redshift:ModifyQev2IdcApplication`— Utilizzato per modificare l'applicazione IAM Identity Center QEV2.
- `sso:UpdateApplication`— Utilizzato per modificare l'applicazione IAM Identity Center QEV2.

## Eliminare l'applicazione Query Editor v2

- `redshift:DeleteQev2IdcApplication`— Utilizzato per eliminare l'applicazione QEV2.
- `sso:DeleteApplication`— Utilizzato per eliminare l'applicazione QEV2.

### Note

Nell'SDK Amazon Redshift, le seguenti API non sono disponibili:

- `CreateQev2 IdcApplication`
- `DescribeQev2 IdcApplications`
- `ModifyQev2 IdcApplication`
- `DeleteQev2 IdcApplication`

Queste azioni sono specifiche per eseguire l'integrazione di IAM Identity Center con Redshift QEV2 nella console. AWS Per ulteriori informazioni, consulta [Azioni definite da Amazon Redshift](#).

Autorizzazioni richieste all'amministratore del database per connettere nuove risorse nella console

Le seguenti autorizzazioni sono necessarie per connettere nuovi cluster con provisioning o gruppi di lavoro Amazon Redshift serverless durante il processo di creazione. Se disponi di queste autorizzazioni, nella console viene visualizzata la selezione per connettersi all'applicazione gestita dal Centro identità IAM per Redshift.

- `redshift:DescribeRedshiftIdcApplications`
- `sso:ListApplicationAccessScopes`
- `sso:GetApplicationAccessScope`
- `sso:GetApplicationGrant`

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

## Configurazione di Redshift come applicazione AWS gestita con IAM Identity Center

Prima che il Centro identità IAM possa gestire le identità di un cluster con provisioning Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless, l'amministratore di Redshift deve completare i passaggi per rendere Redshift un'applicazione gestita dal Centro identità IAM:

1. Seleziona Integrazione del Centro identità IAM nel menu della console Amazon Redshift o Amazon Redshift serverless, quindi seleziona Connessione al Centro identità IAM. Quindi, esegui una serie di selezioni per compilare le proprietà dell'integrazione con il Centro identità IAM.
2. Scegli un nome visualizzato e un nome univoco per l'applicazione gestita dal Centro identità di Redshift.
3. Specifica lo spazio dei nomi dell'organizzazione. In genere è una versione abbreviata del nome dell'organizzazione che viene aggiunta come prefisso per gli utenti e i ruoli gestiti dal Centro identità nel database Redshift.
4. Seleziona un ruolo IAM da utilizzare. Questo ruolo IAM deve essere separato da quelli utilizzati per Redshift e consigliamo di non usarlo per altri scopi. Le specifiche autorizzazioni policy richieste sono riportate di seguito:
  - `sso:DescribeApplication`: necessario per creare una voce del gestore dell'identità digitale nel catalogo.
  - `sso:DescribeInstance`: utilizzato per creare manualmente ruoli o utenti federati del gestore dell'identità digitale.
5. Configura le connessioni client e gli emittenti di token attendibili. La configurazione di emittenti di token attendibili facilita la propagazione delle identità attendibili impostando una relazione con un gestore dell'identità digitale esterno. La propagazione dell'identità consente a un utente, ad esempio, di accedere a un'applicazione e a dati specifici in un'altra applicazione. In tal modo gli utenti possono raccogliere dati da diverse postazioni in modo più semplice. In questa fase, si impostano nella console gli attributi per ogni emittente di token attendibile. Gli attributi includono il nome e l'attestazione del pubblico (o `aud claim`), che potresti dover ricavare dagli attributi di configurazione dello strumento o del servizio. Inoltre, potrebbe essere necessario fornire il nome dell'applicazione dal JSON Web Token (JWT) dello strumento di terze parti.

### Note

L'attributo `aud claim` richiesto da ogni strumento o servizio di terze parti può variare in base al tipo di token, che può essere un token di accesso emesso da un gestore

dell'identità digitale o un altro tipo, come un token ID. Ogni fornitore può essere diverso. Quando si implementa la propagazione di identità attendibili e si integra con Redshift, è necessario fornire il valore `aud` corretto per il tipo di token che lo strumento di terze parti invia ad AWS. Consulta i suggerimenti del provider di strumenti o servizi.

Per informazioni dettagliate sulla propagazione delle identità attendibili, consulta [How trusted identity propagation works](#). Inoltre, consulta la documentazione beta del Centro identità IAM a cui fa riferimento la presente guida.

Dopo che l'amministratore di Redshift ha completato i passaggi e salvato la configurazione, le proprietà del Centro identità IAM vengono visualizzate nella console Redshift. Puoi anche eseguire query sulla vista di sistema [SVV\\_IDENTITY\\_PROVIDERS](#) per verificare le proprietà dell'applicazione, che includono il nome dell'applicazione e lo spazio dei nomi. Lo spazio dei nomi viene utilizzato come prefisso per gli oggetti del database Redshift associati all'applicazione. Il completamento di queste attività rende Redshift un'applicazione abilitata per il Centro identità IAM. Le proprietà della console includono lo stato dell'integrazione. Quando l'integrazione è completata, lo stato è Abilitato. Dopo questo processo, l'integrazione del Centro identità IAM può essere abilitata su ogni nuovo cluster.

Dopo la configurazione, puoi includere gli utenti e i gruppi del Centro identità IAM in Redshift scegliendo la scheda Utenti o Gruppi e selezionando Assegna.

Abilitazione dell'integrazione del Centro identità IAM per un nuovo cluster Amazon Redshift o un gruppo di lavoro Amazon Redshift serverless

L'amministratore del database configura le nuove risorse Redshift in modo che funzionino in linea con il Centro identità IAM per semplificare l'accesso ai dati. Questa operazione viene eseguita come parte dei passaggi per creare un cluster con provisioning o un gruppo di lavoro serverless. Chiunque disponga delle autorizzazioni per creare risorse Redshift può eseguire queste attività di integrazione del Centro identità IAM. Per creare un cluster con provisioning, inizi scegliendo Crea cluster nella console Amazon Redshift. Di seguito viene mostrato come abilitare la gestione del Centro identità IAM per un database, ma non sono inclusi tutti i passaggi per creare un cluster.

1. Scegli Abilita per <nome del cluster> nella sezione Integrazione con il Centro identità IAM nei passaggi di creazione del cluster.
2. C'è un passaggio del processo in cui abiliti l'integrazione. Puoi farlo scegliendo Abilita l'integrazione con il Centro identità IAM nella console.

3. Per il nuovo cluster o gruppo di lavoro, crea i ruoli di database in Redshift utilizzando i comandi SQL. Il comando è il seguente:

```
CREATE ROLE <idcnamespace:rolename>;
```

Lo spazio dei nomi e il nome del ruolo sono i seguenti:

- Prefisso dello spazio dei nomi del Centro identità IAM: è lo spazio dei nomi definito durante la configurazione della connessione tra il Centro identità IAM e Redshift.
- Nome ruolo: questo ruolo del database Redshift deve corrispondere al nome del gruppo nel Centro identità IAM.

Redshift si connette al Centro identità IAM e recupera le informazioni necessarie per creare e mappare il ruolo del database al gruppo del Centro identità IAM.

Tieni presente che quando viene creato un nuovo data warehouse, il ruolo IAM specificato per l'integrazione del Centro identità viene automaticamente collegato al cluster o al gruppo di lavoro Amazon Redshift serverless fornito. Dopo aver inserito i metadati del cluster richiesti e aver creato la risorsa, puoi verificare lo stato dell'integrazione del Centro identità IAM nelle proprietà. Se i nomi dei gruppi nel Centro identità IAM contengono spazi, è necessario utilizzare le virgolette in SQL quando si crea il ruolo corrispondente.

Dopo aver abilitato il database Redshift e creato i ruoli, puoi connetterti al database con l'Editor di query Amazon Redshift v2 o Amazon QuickSight. I dettagli sono spiegati ampiamente nelle sezioni che seguono.

### Configurazione dell'impostazione predefinita di **RedshiftIdcApplication** tramite l'API

La configurazione viene eseguita dall'amministratore delle identità. Utilizzando l'API, crei e compili `RedshiftIdcApplication` che rappresenta l'applicazione Redshift nel Centro identità IAM.

1. Per iniziare, puoi creare gli utenti e aggiungerli ai gruppi nel Centro identità IAM. Questa operazione viene eseguita nella AWS console di IAM Identity Center (IDC).
2. Chiama `create-redshift-idc-application` per creare un'applicazione Centro identità e renderla compatibile per l'utilizzo di Redshift. L'applicazione viene creata inserendo i valori richiesti. Il nome visualizzato è quello che viene mostrato nel pannello di controllo del Centro

identità. L'ARN del ruolo IAM è un nome della risorsa Amazon che dispone delle autorizzazioni per il Centro identità IAM e può essere utilizzato anche da Redshift.

```
aws redshift create-redshift-idc-application
--idc-instance-arn 'arn:aws:sso:::instance/ssoins-1234a01a1b12345d'
--identity-namespace 'MYCO'
--idc-display-name 'TEST-NEW-APPLICATION'
--iam-role-arn 'arn:aws:redshift:us-east-1:012345678901:role/TestRedshiftRole'
--redshift-idc-application-name 'myredshiftidcapplication'
```

L'esempio seguente mostra la risposta `RedshiftIdcApplication` restituita dalla chiamata a `create-redshift-idc-application`.

```
"RedshiftIdcApplication": {
  "IdcInstanceArn": "arn:aws:sso:::instance/ssoins-1234a01a1b12345d",
  "RedshiftIdcApplicationName": "test-application-1",
  "RedshiftIdcApplicationArn": "arn:aws:redshift:us-
east-1:012345678901:redshiftidcapplication:12aaa111-3ab2-3ab1-8e90-b2d72aea588b",
  "IdentityNamespace": "MYCO",
  "IdcDisplayName": "Redshift-Idc-Application",
  "IamRoleArn": "arn:aws:redshift:us-east-1:012345678901:role/
TestRedshiftRole",
  "IdcManagedApplicationArn": "arn:aws:sso:::012345678901:application/
ssoins-1234a01a1b12345d/apl-12345678910",
  "IdcOnboardStatus": "arn:aws:redshift:us-
east-1:123461817589:redshiftidcapplication",
  "RedshiftIdcApplicationArn": "Completed",
  "AuthorizedTokenIssuerList": [
    "TrustedTokenIssuerArn": ...,
    "AuthorizedAudiencesList": [...]...
  ]
}
```

3. Puoi usare `create-application-assignment` per assegnare gruppi particolari o singoli utenti all'applicazione gestita nel Centro identità IAM. In questo modo, puoi specificare i gruppi da gestire tramite il Centro identità IAM. Se l'amministratore del database crea i ruoli del database in Redshift, i nomi dei gruppi nel Centro identità IAM vengono mappati ai nomi dei ruoli in Redshift. I ruoli controllano le autorizzazioni nel database. Per ulteriori informazioni, consulta [Assign user access to applications in the IAM Identity Center console](#).

4. Dopo aver abilitato l'applicazione, chiama `create-cluster` e includi l'ARN dell'applicazione gestita da Redshift del Centro identità IAM. In questo modo il cluster viene associato all'applicazione gestita nel Centro identità IAM.

## Associazione di un'applicazione Centro identità IAM a un cluster o un gruppo di lavoro esistente

Se disponi di un cluster o un gruppo di lavoro e desideri abilitarlo per l'integrazione con il Centro identità IAM, puoi eseguire un comando SQL. Per abilitare l'integrazione, esegui il comando riportato di seguito. È necessario che la query venga eseguita da un amministratore del database e che la connessione tra Redshift e il Centro identità IAM sia già stata configurata. Una volta impostato `ENABLE`, il Centro identità IAM può eseguire la gestione delle identità per il cluster o il gruppo di lavoro.

```
ALTER IDENTITY PROVIDER
<idp_name> | NAMESPACE <namespace> | IAM_ROLE default | 'arn:aws:iam::<AWS account-
id-1>:role/<role-name>' | [DISABLE | ENABLE]
```

È possibile eliminare un gestore dell'identità digitale esistente. L'esempio seguente mostra come `CASCADE` elimina gli utenti e i ruoli collegati al gestore dell'identità digitale.

```
DROP IDENTITY PROVIDER
<provider_name> [ CASCADE ]
```

## Impostazione delle autorizzazioni degli utenti

L'amministratore configura le autorizzazioni per varie risorse, in base agli attributi di identità degli utenti e all'appartenenza ai gruppi, all'interno del gestore dell'identità digitale o direttamente nel Centro identità IAM. Ad esempio, l'amministratore del gestore dell'identità digitale può aggiungere un ingegnere di database al gruppo appropriato al suo ruolo. Questo nome di gruppo corrisponde a un nome di ruolo del database Redshift. Il ruolo fornisce o limita l'accesso a tabelle o viste specifiche in Redshift.

## Utenti tipo amministratore per il collegamento delle applicazioni

Di seguito sono riportati gli utenti tipo per connettere le applicazioni di analisi all'applicazione gestita dal Centro identità IAM per Redshift:

- Amministratore dell'applicazione: crea un'applicazione e configura i servizi con cui abilita gli scambi di token di identità. Questo amministratore specifica inoltre quali utenti o gruppi hanno accesso all'applicazione.
- Amministratore dei dati: configura l'accesso granulare ai dati. Gli utenti e i gruppi del Centro identità IAM possono essere mappati ad autorizzazioni specifiche.

## Connessione ad Amazon Redshift con IAM Identity Center tramite Amazon QuickSight

Di seguito viene illustrato come utilizzare Amazon QuickSight per l'autenticazione con Redshift quando è connesso e l'accesso è gestito tramite IAM Identity Center: [Autorizzazione delle connessioni da Amazon ai cluster QuickSight Amazon Redshift](#). I passaggi illustrati si applicano anche ad Amazon Redshift serverless.

## Connessione ad Amazon Redshift con il Centro identità IAM tramite l'Editor di query Amazon Redshift v2

Dopo aver completato i passaggi per configurare la connessione del Centro identità IAM con Redshift, l'utente può accedere al database e agli oggetti appropriati nel database con l'identità basata sul Centro identità IAM e lo spazio dei nomi come prefisso. Per ulteriori informazioni sulla connessione ai database Redshift con l'editor di query v2, consulta [Utilizzo dell'editor di query v2](#).

## Interrogazione dei dati tramite AWS Lake Formation

L'utilizzo AWS Lake Formation semplifica la gestione e la protezione centralizzate del data lake e l'accesso ai dati. Con la configurazione della propagazione delle identità su Lake Formation tramite il Centro identità IAM e Redshift, l'amministratore può definire l'accesso granulare a un data lake Amazon S3, in base ai gruppi di gestori dell'identità digitale dell'organizzazione. Questi gruppi sono gestiti tramite il Centro identità IAM. In questa sezione viene illustrato come configurare un paio di casi d'uso, l'esecuzione di query da un data lake e l'esecuzione di query da un'unità di condivisione dati, che dimostrano come utilizzare il Centro identità IAM con Redshift per connettersi alle risorse gestite da Lake Formation.

Utilizzo del Centro identità IAM connesso a Redshift per l'esecuzione di query su un data lake

Questi passaggi si riferiscono al caso d'uso in cui utilizzi il Centro identità IAM connesso a Redshift per eseguire query su un data lake gestito da Lake Formation.

### Prerequisiti

Questa procedura prevede diversi prerequisiti:

1. Il Centro identità IAM deve essere configurato per supportare l'autenticazione e la gestione delle identità con Redshift. Puoi abilitare il Centro identità IAM dalla console e selezionare un'origine del gestore dell'identità digitale. Dopodiché, sincronizza un set di utenti del gestore dell'identità digitale con il Centro identità IAM. Inoltre dovrai configurare una connessione tra il Centro identità IAM e Redshift, seguendo i passaggi descritti in precedenza in questo documento.
2. Crea un nuovo cluster Amazon Redshift e abilita la gestione delle identità tramite il Centro identità IAM nei passaggi di configurazione.
3. Crea un'applicazione Centro identità IAM gestita per Lake Formation e configurala. Quindi, configura la connessione tra il Centro identità IAM e Redshift. Di seguito sono riportati i passaggi:
  - a. Nella AWS CLI, utilizza il comando `modify-redshift-idc-application` per abilitare l'integrazione del servizio Lake Formation con l'applicazione gestita Centro identità IAM per Redshift. Questa chiamata include il parametro `service-integrations`, che è impostato su un valore di stringa di configurazione che consente l'autorizzazione per Lake Formation.
  - b. Configura Lake Formation utilizzando il comando `create-lake-formation-identity-center-configuration`, che crea un'applicazione Centro identità IAM per Lake Formation, visibile nel portale Centro identità IAM. L'amministratore deve impostare `--cli-input-json` argomento, il cui valore è il percorso di un file JSON che utilizza il formato standard per tutte le chiamate API AWS CLI. È necessario specificare i seguenti valori:
    - `CatalogId`: l'ID catalogo di Lake Formation.
    - `InstanceArn`: il valore ARN dell'istanza Centro identità IAM.

Una volta completata la configurazione dei prerequisiti, l'amministratore del database può creare uno schema esterno allo scopo di eseguire query sul data lake.

1. L'amministratore crea lo schema esterno: l'amministratore del database Redshift si connette al database e crea uno schema esterno, utilizzando la seguente istruzione SQL:

```
CREATE EXTERNAL SCHEMA if not exists my_external_schema from DATA CATALOG database
'my_lf_integrated_db' catalog_id '12345678901234';
```

Tieni presente che in questo caso non è necessario specificare un ruolo IAM perché l'accesso è gestito tramite il Centro identità IAM.

2. L'amministratore fornisce le autorizzazioni: l'amministratore assegna l'utilizzo a un gruppo del Centro identità IAM che fornisce le autorizzazioni per le risorse Redshift. Per farlo, esegue un'istruzione SQL come la seguente:

```
GRANT USAGE ON SCHEMA "my_external_schema" to "MYC0:sales";
```

Successivamente, l'amministratore concede le autorizzazioni di Lake Formation sugli oggetti, in base ai requisiti dell'organizzazione, utilizzando la AWS CLI:

```
aws lakeformation grant-permissions ...
```

3. Gli utenti eseguono le query: a questo punto, un utente del Centro identità IAM che fa parte del gruppo di vendita, a scopo illustrativo, può accedere tramite l'editor di query v2 al database Redshift. Quindi può eseguire una query che accede a una tabella nello schema esterno, come nell'esempio seguente:

```
SELECT * from my_external_schema.table1;
```

Utilizzo del Centro identità IAM connesso a Redshift per la connessione a un'unità di condivisione dati

Puoi accedere a un'unità di condivisione dati da un data warehouse Redshift diverso quando l'accesso è gestito tramite il Centro identità IAM. A tale scopo, esegui una query per configurare un database esterno. Prima di completare questi passaggi, si presuppone che tu abbia configurato una connessione tra Redshift e IAM Identity Center e che tu abbia creato l' AWS Lake Formation applicazione, come descritto nella procedura precedente.

1. Creazione del database esterno: l'amministratore crea un database esterno per la condivisione dei dati usando come riferimento il relativo ARN. Di seguito è riportato un esempio che mostra come eseguire questa operazione:

```
CREATE DATABASE "redshift_external_db" FROM ARN 'arn:aws:glue:us-east-1:123456789012:database/redshift_external_db-iad' WITH NO DATA CATALOG SCHEMA;
```

In questo caso d'uso, in cui si utilizza il Centro identità IAM con Redshift per la gestione delle identità, il ruolo IAM non è incluso.

2. L'amministratore imposta le autorizzazioni: dopo aver creato un database, l'amministratore ne assegna l'utilizzo a un gruppo del Centro identità IAM. In tal modo si forniscono le autorizzazioni per le risorse Redshift:

```
GRANT USAGE ON DATABASE "my_external_db" to "MYC0:sales";
```

L'amministratore concede anche le autorizzazioni di Lake Formation sugli oggetti, utilizzando la CLI AWS :

```
aws lakeformation grant-permissions ...
```

3. Gli utenti eseguono le query: un utente del gruppo di vendita può eseguire le query su una tabella nel database, in base alle autorizzazioni assegnate:

```
select * from redshift_external_db.public.employees;
```

Per ulteriori informazioni sull'assegnazione delle autorizzazioni per un data lake e per le unità di condivisione dati, consulta [Granting permissions to users and groups](#). Per ulteriori informazioni sull'assegnazione dell'utilizzo per uno schema o un database, consulta [GRANT](#).

## Integrazione dell'applicazione o dello strumento con OAuth utilizzando un emittente di token attendibile

Puoi aggiungere funzionalità agli strumenti client che crei per connetterti a Redshift tramite la connessione IAM Identity Center. Se hai già configurato l'integrazione di Redshift con IAM Identity Center, utilizza le proprietà dettagliate in questa sezione per configurare una connessione.

### Plugin di autenticazione per la connessione a Redshift tramite IAM Identity Center

`IdpTokenAuthPlugin` fornisce proprietà di connessione e facilita l'autenticazione con IAM Identity Center. Accetta un token web JSON (JWT) OpenID Connect (OIDC) da qualsiasi provider di identità web connesso a IAM Identity Center.

Se utilizzi un driver Amazon Redshift, puoi utilizzarlo `IdpTokenAuthPlugin` per l'autenticazione su Redshift con IAM Identity Center. Questo plugin accetta un JWT OIDC da qualsiasi provider di identità web collegato a IAM Identity Center. La tabella seguente descrive in dettaglio le opzioni di connessione da utilizzare per una corretta autenticazione.

Driver	Chiave delle opzioni di connessione	Valore	Note
JDBC	<code>plugin_name</code>	<code>com.amazon.redshift.plugin.IdpTokenAuthPlugin</code>	È necessario inserire il nome completo della classe del plugin quando ci si connette.
ODBC	<code>plugin_name</code>	<code>IdpTokenAuthPlugin</code>	
Python	<code>credentials_provider</code>	<code>IdpTokenAuthPlugin</code>	Non è disponibile alcuna <code>plugin_name</code> opzione per il driver Python. Utilizza invece <code>credentials_provider</code> .

Il plugin ha queste opzioni di connessione aggiuntive:

- `token`: un JSON Web Token (JWT) OpenID Connect (OIDC) fornito da un provider di identità Web collegato a IAM Identity Center. L'applicazione deve generare questo token autenticando l'utente dell'applicazione con un provider di identità connesso a IAM Identity Center.
- `token_type` — Il tipo di token utilizzato per. `IdpTokenAuthPlugin` È possibile specificare i valori per la seguente opzione:
  - `EXT_JWT` — Fornisci questa opzione se utilizzi un JSON Web Token (JWT) OpenID Connect (OIDC) fornito da un provider di identità basato sul Web connesso a IAM Identity Center.

È necessario inserire questi valori nelle proprietà di connessione dello strumento creato e con cui ci si connette. Per ulteriori informazioni, consultate la documentazione sulle opzioni di connessione per ogni rispettivo driver:

- [Opzioni per la configurazione del driver JDBC versione 2.1](#)
- [Configurazione delle opzioni del driver ODBC](#)
- [Opzioni di configurazione per il connettore Amazon Redshift Python](#)

## Risoluzione dei problemi di connessione da Amazon Redshift Query Editor v2

Questo elenco descrive in dettaglio gli errori che si verificano comunemente e può aiutarti a connetterti al tuo database Redshift con l'editor di query v2, utilizzando un'identità IAM Identity Center.

- **Errore: problema di connessione: nessuna informazione disponibile sulla sessione dell'Identity Center.** — Quando si verifica questo errore, controlla le impostazioni di sicurezza e privacy del browser. Queste impostazioni del browser, in particolare quelle per i cookie sicuri, come la funzione Total Cookie Protection di Firefox, possono comportare il blocco dei tentativi di connessione dall'editor di query di Amazon Redshift v2 a un database Redshift. Segui i passaggi di riparazione dettagliati per il tuo browser:
  - **Firefox:** attualmente, i cookie di terze parti sono bloccati per impostazione predefinita. Fai clic sullo scudo nella barra degli indirizzi del browser e attiva l'interruttore per disattivare la protezione antitracciamento avanzata per Query Editor v2.
  - **Modalità di navigazione in incognito di Chrome:** per impostazione predefinita, la modalità di navigazione in incognito di Chrome blocca i cookie di terze parti. Fai clic sull'icona a forma di occhio nella barra degli indirizzi per consentire i cookie di terze parti per l'editor di query v2. Dopo aver modificato l'impostazione per consentire i cookie, potresti non vedere l'icona a forma di occhio sulla barra degli indirizzi.
  - **Safari:** su Mac, apri l'app Safari. Scegli Impostazioni, quindi scegli Avanzate. Attiva per disattivare: blocca tutti i cookie.
  - **Edge:** scegli Impostazioni, quindi scegli Cookie e autorizzazioni del sito. Quindi seleziona Gestisci ed elimina i cookie e i dati dei siti e disattiva Blocca i cookie di terze parti.

Se provi a connetterti dopo aver modificato le impostazioni e continui a ricevere il messaggio di errore Problema di connessione: nessuna informazione sulla sessione dell'Identity Center disponibile, ti consigliamo di aggiornare la connessione con IAM Identity Center. Per fare ciò, fai clic con il pulsante destro del mouse sull'istanza del database Redshift e scegli Aggiorna. Viene visualizzata una nuova finestra che puoi utilizzare per l'autenticazione.

- **Errore: problema di connessione: sessione dell'Identity Center scaduta o non valida.** — Dopo l'integrazione di un cluster o di un gruppo di lavoro Serverless con provisioning Redshift con IAM Identity Center, un utente potrebbe ricevere questo errore quando tenta di connettersi a un database Redshift dall'editor di query v2. Ciò può essere dovuto a tentativi di connessione riusciti. In questo caso, ti consigliamo di effettuare nuovamente l'autenticazione. Per fare ciò, fai clic con il

pulsante destro del mouse sull'istanza del database Redshift e scegli **Aggiorna**. Viene visualizzata una nuova finestra che puoi utilizzare per l'autenticazione.

- **Errore: ambito non valido.** Le credenziali utente non sono autorizzate a connettersi a Redshift. — Dopo l'integrazione di un cluster o di un gruppo di lavoro Serverless con provisioning Redshift con IAM Identity Center per la gestione delle identità, un utente potrebbe ricevere questo errore quando tenta di connettersi a un database Redshift dall'editor di query v2. In questo caso, affinché Query Editor v2 possa connettersi e autenticare correttamente un utente tramite IAM Identity Center per accedere alle risorse corrette, un amministratore deve assegnare l'utente all'applicazione Redshift IAM Identity Center tramite la console Redshift. Questa operazione viene completata nelle connessioni IAM Identity Center. Successivamente, l'utente può stabilire una connessione riuscita dopo un'ora, che è il limite della memorizzazione nella cache delle sessioni di IAM Identity Center.
- **Errore: i database non possono essere elencati. FATALE: interrogazione non riuscita** quando il cluster viene messo in pausa automaticamente. — Quando un database Serverless Amazon Redshift è inattivo e non elabora alcun carico di lavoro, può rimanere in pausa quando ti connetti con un'identità IAM Identity Center. Per ovviare a questo problema, accedi con un altro metodo di autenticazione per riprendere il gruppo di lavoro Serverless. Quindi connettiti al database con la tua identità IAM Identity Center.
- **Errore: si è verificato un errore durante il tentativo di federazione con IAM Identity Center.** Un amministratore di Amazon Redshift deve eliminare e ricreare l'applicazione IAM Identity Center QEV2 utilizzando la console Redshift. — Questo errore si verifica in genere quando l'istanza dell'applicazione IAM Identity Center associata a Query Editor v2 viene eliminata. Per ovviare a questo problema, un amministratore di Amazon Redshift deve eliminare e ricreare le applicazioni Redshift e Query Editor v2 per IAM Identity Center. Questa operazione può essere eseguita sulla console Redshift o utilizzando il comando CLI <https://docs.aws.amazon.com/cli/latest/reference/redshift/delete-redshift-idc-application.html>.

## Limitazioni

Si applicano le limitazioni indicate di seguito:

- **Utilizzo di IAM Identity Center con i driver Redshift:** quando si utilizza `IdpTokenAuthPlugin`, disponibile tramite gli attuali driver Redshift, è necessario che l'applicazione client generi il token di autenticazione. Tuttavia, tieni presente che AWS IAM Identity Center attualmente non supporta la generazione di un token di accesso per Redshift. Pertanto, l'utilizzo di un token di accesso IAM Identity Center non è supportato. Attualmente è possibile connettersi `IdpTokenAuthPlugin` a un database Amazon Redshift tramite un provider di identità Web esterno, come Okta, PingOne

o Microsoft Entra ID (Azure AD), integrato con IAM Identity Center. In questo caso, il client è responsabile della generazione di un token Web JSON (JWT) OpenID Connect (OIDC) dal provider di identità Web e della sua fornitura come input al driver. `IdpTokenAuthPlugin` Il plugin è descritto nella sezione precedente. Puoi anche connetterti utilizzando l'editor di query v2, se desideri utilizzare direttamente l'autorizzazione e l'autenticazione di IAM Identity Center.

- Nessun supporto per VPC avanzato: il VPC avanzato non è supportato quando si configura la propagazione delle identità affidabili di Redshift con IAM Identity Center. Per ulteriori informazioni sul VPC avanzato, consulta Routing [VPC avanzato in Amazon Redshift](#).
- Memorizzazione nella cache di IAM Identity Center: IAM Identity Center memorizza nella cache le informazioni sulla sessione. Ciò potrebbe causare problemi di accesso imprevedibili quando si tenta di connettersi al database Redshift tramite Redshift query editor v2. Questo perché la sessione IAM Identity Center associata nell'editor di query v2 rimane valida, anche nel caso in cui l'utente del database sia disconnesso dalla console. AWS La cache scade dopo un'ora, il che in genere risolve eventuali problemi.

## Utilizzo di ruoli collegati ai servizi per Amazon Redshift

Amazon Redshift utilizza ruoli collegati ai [servizi AWS Identity and Access Management \(IAM\)](#). Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Amazon Redshift. I ruoli collegati ai servizi sono predefiniti da Amazon Redshift e includono tutte le autorizzazioni richieste dal servizio per chiamare i AWS servizi per conto del tuo cluster Amazon Redshift.

Un ruolo legato a un servizio rende la configurazione di Amazon Redshift più facile perché non è necessario aggiungere manualmente i permessi necessari. Il ruolo è collegato a casi d'uso di Amazon Redshift e ha autorizzazioni predefinite. Solo Amazon Redshift può assumere il ruolo e solo questo ruolo collegato ai servizi può utilizzare la policy di autorizzazione predefinita. Amazon Redshift crea un ruolo collegato ai servizi nel tuo account la prima volta che crei un cluster o un endpoint VPC gestito da Redshift. Puoi eliminare il ruolo collegato al servizio solo dopo aver eliminato tutti i cluster Amazon Redshift o gli endpoint VPC gestiti da Redshift nel tuo account. Così facendo, le risorse Amazon Redshift restano protette, perché non puoi rimuovere inavvertitamente le autorizzazioni necessarie per l'accesso alle risorse.

Amazon Redshift supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consultare [Regioni ed endpoint di AWS](#).

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consultare [Servizi AWS che funzionano con IAM](#) e cercare i servizi che riportano Yes (Sì) nella colonna Service-Linked Role

(Ruolo associato ai servizi). Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

## Autorizzazioni del ruolo collegato ai servizi per Amazon Redshift

Amazon Redshift utilizza il ruolo collegato ai servizi denominato: consente ad AWSServiceRoleForRedshiftAmazon Redshift di chiamare i servizi per tuo conto.

AWS Questo ruolo collegato ai servizi è collegato alle seguenti policy gestite:

AmazonRedshiftServiceLinkedRolePolicy. Per gli aggiornamenti di questa policy, consultare [Policy gestite da AWS\(predefinite\) per Amazon Redshift](#).

Il ruolo AWSServiceRoleForRedshift collegato ai servizi si fida solo dell'assunzione del ruolo.

**redshift.amazonaws.com**

La politica AWSServiceRoleForRedshift di autorizzazione dei ruoli collegati ai servizi consente ad Amazon Redshift di completare quanto segue su tutte le risorse correlate:

- ec2:DescribeVpcs
- ec2:DescribeSubnets
- ec2:DescribeNetworkInterfaces
- ec2:DescribeAddress
- ec2:AssociateAddress
- ec2:DisassociateAddress
- ec2:CreateNetworkInterface
- ec2>DeleteNetworkInterface
- ec2:ModifyNetworkInterfaceAttribute
- ec2:CreateVpcEndpoint
- ec2>DeleteVpcEndpoints
- ec2:DescribeVpcEndpoints
- ec2:ModifyVpcEndpoint
- ec2:DescribeVpcAttribute
- ec2:DescribeSecurityGroups
- ec2:DescribeInternetGateways
- ec2:DescribeSecurityGroupRules
- ec2:DescribeAvailabilityZones

- `ec2:DescribeNetworkAcls`
- `ec2:DescribeRouteTables`
- `ec2:AssignIpv6Addresses`
- `ec2:UnassignIpv6Addresses`

### Autorizzazioni per risorse di rete

Le seguenti autorizzazioni consentono operazioni su Amazon EC2 per la creazione e la gestione di regole dei gruppi di sicurezza. Queste regole e gruppi di sicurezza sono specificamente associati al tag delle risorse `aws:RequestTag/Redshift` di Amazon Redshift. Ciò limita l'ambito delle autorizzazioni a risorse specifiche di Amazon Redshift.

- `ec2:CreateSecurityGroup`
- `ec2:AuthorizeSecurityGroupEgress`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:ModifySecurityGroupRules`
- `ec2>DeleteSecurityGroup`

### Operazioni per il logging di verifica

Le azioni elencate con il prefisso `logs` riguardano il logging di verifica e le funzionalità correlate. Nello specifico, creazione e gestione di gruppi di log e flussi di log.

- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `logs:CreateLogStream`
- `logs:PutLogEvents`
- `logs:DescribeLogStreams`
- `logs:GetLogEvents`

Il seguente JSON mostra le operazioni e l'ambito delle risorse, ad Amazon Redshift, per il logging di verifica.

```
[
  {
    "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogGroups",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogGroup",
      "logs:PutRetentionPolicy"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*"
    ]
  },
  {
    "Sid": "EnableCreationAndManagementOfRedshiftCloudwatchLogStreams",
    "Effect": "Allow",
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents",
      "logs:DescribeLogStreams",
      "logs:GetLogEvents"
    ],
    "Resource": [
      "arn:aws:logs:*:*:log-group:/aws/redshift/*:log-stream:*"
    ]
  }
]
```

[Per ulteriori informazioni sui ruoli collegati ai servizi e sul loro scopo, consulta Using service-linked roles. AWS](#) Per ulteriori informazioni su operazioni specifiche e altre risorse IAM per Amazon Redshift, consultare [Operazioni, risorse e chiavi di condizione per Amazon Redshift](#).

### Azioni per la gestione delle credenziali di amministratore con AWS Secrets Manager

Le azioni elencate con il prefisso `secretsmanager` riguardano l'utilizzo di Amazon Redshift per gestire le credenziali di amministratore. Queste azioni consentono ad Amazon Redshift di creare e gestire AWS Secrets Manager i segreti delle credenziali di amministratore.

Il seguente codice JSON mostra le azioni e l'ambito delle risorse, ad Amazon Redshift, per la gestione delle credenziali di amministratore con. AWS Secrets Manager

```
[
  {
```

```

    "Effect": "Allow",
    "Action": [
      "secretsmanager:DescribeSecret",
      "secretsmanager>DeleteSecret",
      "secretsmanager:PutSecretValue",
      "secretsmanager:UpdateSecret",
      "secretsmanager:UpdateSecretVersionStage",
      "secretsmanager:RotateSecret"
    ],
    "Resource": [
      "arn:aws:secretsmanager:*:*:secret:redshift!*"
    ],
    "Condition": {
      "StringEquals": {
        "secretsmanager:ResourceTag/aws:secretsmanager:owningService":
"redshift"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "secretsmanager:GetRandomPassword"
    ],
    "Resource": "*"
  }
]

```

Per consentire a un'entità IAM di creare ruoli collegati ai servizi AWSServiceRoleForRedshift

```

{
  "Effect": "Allow",
  "Action": [
    "iam:CreateServiceLinkedRole"
  ],
  "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/
redshift.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}

```

Per consentire a un'entità IAM di eliminare i ruoli collegati ai servizi AWSServiceRoleForRedshift

Aggiungi la seguente istruzione di policy alle autorizzazioni per l'entità IAM.

```
{
  "Effect": "Allow",
  "Action": [
    "iam:DeleteServiceLinkedRole",
    "iam:GetServiceLinkedRoleDeletionStatus"
  ],
  "Resource": "arn:aws:iam::<AWS-account-ID>:role/aws-service-role/redshift.amazonaws.com/AWSServiceRoleForRedshift",
  "Condition": {"StringLike": {"iam:AWSServiceName": "redshift.amazonaws.com"}}
}
```

In alternativa, puoi utilizzare una policy AWS gestita per [fornire l'accesso completo](#) ad Amazon Redshift.

## Creazione di un ruolo collegato ai servizi per Amazon Redshift

Non è necessario creare manualmente un ruolo collegato al AWSServiceRoleForRedshift servizio. Amazon Redshift crea il ruolo collegato al servizio per te. Se il ruolo AWSServiceRoleForRedshift collegato al servizio è stato eliminato dal tuo account, Amazon Redshift lo crea quando avvii un nuovo cluster Amazon Redshift.

### Important

Se hai utilizzato il servizio Amazon Redshift prima del 18 settembre 2017, quando ha iniziato a supportare ruoli collegati ai servizi, Amazon Redshift ha creato il ruolo nel tuo account. AWSServiceRoleForRedshift Per ulteriori informazioni, consultare [Un nuovo ruolo è apparso nel mio account IAM](#).

## Modifica di un ruolo collegato ai servizi per Amazon Redshift

Amazon Redshift non consente di modificare il ruolo collegato al AWSServiceRoleForRedshift servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. Tuttavia, puoi modificare la descrizione del ruolo utilizzando la console IAM, la AWS Command Line Interface (AWS CLI) o l'API IAM. Per ulteriori informazioni, consultare [Modifica di un ruolo](#) nella Guida per l'utente di IAM.

## Eliminazione di un ruolo collegato ai servizi per Amazon Redshift

Se non è più necessario utilizzare una caratteristica o un servizio che richiede un ruolo collegato ai servizi, ti consigliamo di eliminare quel ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente.

Prima di poter eliminare un ruolo legato a un servizio per un account, è necessario arrestare ed eliminare qualsiasi cluster nell'account. Per ulteriori informazioni, consulta [Chiusura ed eliminazione di cluster](#).

Puoi utilizzare la console IAM AWS CLI, l'API IAM per eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consultare [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

## Utilizzo dell'autenticazione IAM per generare credenziali utente di database

Per gestire l'accesso degli utenti al database Amazon Redshift, puoi generare credenziali di database temporanee in base alle autorizzazioni concesse tramite una policy di autorizzazioni AWS Identity and Access Management (IAM).

In genere, gli utenti di database Amazon Redshift accedono al database fornendo un nome utente e una password. Tuttavia, non è necessario mantenere nomi utente e password nel database Amazon Redshift. In alternativa, puoi configurare il sistema in modo da consentire agli utenti di creare credenziali utente e di accedere al database con le proprie credenziali IAM.

Per ulteriori informazioni, consulta [Provider di identità e federazione](#) nella Guida per l'utente di IAM.

### Argomenti

- [Panoramica](#)
- [Creazione di credenziali IAM temporanee](#)
- [Opzioni per fornire credenziali IAM](#)

## Panoramica

Amazon Redshift fornisce il funzionamento dell'[GetClusterCredentials](#) API per generare credenziali utente temporanee del database. Puoi configurare il tuo client SQL con i driver JDBC o ODBC di Amazon Redshift, i quali gestiscono il processo di chiamata dell'operazione `GetClusterCredentials`. Ciò è possibile recuperando le credenziali utente di database

e stabilendo una connessione tra il client SQL e il database Amazon Redshift. Per chiamare l'operazione `GetClusterCredentials` in modo programmatico, recuperare le credenziali utente e connetterti al database, puoi anche utilizzare la tua applicazione di database.

Se gestisci già le identità degli utenti all'esterno AWS, puoi utilizzare un provider di identità (IdP) conforme al Security Assertion Markup Language (SAML) 2.0 per gestire l'accesso alle risorse di Amazon Redshift. L'IdP può essere configurato per consentire agli utenti federati di accedere a un ruolo IAM. Con quel ruolo IAM, puoi generare credenziali di database temporanee e accedere ai database Amazon Redshift.

Il client SQL richiede un'autorizzazione per chiamare l'operazione `GetClusterCredentials` per tuo conto. Per la gestione di tali autorizzazioni, devi creare un ruolo IAM e collegare una policy di autorizzazione IAM che concede o limita l'accesso all'operazione `GetClusterCredentials` e alle operazioni correlate. Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

La policy concede o limita anche l'accesso a specifiche risorse, come cluster Amazon Redshift, database, nomi utente di database e nomi di gruppo utente.

#### Note

Ti consigliamo di utilizzare i driver JDBC o ODBC di Amazon Redshift per gestire il processo di chiamata dell'operazione `GetClusterCredentials` e accedere al database. Per semplicità, in questo argomento considereremo che stai utilizzando un client SQL con driver JDBC o ODBC.

Per dettagli ed esempi specifici sull'utilizzo dell'operazione `GetClusterCredentials` o del comando `get-cluster-credentials` CLI, consulta [GetClusterCredentials](#). [get-cluster-credentials](#)

Per gestire centralmente l'autenticazione e l'autorizzazione, Amazon Redshift supporta l'autenticazione database con IAM, abilitando l'autenticazione utente tramite la federazione aziendale. Invece di creare un utente, puoi utilizzare le identità esistenti in AWS Directory Service, nella tua directory di utenti aziendale o in un provider di identità Web. Questi sono noti come utenti federati. AWS assegna un ruolo a un utente federato quando l'accesso viene richiesto tramite un IdP.

Per fornire l'accesso federato a un utente o un'applicazione client nell'organizzazione per chiamare le operazioni API di Amazon Redshift, puoi anche utilizzare il driver JDBC o ODBC con supporto

SAML 2.0 per richiedere l'autenticazione dal provider di identità dell'organizzazione. In questo caso, gli utenti dell'organizzazione non hanno accesso diretto ad Amazon Redshift.

## Creazione di credenziali IAM temporanee

In questa sezione viene descritto come configurare il sistema per generare credenziali utente temporanee basate su IAM e accedere al database utilizzando le nuove credenziali.

A livello generale, il processo è il seguente:

### 1. [Passaggio 1: creazione di un ruolo IAM per un accesso Single Sign-On IAM](#)

(Facoltativo) Puoi autenticare gli utenti per l'accesso a un database Amazon Redshift integrando l'autenticazione IAM e un provider di identità (IdP) di terza parte.

### 2. [Fase 2: configurazione di asserzioni SAML per l'IdP](#)

(Facoltativo) Per utilizzare l'autenticazione IAM mediante un IdP, devi definire una regola di attestazione nell'applicazione IdP che mappa gli utenti o i gruppi nella tua organizzazione al ruolo IAM. Facoltativamente, è possibile includere elementi di attributo per impostare i parametri `GetClusterCredentials`.

### 3. [Passaggio 3: creare un ruolo IAM con autorizzazioni per la chiamata `GetClusterCredentials`](#)

L'applicazione client SQL assume l'utente quando chiama l'operazione `GetClusterCredentials`. Se hai creato un ruolo IAM per l'accesso al provider di identità, puoi aggiungere l'autorizzazione necessaria a quel ruolo.

### 4. [Fase 4: creazione di un utente di database e di gruppi di database](#)

(Facoltativo) Per impostazione predefinita, `GetClusterCredentials` restituisce le credenziali per creare un nuovo utente se il nome utente non esiste. Puoi anche scegliere di specificare gruppi di utenti a cui gli utenti vengono aggiunti all'accesso. Per impostazione predefinita, gli utenti di database sono aggiunti al gruppo PUBLIC.

### 5. [Fase 5: configurazione di una connessione JDBC o ODBC per utilizzare credenziali IAM](#)

Per connettersi al database Amazon Redshift, è necessario configurare il client SQL per utilizzare i driver JDBC o ODBC di Amazon Redshift.

## Passaggio 1: creazione di un ruolo IAM per un accesso Single Sign-On IAM

Se non utilizzi un provider di identità per l'accesso single-sign on, puoi ignorare questa fase.

Se gestisci già le identità degli utenti all'esterno AWS, puoi autenticare gli utenti per l'accesso a un database Amazon Redshift integrando l'autenticazione IAM e un provider di identità SAML-2.0 (IdP) di terze parti.

Per ulteriori informazioni, consulta [Provider di identità e federazione](#) nella Guida per l'utente di IAM.

Prima di poter utilizzare l'autenticazione IdP di Amazon Redshift, crea un AWS provider di identità SAML. Crea un IdP nella console IAM per fornire AWS informazioni sull'IdP e sulla sua configurazione. In questo modo si instaura un rapporto di fiducia tra il tuo AWS account e l'IdP. Per la procedura relativa alla creazione di un ruolo, consultare [Creazione di un ruolo per una federazione SAML 2.0 \(console\)](#) nella Guida per l'utente di IAM.

Fase 2: configurazione di asserzioni SAML per l'IdP

Dopo la creazione del ruolo IAM, definisci una regola di registrazione nell'applicazione IdP che mappa gli utenti o i gruppi nella tua organizzazione al ruolo IAM. Per ulteriori informazioni, consultare [Configurazione delle asserzioni SAML per la risposta di autenticazione](#) nella Guida per l'utente di IAM.

Se scegli di utilizzare i parametri `GetClusterCredentials` facoltativi `DbUser`, `AutoCreate` e `DbGroups`, puoi impostare i valori per i parametri con la connessione JDBC o ODBC oppure aggiungendo elementi attributo SAML all'IdP. Per ulteriori informazioni sui parametri `DbUser`, `AutoCreate` e `DbGroups`, consultare [Fase 5: configurazione di una connessione JDBC o ODBC per utilizzare credenziali IAM](#).

#### Note

Se si utilizza una variabile di policy IAM `${redshift:DbUser}`, come descritto in [Politiche relative alle risorse per GetClusterCredentials](#), il valore per `DbUser` è sostituito con il valore recuperato dal contesto della richiesta dell'operazione API. I driver Amazon Redshift utilizzano il valore per la variabile `DbUser` fornito dalla connessione URL, piuttosto che il valore fornito come attributo SAML.

Per proteggere questa configurazione, ti consigliamo di utilizzare una condizione in una policy IAM per convalidare il valore `DbUser` con il codice `RoleSessionName`. È possibile trovare esempi di come impostare una condizione utilizzando una policy IAM in [Esempio di politica per l'utilizzo GetClusterCredentials](#).

Per configurare l'IdP allo scopo di impostare i parametri `DbUser`, `AutoCreate` e `DbGroups`, includi i seguenti elementi `Attribute`:

- Un `Attribute` elemento con l'`Name` attributo impostato su `"https://redshift.amazon.com/SAML/Attributes/DbUser"`

Imposta l'elemento `AttributeValue` sul nome di un utente che si conatterà al database Amazon Redshift.

Il valore nell'elemento `AttributeValue` deve essere in minuscolo, iniziare con una lettera, contenere solo caratteri alfanumerici, caratteri di sottolineatura ('\_'), segni più ('+'), punti ('.'), chioccioline ('@') o trattini ('-') e non essere lungo più di 128 caratteri. In genere, il nome utente è un ID utente (ad esempio, `bobsmith`) o un indirizzo e-mail (ad esempio, `bobsmith@example.com`). Il valore non può includere uno spazio (ad esempio, un nome visualizzato di un utente come `Bob Smith`).

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
  <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- Un elemento `Attribute` con l'attributo `Name` impostato su `"https://redshift.amazon.com/SAML/Attributes/AutoCreate"`

Imposta l' `AttributeValue` elemento su `true` per creare un nuovo utente del database, se non ne esiste uno. Imposta su `false` `AttributeValue` per specificare che l'utente del database deve esistere nel database Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
  <AttributeValue>>true</AttributeValue>
</Attribute>
```

- Un `Attribute` elemento con l'`Name` attributo impostato su `"https://redshift.amazon.com/SAML/Attributes/DbGroups"`

Questo elemento contiene uno o più elementi `AttributeValue`. Imposta ogni elemento `AttributeValue` su un nome di gruppo di database a cui si unisce `DbUser` per la durata della sessione quando si connette al database Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
  <AttributeValue>group1</AttributeValue>
```

```
<AttributeValue>group2</AttributeValue>
<AttributeValue>group3</AttributeValue>
</Attribute>
```

### Passaggio 3: creare un ruolo IAM con autorizzazioni per la chiamata `GetClusterCredentials`

Il client SQL ha bisogno dell'autorizzazione per chiamare l'operazione `GetClusterCredentials` per conto dell'utente. Per fornire tale autorizzazione, devi creare un utente o un ruolo e collegare una policy che concede le autorizzazioni necessarie.

Per creare un ruolo IAM con i permessi di chiamata `GetClusterCredentials`

1. Crea un utente o un ruolo mediante il servizio IAM. È anche possibile utilizzare un ruolo o un utente esistente. Ad esempio, se si è creato un ruolo IAM per l'accesso al provider di identità, è possibile collegare le policy IAM necessarie a quel ruolo.
2. Collegare una policy di autorizzazione con l'autorizzazione per chiamare l'operazione `redshift:GetClusterCredentials`. A seconda dei parametri facoltativi specificati, è anche possibile consentire o limitare ulteriori operazioni e risorse nella policy:
  - Per consentire al client SQL di recuperare l'ID, la AWS regione e la porta del cluster, includi l'autorizzazione a chiamare l'operazione `redshift:DescribeClusters` con la risorsa del cluster Redshift.
  - Se si utilizza l'opzione `AutoCreate`, includere l'autorizzazione per chiamare `redshift>CreateClusterUser` con la risorsa `dbuser`. L'Amazon Resource Name (ARN) seguente specifica il `dbuser` di Amazon Redshift. Sostituisci *regione* *cluster-name* con i valori per la tua AWS regione, account e cluster. *account-id* Per *dbuser-name*, specificare il nome utente da utilizzare per accedere al database del cluster.

```
arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
```

- (Facoltativo) Aggiungere un ARN che specifica la risorsa `dbname` di Amazon Redshift nel formato riportato di seguito. Sostituisci *regione* *cluster-name* con i valori per la tua AWS regione, account e cluster. *account-id* Per *database-name*, specificare il nome di una database a cui l'utente accederà.

```
arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
```

- Se utilizzi l'opzione DbGroups, includi l'autorizzazione per chiamare l'operazione `redshift:JoinGroup` con la risorsa `dbgroup` di Amazon Redshift nel formato seguente. Sostituisci *regione* *cluster-name* con i valori per la tua AWS regione, account e cluster. *account-id* Per *dbgroup-name*, specificare il nome di un gruppo di utenti a cui l'utente viene aggiunto all'accesso.

```
arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
```

Per maggiori informazioni ed esempi, consulta [Politiche relative alle risorse per GetClusterCredentials](#).

L'esempio seguente mostra una policy che consente a un ruolo IAM di chiamare l'operazione `GetClusterCredentials`. Specificando la risorsa `dbuser` di Amazon Redshift, si concede l'accesso al ruolo al nome utente di database `temp_creds_user` sul cluster denominato `examplecluster`.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/
temp_creds_user"
  }
}
```

Puoi utilizzare un carattere jolly (\*) per sostituire in parte o interamente il nome di cluster, il nome utente o i nomi di gruppi di database. L'esempio seguente autorizza qualsiasi nome utente che inizia con `temp_` e con qualsiasi cluster nell'account specificato.

#### Important

L'istruzione nell'esempio seguente specifica un carattere jolly (\*) come valore della risorsa in modo che la policy autorizzi qualsiasi risorsa che inizia con i caratteri specificati. L'utilizzo di un carattere jolly nelle policy IAM può risultare eccessivamente permissivo. Come best practice, si consiglia di utilizzare la policy più restrittiva accettabile per l'applicazione aziendale.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

Nell'esempio seguente viene mostrata una policy che consente al ruolo IAM di chiamare l'operazione `GetClusterCredentials` con l'opzione di creare automaticamente un nuovo utente e di specificare gruppi a cui l'utente viene aggiunto all'accesso. La clausola `"Resource": "*"`  concede l'accesso al ruolo a qualsiasi risorsa, inclusi cluster, utenti di database o gruppi di utenti.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "redshift:GetClusterCredentials",
      "redshift:CreateClusterUser",
      "redshift:JoinGroup"
    ],
    "Resource": "*"
  }
}
```

Per ulteriori informazioni, consultare la pagina [sintassi dell'ARN Amazon Redshift](#).

#### Fase 4: creazione di un utente di database e di gruppi di database

Se lo desideri, puoi creare un utente di database che utilizzi per accedere al database del cluster. Se crei credenziali utente temporanee per un utente esistente, puoi disabilitare la password dell'utente per forzare l'utente ad accedere con la password temporanea. In alternativa, puoi utilizzare l'opzione `Autocreate` di `GetClusterCredentials` per creare automaticamente un nuovo utente di database.

Puoi creare gruppi di utenti di database con le autorizzazioni desiderate a cui un utente di database IAM viene aggiunto all'accesso. Quando chiami l'operazione `GetClusterCredentials`, puoi specificare un elenco di nomi di gruppo utenti a cui il nuovo utente viene aggiunto all'accesso. Queste appartenenze a gruppi sono valide unicamente per le sessioni create utilizzando le credenziali generate con la richiesta specificata.

## Per creare un utente di database e gruppi di database

1. Accedi al database Amazon Redshift e crea un utente di database utilizzando [CREATE USER](#) oppure modificare un utente esistente utilizzando [ALTER USER](#).
2. Specificare eventualmente l'opzione PASSWORD DISABLE per impedire all'utente di utilizzare una password. Quando la password di un utente è disabilitata, l'utente può accedere soltanto utilizzando le credenziali temporanee. Se la password non è disabilitata, l'utente può accedere con la password o utilizzando le credenziali temporanee. Non è possibile disabilitare la password di un utente con privilegi avanzati.

Gli utenti necessitano dell'accesso programmatico se desiderano interagire con l' AWS Management Console esterno di. Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente.AWS Command Line Interface</a></li> <li>• Per AWS SDK, strumenti e AWS API, consulta <a href="#">l'autenticazione IAM Identity Center</a> nella Guida di riferimento agli AWS SDK e agli strumenti.</li> </ul>
IAM	Utilizza credenziali temporanee per firmare le richieste programmatiche	Segui le istruzioni in <a href="#">Uso delle credenziali temporanee</a>

Quale utente necessita dell'accesso programmatico?	Per	Come
	agli SDK o alle API AWS CLI. AWS AWS	<a href="#">con AWS risorse</a> nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Autenticazione tramite credenziali utente IAM nella Guida per l'utente</a>.AWS Command Line Interface</li> <li>• Per gli AWS SDK e gli strumenti, consulta <a href="#">Autenticazione tramite credenziali a lungo termine</a> nella Guida di riferimento agli SDK e agli AWS strumenti.</li> <li>• Per le AWS API, consulta <a href="#">Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM</a>.</li> </ul>

L'esempio seguente crea un utente con password disabilitata.

```
create user temp_creds_user password disable;
```

L'esempio seguente disabilita la password per un utente esistente.

```
alter user temp_creds_user password disable;
```

### 3. Creare gruppi di utenti di database mediante [CREATE GROUP](#).

4. Utilizzare il comando [GRANT](#) per definire i privilegi di accesso per i gruppi.

Fase 5: configurazione di una connessione JDBC o ODBC per utilizzare credenziali IAM

Puoi configurare il client SQL con un driver JDBC o ODBC di Amazon Redshift. Questo driver gestisce il processo per creare le credenziali utente del database e per stabilire una connessione tra il client SQL e il database Amazon Redshift.

Se utilizzi un provider di identità per l'autenticazione, specifica il nome di un plug-in di provider di identità. I driver JDBC e ODBC di Amazon Redshift includono plug-in per i seguenti provider di identità basati su SAML:

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

Per la procedura per configurare Microsoft Azure AD come provider di identità, consultare [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

Per configurare una connessione JDBC per utilizzare credenziali IAM

1. Scarica il driver JDBC di Amazon Redshift più recente dalla pagina [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).
2. Creare un URL JDBC con le opzioni delle credenziali IAM in uno dei formati seguenti. Per utilizzare l'autenticazione IAM, aggiungi `iam:` all'URL JDBC di Amazon Redshift dopo `jdbc:redshift:` come mostrato nell'esempio seguente.

```
jdbc:redshift:iam://
```

Aggiungi `cluster-name`, `region` e `account-id`. Il driver JDBC utilizza le informazioni dell'account IAM e il nome del cluster per recuperare l'ID e la regione del cluster. AWS A tale scopo, l'utente o il ruolo deve disporre dell'autorizzazione per chiamare l'operazione `redshift:DescribeClusters` con il cluster specificato. Se l'utente o il ruolo non dispone dell'autorizzazione per chiamare l'operazione `redshift:DescribeClusters`, includi l'ID del cluster, la AWS regione e la porta come mostrato nell'esempio seguente. Il numero di porta è facoltativo.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-
west-2.redshift.amazonaws.com:5439/dev
```

3. Aggiungere le opzioni JDBC per fornire le credenziali IAM. Si utilizzano differenti combinazioni delle opzioni JDBC per fornire le credenziali IAM. Per informazioni dettagliate, vedi [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

L'URL seguente specifica l' AccessKeyID e SecretAccessKey per un utente.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY
```

L'esempio seguente specifica un profilo con nome che contiene le credenziali IAM.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
```

4. Aggiungere le opzioni JDBC utilizzate dal driver JDBC per chiamare l'operazione API `GetClusterCredentials`. Non includere queste opzioni se si chiama l'operazione API `GetClusterCredentials` a livello di codice.

L'esempio seguente include le opzioni `GetClusterCredentials` JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?
plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_t
```

Per configurare una connessione ODBC per utilizzare credenziali IAM

Nella procedura seguente, è possibile trovare i passaggi solo per configurare l'autenticazione IAM. Per le fasi relative all'utilizzo dell'autenticazione standard con un nome utente di database e una password, consultare [Configurazione di una connessione ODBC](#).

1. Installa e configura il driver ODBC di Amazon Redshift più recente per il sistema operativo in uso. Per ulteriori informazioni, consultare la pagina [Configurazione di una connessione ODBC](#).

#### Important

La versione del driver ODBC di Amazon Redshift deve essere 1.3.6.1000 o successiva.

2. Seguire la procedura per il sistema operativo in uso per configurare le impostazioni di connessione.

Per ulteriori informazioni, consultare uno dei seguenti argomenti:

- [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#)
- [Utilizzo di una gestione del driver ODBC per configurare il driver su sistemi operativi Linux e macOS X](#)

3. Nei sistemi operativi Microsoft Windows, accedi alla finestra Configurazione DSN driver ODBC di Amazon Redshift.

- a. In Connection Settings (Impostazioni di connessione), inserire le informazioni riportate di seguito:

- Data Source Name (Nome origine dati)
- Server (facoltativo)
- Port (Porta) (facoltativo)
- Database

Se l'utente o il ruolo dispone dell'autorizzazione per chiamare l'operazione `redshift:DescribeClusters`, sono necessari solo Nome origine dati e Database. Amazon Redshift utilizza ClusterId and Region per ottenere il server e la porta chiamando l'DescribeClusteroperazione.

Se l'utente o il ruolo non dispone dell'autorizzazione per chiamare l'operazione `redshift:DescribeClusters`, specifica Server e Porta.

- b. In Authentication (Autenticazione), scegliere un valore per Auth Type (Tipo di autenticazione).

Per ogni tipo di autenticazione, immettere i valori come indicato di seguito:

#### Profilo AWS

Immetti le seguenti informazioni:

- ClusterID
- Region
- Profile name (Nome profilo)

Inserisci il nome di un profilo in un file di AWS configurazione che contiene i valori per le opzioni di connessione ODBC. Per ulteriori informazioni, consulta [Utilizzo di un profilo di configurazione](#).

(Facoltativo) Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API `GetClusterCredentials`:

- DbUser
- Utente AutoCreate
- DbGroups

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

## Credenziali IAM

Immetti le seguenti informazioni:

- ClusterID
- Region
- AccessKeyId e SecretAccessKey

L'ID chiave di accesso e la chiave di accesso segreta per l'utente o il ruolo IAM configurato per l'autenticazione database IAM.

- SessionToken

SessionToken è richiesto per un ruolo IAM con credenziali temporanee. Per ulteriori informazioni, consultare [Credenziali di sicurezza temporanee](#).

Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API `GetClusterCredentials`:

- DbUser(obbligatorio)
- Utente AutoCreate (opzionale)
- DbGroups(opzionale)

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

## Identity Provider: AD FS

Per l'autenticazione integrata di Windows con AD FS, lasciare i campi User (Utente) e Password vuoti.

Specificare i dettagli dell'IdP:

- IdP Host (Host IdP)

Il nome dell'host del provider di identità dell'azienda. Questo nome non deve includere barre rovesciate ( / ).

- IdP Port (Porta IdP) (facoltativo)

La porta utilizzata dal provider di identità. Il valore predefinito è 443.

- Preferred Role (Ruolo preferito)

Un Amazon Resource Name (ARN) di un ruolo IAM negli elementi AttributeValue con più valori per l'attributo Role nell'asserzione SAML. Per trovare il valore appropriato per il ruolo preferito, collaborare con l'amministratore IdP. Per ulteriori informazioni, consulta [Configurazione di asserzioni SAML per l'IdP](#).

(Facoltativo) Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API GetClusterCredentials:

- DbUser
- Utente AutoCreate
- DbGroups

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

## Provider di identità: PingFederate

In User (Utente) e Password, immettere il nome utente e la password dell'IdP.

Specificare i dettagli dell'IdP:

- IdP Host (Host IdP)

Il nome dell'host del provider di identità dell'azienda. Questo nome non deve includere barre rovesciate ( / ).

- IdP Port (Porta IdP) (facoltativo)

La porta utilizzata dal provider di identità. Il valore predefinito è 443.

- Preferred Role (Ruolo preferito)

Un Amazon Resource Name (ARN) di un ruolo IAM negli elementi `AttributeValue` con più valori per l'attributo `Role` nell'asserzione SAML. Per trovare il valore appropriato per il ruolo preferito, collaborare con l'amministratore IdP. Per ulteriori informazioni, consulta [Configurazione di asserzioni SAML per l'IdP](#).

(Facoltativo) Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API `GetClusterCredentials`:

- DbUser
- Utente AutoCreate
- DbGroups

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

Identity Provider: Okta

In `User` (Utente) e `Password`, immettere il nome utente e la password dell'IdP.

Specificare i dettagli dell'IdP:

- IdP Host (Host IdP)

Il nome dell'host del provider di identità dell'azienda. Questo nome non deve includere barre rovesciate ( / ).

- IdP Port (Porta IdP)

Questo valore non viene utilizzato da Okta.

- Preferred Role (Ruolo preferito)

Un Amazon Resource Name (ARN) di un ruolo IAM negli elementi `AttributeValue` per l'attributo `Role` nell'asserzione SAML. Per trovare il valore appropriato per il ruolo

preferito, collaborare con l'amministratore IdP. Per ulteriori informazioni, consulta [Configurazione di asserzioni SAML per l'IdP](#).

- Okta App ID (ID app Okta)

Un ID per l'applicazione Okta. Il valore dell'ID dell'app segue "amazon\_aws" nel collegamento incorporato dell'applicazione Okta. Collaborare con l'amministratore IdP per ottenere questo valore.

(Facoltativo) Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API `GetClusterCredentials`:

- DbUser
- Utente AutoCreate
- DbGroups

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

#### Provider di identità: Azure AD

In User (Utente) e Password, immettere il nome utente e la password dell'IdP.

Per ID cluster e Regione, immettere l'ID cluster e la regione AWS del cluster Amazon Redshift.

Per Database, specifica il database creato per il cluster Amazon Redshift.

Specificare i dettagli dell'IdP:

- IdP Tenant (Tenant IdP)

Il tenant usato per Azure AD.

- Azure Client Secret (Segreto client Azure)

Il segreto client dell'app aziendale Amazon Redshift in Azure.

- Azure Client ID (ID client di Azure)

L'ID client (ID applicazione) dell'app aziendale Amazon Redshift in Azure.

(Facoltativo) Fornire dettagli per le opzioni utilizzate dal driver ODBC per chiamare l'operazione API `GetClusterCredentials`:

- DbUser
- Utente AutoCreate
- DbGroups

Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

## Opzioni per fornire credenziali IAM

Per fornire credenziali IAM per una connessione ODBC o JDBC, scegli una delle opzioni seguenti.

- AWS profile

Anziché fornire i valori delle credenziali come impostazioni JDBC o ODBC, puoi includere i valori in un profilo con nome. Per ulteriori informazioni, consulta [Utilizzo di un profilo di configurazione](#).

- Credenziali IAM

Fornisci valori per `AccessKey ID` e `SecretAccessKey`, facoltativamente, `SessionToken` sotto forma di impostazioni JDBC o ODBC. `SessionToken` è richiesto solo per un ruolo IAM con credenziali temporanee. Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per fornire credenziali IAM](#).

- Federazione del provider di identità

Se utilizzi la federazione del provider di identità per consentire agli utenti di un provider di identità di eseguire l'autenticazione in Amazon Redshift, specifica il nome di un plug-in del provider di credenziali. Per ulteriori informazioni, consulta [Utilizzo di un plug-in di provider di credenziali](#).

I driver JDBC e ODBC di Amazon Redshift includono plug-in per i seguenti provider di credenziali di federazione delle identità basate su SAML:

- Microsoft Active Identity Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (AD)

Puoi fornire il nome di plug-in e i valori correlati come impostazioni JDBC o ODBC oppure utilizzando un profilo. Per ulteriori informazioni, consultare [Opzioni per la configurazione del driver JDBC versione 2.1](#) e [Configurazione delle opzioni del driver ODBC](#).

Per ulteriori informazioni, consulta [Configurazione di una connessione JDBC o ODBC per utilizzare credenziali IAM](#).

### Utilizzo di un profilo di configurazione

Puoi fornire le opzioni e `GetClusterCredentials` le opzioni delle credenziali IAM come impostazioni nei profili denominati nel tuo AWS file di configurazione. Per specificare il nome di profilo, utilizzare l'opzione `Profile JDBC`. La configurazione è archiviata in un file denominato `config` o `credentials` in una cartella `.aws` della tua home directory.

Per un plug-in di provider di credenziali basate su SAML incluso con un driver JDBC o ODBC di Amazon Redshift, puoi utilizzare le impostazioni descritte in precedenza in [Utilizzo di un plug-in di provider di credenziali](#). Se `plugin_name` non viene utilizzato, le altre opzioni vengono ignorate.

L'esempio seguente mostra il file `~/.aws/credentials` con due profili:

```
[default]
aws_access_key_id=AKIAIOSFODNN7EXAMPLE
aws_secret_access_key=wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY

[user2]
aws_access_key_id=AKIAI44QH8DHBEXAMPLE
aws_secret_access_key=je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY
session_token=AQoDYXdzEPT//////////
wEXAMPLEtc764bNrC9SAPBSM22wD0k4x4HIZ8j4FZTwdQWLwsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTf1fKD8YUuwthAx7
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPkyQDYwT7WZ0wq5V5XDvp75YU
9HFv1Rd8Tx6q6fE8YQcHNvXakiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fP0Ln9FX9KSYvKTr4rvx3iSI1TJabIQwj2ICCR/oLxBA==
```

Per utilizzare le credenziali per l'esempio `user2`, specifica `Profile=user2` nell'URL JDBC.

Per ulteriori informazioni sull'utilizzo dei profili, consulta [Configurazione e impostazioni dei file di credenziali nella Guida](#) per l' AWS Command Line Interface utente.

Per ulteriori informazioni sull'utilizzo dei profili per il driver JDBC, consulta [Specifica di profili](#).

Per ulteriori informazioni sull'utilizzo dei profili per il driver ODBC, consulta [Configurazione dell'autenticazione](#).

Opzioni JDBC e ODBC per fornire credenziali IAM

La tabella seguente elenca le opzioni JDBC e ODBC per fornire credenziali IAM.

Opzione	Descrizione
Iam	Da utilizzare solo in una stringa di connessione ODBC. Imposta questa opzione su 1 per utilizzare l'autenticazione IAM.
AccessKey ID	L'ID della chiave di accesso e la chiave di accesso segreta per il ruolo o l'utente IAM configurati per l'autenticazione del database IAM. SessionToken è richiesto solo per un ruolo IAM con credenziali temporanee. SessionToken non viene utilizzato per un utente. Per ulteriori informazioni, consultare <a href="#">Credenziali di sicurezza temporanee</a> .
SecretAcc essKey	
SessionTo ken	
plugin_na me	Il nome completo di una classe che implementa un provider di credenziali. Il driver JDBC di Amazon Redshift include plug-in per provider di credenziali basati su SAML. Se fornisci plugin_name , puoi anche fornire altre opzioni correlate. Per ulteriori informazioni, consulta <a href="#">Utilizzo di un plug-in di provider di credenziali</a> .
Profile	Il nome di un profilo in un file di AWS credenziali o di configurazione che contiene i valori per le opzioni di connessione JDBC. Per ulteriori informazioni, consulta <a href="#">Utilizzo di un profilo di configurazione</a> .

Utilizzo di un plug-in di provider di credenziali

Amazon Redshift utilizza plug-in di provider di credenziali per l'autenticazione Single Sign-On.

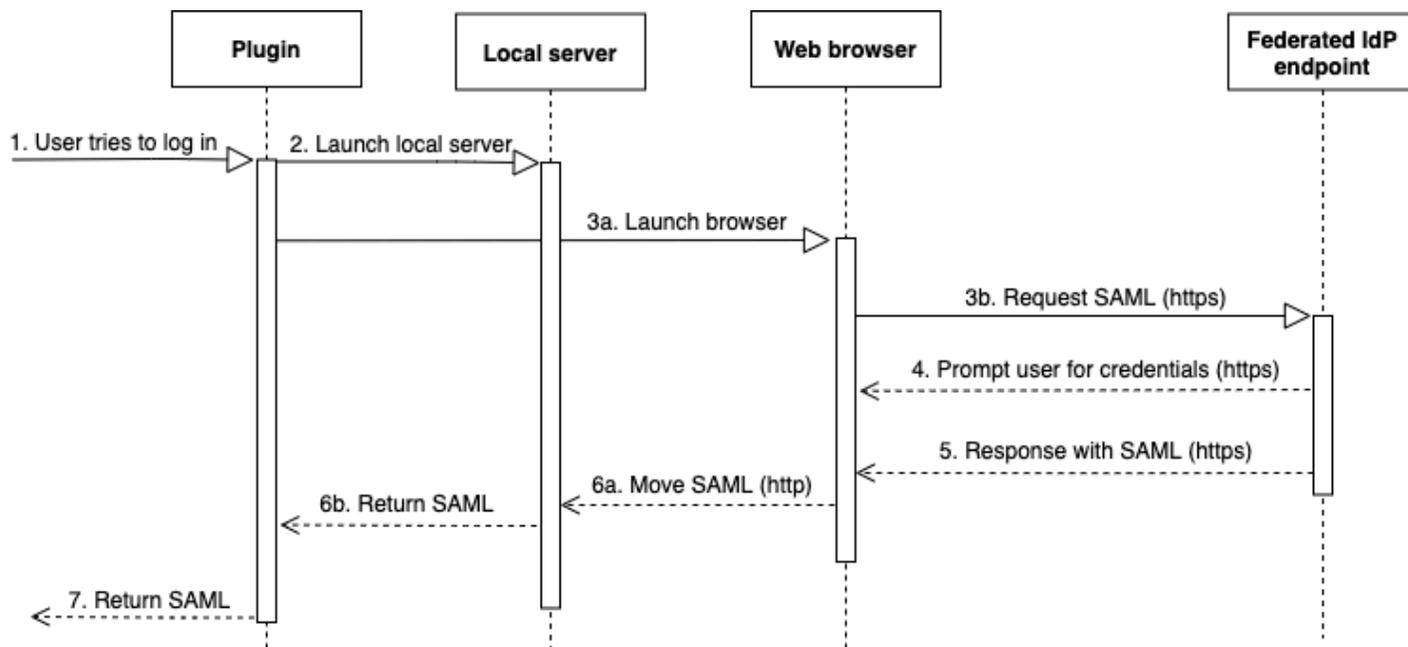
Per supportare l'autenticazione Single Sign-On, Amazon Redshift fornisce il plug-in Azure AD per Microsoft Azure Active Directory. Per informazioni su come configurare questo plugin, consultare [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

## Impostazione dell'autenticazione a più fattori

### Impostazione dell'autenticazione a più fattori

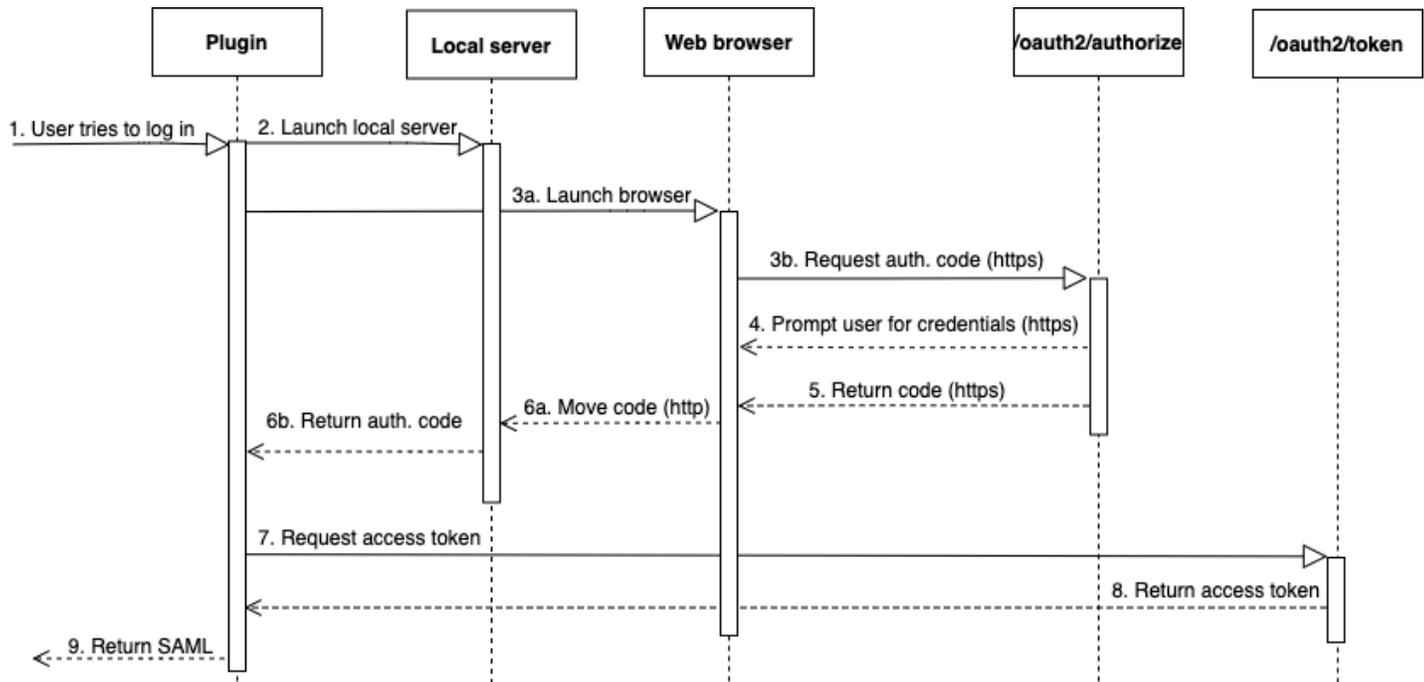
Per supportare autenticazione a più fattori (MFA), Amazon Redshift fornisce plug-in basati su browser. Usa il plug-in SAML del browser per Okta e il plug-in Azure AD del browser per Microsoft Azure Active Directory. PingOne

Con il plugin SAML del browser, il flusso dell'autenticazione SAML è il seguente:



1. Un utente tenta di eseguire l'accesso.
2. Il plugin avvia un server locale per ascoltare le connessioni in entrata sul localhost.
3. Il plug-in avvia un browser Web per richiedere una risposta SAML su HTTPS dall'endpoint del provider di identità federate dell'URL di accesso Single Sign-On specificato.
4. Il browser Web segue il collegamento e invia all'utente una richiesta di immissione delle credenziali.
5. Dopo che l'utente esegue l'autenticazione e concede l'autorizzazione, l'endpoint del provider di identità federate restituisce una risposta SAML su HTTPS all'URI indicato da `redirect_uri`.
6. Il browser Web sposta il messaggio di risposta con la risposta SAML nel `redirect_uri` indicato.
7. Il server locale accetta la connessione in entrata, il plugin recupera la risposta SAML e la invia ad Amazon Redshift .

Con il plug-in Azure AD del browser, il flusso di autenticazione SAML è il seguente:



1. Un utente tenta di eseguire l'accesso.
2. Il plugin avvia un server locale per ascoltare le connessioni in entrata sul localhost.
3. Il plug-in avvia un browser Web per richiedere un codice di autorizzazione dall'endpoint `oauth2/authorize` di Azure AD.
4. Il browser Web segue il collegamento generato su HTTPS e richiede all'utente di immettere le credenziali. Il collegamento viene generato utilizzando le proprietà di configurazione, ad esempio `tenant` e `client_id`.
5. Dopo che l'utente esegue l'autenticazione e concede l'autorizzazione, l'endpoint `oauth2/authorize` di Azure AD restituisce e invia una risposta tramite HTTPS con il codice di autorizzazione a `redirect_uri` indicato.
6. Il browser Web sposta il messaggio di risposta con la risposta SAML nel `redirect_uri` indicato.
7. Il server locale accetta la connessione in ingresso e il plug-in richiede e recupera il codice di autorizzazione e invia una richiesta POST all'endpoint `oauth2/token` di Azure AD.
8. L'endpoint `oauth2/token` di Azure AD restituisce una risposta con un token di accesso al `redirect_uri` indicato.
9. Il plug-in recupera la risposta SAML e la invia ad Amazon Redshift.

Vedere le seguenti sezioni:

- Active Directory Federation Services (AD FS)

Per ulteriori informazioni, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con AD FS](#).

- PingOne (Ping)

Il ping è supportato solo con l'adattatore PingOne IdP predeterminato che utilizza l'autenticazione Forms.

Per ulteriori informazioni, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Ping Identity](#).

- Okta

Okta è supportato solo per l'applicazione fornita da Okta utilizzata con la AWS Management Console.

Per ulteriori informazioni, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Okta](#).

- Microsoft Azure Active Directory

Per ulteriori informazioni, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

Configurazione delle opzioni dei plugin

Configurazione delle opzioni dei plugin

Per usare un plugin per il provider di credenziali basato su SAML, specificare le seguenti opzioni usando le opzioni JDBC o ODBC o in un profilo con nome. Se `plugin_name` non è specificato, le altre opzioni vengono ignorate.

Opzione	Descrizione
<code>plugin_name</code>	<p>Per JDBC, il nome di classe che implementa un provider di credenziali. Specifica una delle seguenti proprietà:</p> <ul style="list-style-type: none"> <li>• Per Active Directory Federation Services</li> </ul> <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin-top: 10px;"> <code>com.amazon.redshift.plugin.AdfsCredentialsProvider</code> </div>

Opzione	Descrizione
	<ul style="list-style-type: none"> <li>• Per Okta           <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.OktaCredentialsProvider</code> </div> </li> <li>• Per PingFederate           <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.PingCredentialsProvider</code> </div> </li> <li>• Per Microsoft Azure Active Directory           <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.AzureCredentialsProvider</code> </div> </li> <li>• Per SAML MFA           <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.BrowserSamlCredentialsProvider</code> </div> </li> <li>• Per l'accesso Single Sign-On in Microsoft Azure Active Directory con autenticazione a più fattori (MFA)           <div style="border: 1px solid #ccc; border-radius: 10px; padding: 5px; margin: 5px 0;"> <code>com.amazon.redshift.plugin.BrowserAzureCredentialsProvider</code> </div> </li> </ul> <p>Per ODBC, specifica uno dei seguenti valori:</p> <ul style="list-style-type: none"> <li>• Per Active Directory Federation Services: <code>adfs</code></li> <li>• Per Okta: <code>okta</code></li> <li>• Per PingFederate: <code>ping</code></li> <li>• Per Microsoft Azure Active Directory: <code>azure</code></li> <li>• Per SAML MFA: <code>browser saml</code></li> <li>• Per l'accesso Single Sign-On in Microsoft Azure Active Directory con autenticazione a più fattori (MFA): <code>browser azure ad</code></li> </ul>
<code>idp_host</code>	Il nome dell'host del provider di identità dell'azienda. Questo nome non deve includere barre rovesciate ( / ). Per un provider di identità Okta, il valore per <code>idp_host</code> deve terminare con <code>.okta.com</code> .

Opzione	Descrizione
<code>idp_port</code>	La porta utilizzata dal provider di identità. Il valore predefinito è 443. Questa porta viene ignorata per Okta.
<code>preferred_role</code>	L'Amazon Resource Name (ARN) di un ruolo dagli elementi <code>AttributeValue</code> per l'attributo <code>Role</code> nell'asserzione SAML. Per trovare il valore appropriato per il ruolo preferito, collaborare con l'amministratore IdP. Per ulteriori informazioni, consulta <a href="#">Configurazione di asserzioni SAML per l'IdP</a> .
<code>user</code>	Un nome utente aziendale, incluso il dominio quando applicabile. Ad esempio, per Active Directory, il nome di dominio è obbligatorio nel formato dominio\nome utente.
<code>password</code>	La password dell'utente aziendale. È consigliabile non utilizzare questa opzione. Utilizza piuttosto il client SQL per fornire la password.
<code>app_id</code>	Un ID per l'applicazione Okta. Utilizzata solo con Okta. Il valore di <code>app_id</code> segue <code>amazon_aws</code> nel collegamento di incorporamento dell'applicazione Okta. Per ottenere questo valore, collaborare con l'amministratore IdP. Di seguito è riportato un esempio di collegamento di incorporamento di un'applicazione: <code>https://example.okta.com/home/amazon_aws/0oa2hy1wrpM8UGehd1t7/272</code>
<code>idp_tenant</code>	Un tenant usato per Azure AD. Utilizzato solo con Azure.
<code>client_id</code>	Un ID client per l'applicazione aziendale Amazon Redshift in Azure AD. Utilizzato solo con Azure.

## Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD

È possibile utilizzare Microsoft Azure AD come provider di identità (IdP) per accedere al cluster Amazon Redshift. Di seguito, è possibile trovare una procedura che descrive come impostare una relazione di trust per questo scopo. Per ulteriori informazioni sulla configurazione AWS come fornitore di servizi per l'IdP, [consulta \*Configuring Your SAML 2.0 IdP with Relying Party Trust e Adding Claims nella IAM User Guide\*](#).

**Note**

Per usare Azure AD con JDBC, il driver JDBC di Amazon Redshift deve essere la versione 1.2.37.1061 o successiva. Per usare Azure AD con ODBC, il driver ODBC di Amazon Redshift deve essere la versione 1.4.10.1000 o successiva.

Guarda il video seguente per scoprire come federare l'accesso Amazon Redshift al single sign-on di Microsoft Azure AD: [Federazione dell'accesso Amazon Redshift con il single sign-on di Microsoft Azure AD](#).

Per configurare Azure AD e il tuo account in modo che si fidino l'uno dell'altro AWS

1. Crea o utilizza un cluster Amazon Redshift esistente a cui possono connettersi gli utenti di Azure AD. Per configurare la connessione, sono necessarie alcune proprietà di questo cluster, ad esempio l'identificatore del cluster. Per ulteriori informazioni, consulta [Creazione di un cluster](#).
2. Configura un Azure Active Directory, i gruppi e gli utenti utilizzati AWS sul portale Microsoft Azure.
3. Aggiungi Amazon Redshift come applicazione aziendale sul portale Microsoft Azure da utilizzare per il single sign-on alla AWS console e l'accesso federato ad Amazon Redshift. Scegliere Enterprise application (Applicazione aziendale).
4. Scegliere +New application (+Nuova applicazione). Viene visualizzata la pagina di aggiunta di un'applicazione.
5. Cercare **AWS** nel campo di ricerca.
6. Seleziona Amazon Web Services (AWS) quindi scegli Aggiungi. Questo crea l'applicazione. AWS
7. In Manage (Gestisci), scegliere Single Sign-On.
8. Scegli SAML. Viene visualizzata la pagina Amazon Web Services (AWS) | Accesso basato su SAML.
9. Scegliere Yes (Sì) per passare alla pagina di configurazione Single Sign-On con SAML. In questa pagina è riportato l'elenco degli attributi preconfigurati correlati alla funzionalità Single Sign-On.
10. Per Basic SAML Configuration (Configurazione SAML di base), scegliere l'icona di modifica e selezionare Save (Salva).

11. Quando si configurano più applicazioni, fornire un valore di identificatore. Ad esempio, specifica ***https://signin.aws.amazon.com/saml#2***. Dalla seconda applicazione in poi utilizzare questo formato con un segno # per specificare un valore SPN univoco.
12. Nella sezione User Attributes and Claims (Attributi utente e registrazioni), scegliere l'icona di modifica.

Per impostazione predefinita, l'identificatore utente unico (UID), il ruolo e le SessionDuration attestazioni sono preconfigurati. RoleSessionName

13. Scegliere + Add new claim (+ Aggiungi nuova registrazione) per aggiungere una registrazione per gli utenti del database.

Per Nome, immetti **DbUser**.

Per Namespace (Spazio dei nomi), immettere **https://redshift.amazon.com/SAML/Attributes**.

In Source (Origine), scegliere Attribute (Attributo).

In Source attribute (Attributo di origine), scegliere user.userprincipalname. Quindi, scegliere Save (Salva).

14. Scegli + Aggiungi nuovo reclamo per cui aggiungere un reclamo. AutoCreate

Per Nome, immetti **AutoCreate**.

Per Namespace (Spazio dei nomi), immettere **https://redshift.amazon.com/SAML/Attributes**.

In Source (Origine), scegliere Attribute (Attributo).

Per Source attribute (Attributo di origine), scegliere "true". Quindi, scegliere Save (Salva).

Qui, **123456789012** è l'account AWS , **AzureSSO** è un ruolo IAM creato e **AzureADProvider** è il provider IAM.

Nome di registrazione	Valore
Identificatore utente univoco (ID nome)	user.userprincipalname

Nome di registrazione	Valore
https://aws.amazon.com/SAML/Attributes/SessionDuration	900
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: <i>123456789012</i> :role/ <i>AzureSSO</i> ,arn:aws:iam:: <i>123456789012</i> :saml-provider/ <i>AzureADProvider</i>
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.userprincipalname
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbGroups	user.assignedroles
https://redshift.amazon.com/SAML/Attributes/DbUser	user.userprincipalname

15. In App Registration (Registrazione app) > ***your-application-name*** > Authentication (Autenticazione), aggiungere Mobile And Desktop Application (Applicazione mobile e desktop). Specificare l'URL come http://localhost/redshift/.
16. Nella sezione SAML Signing Certificate (Certificato di firma SAML), scegliere Download (Scarica) per scaricare e salvare il file XML dei metadati della federazione da utilizzare durante la creazione di un provider di identità SAML IAM. Questo file viene utilizzato per creare l'identità Single Sign-On federata.
17. Creare un provider di identità SAML IAM nella console IAM. Il documento dei metadati fornito è il file XML dei metadati della federazione salvato quando si configura l'applicazione Azure Enterprise. Per la procedura dettagliata, consultare [Creazione e gestione di un provider di identità IAM \(console\)](#) nella Guida per l'utente di IAM.
18. Creare un ruolo IAM per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di un ruolo per SAML](#) nella Guida per l'utente di IAM.
19. Creare una policy IAM che è possibile collegare al ruolo IAM creato per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Modificare le policy seguenti (in formato JSON) per l'ambiente:

- Sostituisci la AWS regione del tuo cluster con. *us-west-1*
- Sostituisci il tuo AWS account con. *123456789012*
- Sostituire l'identificatore del cluster (o \* per tutti i cluster) per *cluster-identifier*.
- Sostituire il database (o \* per tutti i database) per *dev*.
- Sostituire l'identificatore univoco del ruolo IAM per *AROAJ2UCCR6DPCEXAMPLE*.
- Sostituire il dominio dell'e-mail del tenant o della società per *example.com*.
- Sostituire il gruppo di database a cui si intende assegnare l'utente per *my\_dbgroup*.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:us-west-1:123456789012:dbname:cluster-identifier/dev",
        "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/${redshift:DbUser}",
        "arn:aws:redshift:us-west-1:123456789012:cluster:cluster-identifier"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AROAJ2UCCR6DPCEXAMPLE:${redshift:DbUser}@example.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "redshift:CreateClusterUser",
      "Resource": "arn:aws:redshift:us-west-1:123456789012:dbuser:cluster-identifier/${redshift:DbUser}"
    },
    {
      "Effect": "Allow",
```

```

        "Action": "redshift:JoinGroup",
        "Resource": "arn:aws:redshift:us-west-1:123456789012:dbgroup:cluster-
cluster-identifier/my_dbgroup"
    },
    {
        "Effect": "Allow",
        "Action": [
            "redshift:DescribeClusters",
            "iam:ListRoles"
        ],
        "Resource": "*"
    }
]
}

```

Questa policy concede le autorizzazioni come segue:

- La prima sezione concede l'autorizzazione all'operazione API `GetClusterCredentials` per ottenere credenziali temporanee per il cluster specificato. In questo esempio, la risorsa è `cluster-identifier` con database `dev`, nell'account `123456789012` e nella regione AWS `us-west-1`. La clausola `${redshift:DbUser}` consente di connettersi solo agli utenti che corrispondono al valore `DbUser` specificato in Azure AD.
- La clausola di condizione definisce che solo alcuni utenti ottengono le credenziali temporanee. Sono utenti con il ruolo specificato dall'ID univoco del ruolo `AROAJ2UCCR6DPCEXAMPLE` nell'account IAM identificato da un indirizzo e-mail nel dominio e-mail della società. Per ulteriori informazioni sugli ID univoci, consultare [ID univoci](#) nella Guida per l'utente di IAM.

L'installazione con l'IDP (in questo caso Azure AD) determina la modalità di scrittura della clausola di condizione. Se l'e-mail del dipendente è `johndoe@example.com`, `${redshift:DbUser}` impostare innanzitutto il campo `super` che corrisponde al nome utente del dipendente `johndoe`. Per il funzionamento di questa condizione, imposta il campo `RoleSessionName` di AWS SAML sul campo `super` che corrisponde all'e-mail del dipendente `johndoe@example.com`. Quando si adotta questo approccio, considerare quanto segue:

- Se si imposta `${redshift:DbUser}` in modo che sia l'e-mail del dipendente, rimuovere il JSON `@example.com` di esempio per associare il `RoleSessionName`.
- Se si imposta `RoleSessionId` in modo che sia solo il nome utente del dipendente, rimuovere `@example.com` nell'esempio per associare il `RoleSessionName`.

- Nell'esempio JSON, `${redshift:DbUser}` e `RoleSessionName` sono entrambi impostati sull'e-mail del dipendente. In questo esempio JSON utilizza il nome utente del database Amazon Redshift con `@example.com` per consentire all'utente di accedere al cluster.
- La seconda sezione concede l'autorizzazione per creare un nome `dbuser` nel cluster specificato. In questo esempio, JSON limita la creazione a `${redshift:DbUser}`.
- La terza sezione concede l'autorizzazione per specificare il `dbgroup` al quale un utente può partecipare. In questo esempio JSON, un utente può unirsi al gruppo `my_dbgroup` nel cluster specificato.
- La quarta sezione concede l'autorizzazione alle operazioni che l'utente può eseguire su tutte le risorse. In questo esempio JSON, consente agli utenti di effettuare chiamate per `redshift:DescribeClusters` ottenere informazioni sul cluster come l'endpoint, la AWS regione e la porta del cluster. Consente inoltre agli utenti di chiamare `iam:ListRoles` per verificare quali ruoli un utente può assumere.

Per configurare JDBC per l'autenticazione in Microsoft Azure AD

- Configurare il client di database per connettersi al cluster tramite JDBC usando Azure AD Single Sign-On.

È possibile utilizzare qualsiasi client che utilizza un driver JDBC per connettersi tramite Azure AD Single Sign-On o usare un linguaggio come Java per connettersi utilizzando uno script. Per informazioni sull'installazione e sulla configurazione, consulta [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).

Ad esempio, è possibile utilizzare SQLWorkBench/j come client. Quando si configura SQLWorkBench/j, l'URL del database utilizza il seguente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se si utilizza SQLWorkBench/j come client, attenersi alla seguente procedura:

- a. Avvia SQL Workbench/J. Sulla pagina Seleziona profilo di connessione, aggiungi un Gruppo di profili denominato **AzureAuth**.
- b. Per Connection Profile (Profilo connessione), immettere **Azure**.

- c. Selezionare Manage Drivers (Gestisci driver), quindi Amazon Redshift. Scegliere l'icona Open Folder (Apri cartella) accanto a Library (Libreria), quindi scegliere il file JDBC .jar appropriato.
- d. Nella pagina Select Connection Profile (Seleziona profilo connessione), aggiungere informazioni al profilo di connessione come segue:
  - Per User (Utente), immettere il nome utente di Microsoft Azure. Si tratta del nome utente dell'account Microsoft Azure che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster per il quale si sta tentando di autenticare l'utilizzo.
  - Per Password, immettere la password di Microsoft Azure.
  - Per Drivers (Driver), scegliere Amazon Redshift (com.amazon.comredshift.jdbc.driver).
  - Per URL, immettere **jdbc:redshift:iam://*your-cluster-identifier*:*your-cluster-region*/*your-database-name***.
- e. Scegliere Extended Properties (Proprietà estese) per aggiungere ulteriori informazioni alle proprietà di connessione, come descritto di seguito:

Per la configurazione Single Sign-On di Azure AD, aggiungere ulteriori informazioni come segue:

- Per plugin\_name, immettere **com.amazon.redshift.plugin.AzureCredentialsProvider**. Questo valore indica al driver di utilizzare Azure AD Single Sign-On come metodo di autenticazione.
- Per idp\_tenant, immettere ***your-idp-tenant***. Utilizzato solo per Microsoft Azure AD. Si tratta del nome tenant dell'azienda configurata in Azure AD. Questo valore può essere il nome del tenant o l'ID univoco tenant con trattini.
- Per client\_secret, immettere ***your-azure-redshift-application-client-secret***. Utilizzato solo per Microsoft Azure AD. Questo è il segreto client dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On. Questo è applicabile solo al com.amazon.redshift.plugin.AzureCredentialsProvider plugin.
- Per client\_id, immettere ***your-azure-redshift-application-client-id***. Utilizzato solo per Microsoft Azure AD. Si tratta dell'ID client (con trattini) dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On.

Per la configurazione Single Sign-On di Azure AD con autenticazione a più fattori (MFA), aggiungere ulteriori informazioni alle proprietà di connessione come segue:

- Per `plugin_name`, immettere **`com.amazon.redshift.plugin.BrowserAzureCredentialsProvider`**. Questo valore indica al driver di utilizzare Single Sign-On di Azure AD con autenticazione a più fattori (MFA) come metodo di autenticazione.
- Per `idp_tenant`, immettere **`your-idp-tenant`**. Utilizzato solo per Microsoft Azure AD. Si tratta del nome tenant dell'azienda configurata in Azure AD. Questo valore può essere il nome del tenant o l'ID univoco tenant con trattini.
- Per `client_id`, immettere **`your-azure-redshift-application-client-id`**. Questa opzione è utilizzata solo per Microsoft Azure AD. Si tratta dell'ID client (con trattini) dell'applicazione Amazon Redshift creata durante la configurazione di Single Sign-On di Azure AD con autenticazione a più fattori (MFA).
- Per `listen_port`, immettere **`your-listen-port`**. Questa è la porta ascoltata dal server locale. Il valore predefinito è 7890.
- In `idp_response_timeout`, immettere **`the-number-of-seconds`**. Questo è il numero di secondi di attesa prima del timeout quando il server IdP restituisce una risposta. Il numero minimo di secondi deve essere 10. Se stabilire la connessione richiede più tempo della soglia prevista, l'operazione viene interrotta.

Per configurare ODBC per l'autenticazione in Microsoft Azure AD

- Configurare il client di database per connettersi al cluster tramite ODBC utilizzando Azure AD Single Sign-On.

Amazon Redshift fornisce driver ODBC per i sistemi operativi Linux, Windows e macOS. Prima di installare un driver ODBC, è necessario determinare se lo strumento client SQL è a 32 o 64 bit. Installare il driver ODBC che soddisfa i requisiti dello strumento client SQL.

Installa e configura il driver ODBC di Amazon Redshift più recente per il sistema operativo in uso nel modo seguente:

- In Windows esegui [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).
- Per macOS, consulta [Installazione del driver ODBC di Amazon Redshift su macOS X](#).
- Per Linux, consulta [Installazione del driver ODBC di Amazon Redshift su Linux](#).

In Windows, nella pagina Amazon Redshift ODBC Driver DSN Setup (Configurazione DSN Driver ODBC Amazon Redshift) in Connection Settings (Impostazioni connessione), immettere le seguenti informazioni:

- Per Data Source Name (Nome origine dati), immettere ***your-DSN***. Specificare il nome dell'origine dati utilizzato come nome del profilo ODBC.
- Nel campo Tipo di autenticazione per la configurazione Single Sign-On di Azure AD, scegliere **Identity Provider: Azure AD**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per autenticare mediante Azure Single Sign-On.
- Nel campo Tipo di autenticazione per la configurazione Single Sign-On di Azure AD con autenticazione a più fattori (MFA), scegliere **Identity Provider: Browser Azure AD**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per autenticare mediante Azure Single Sign-On con MFA.
- Per Cluster ID (ID cluster), immettere ***your-cluster-identifier***.
- Per Region (Regione), immettere ***your-cluster-region***.
- Per Database, immettere ***your-database-name***.
- Per User (Utente), immettere ***your-azure-username***. Si tratta del nome utente dell'account Microsoft Azure che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster per il quale si sta tentando di autenticare l'utilizzo. Utilizzarlo solo se Auth Type (Tipo di autorizzazione) è Identity Provider: Azure AD (Provider di identità: Azure AD).
- Per Password, immettere ***your-azure-password***. Utilizzarlo solo se Auth Type (Tipo di autorizzazione) è Identity Provider: Azure AD (Provider di identità: Azure AD).
- Per iDP Tenant (Tenant Idp), immettere ***your-idp-tenant***. Si tratta del nome del tenant della società configurata in IDP (Azure). Questo valore può essere il nome del tenant o l'ID univoco tenant con trattini.
- Per Azure Client Secret (Segreto client di Azure), immettere ***your-azure-redshift-application-client-secret***. Questo è il segreto client dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On.
- Per Azure Client ID (ID client di Azure), immettere ***your-azure-redshift-application-client-id***. Si tratta dell'ID client (con trattini) dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On.

- Per Listen Port (Porta di ascolto), immettere ***your-listen-port***. Questa è la porta di ascolto predefinita ascoltata dal server locale. Il valore predefinito è 7890. Si applica solo al plug-in Browser Azure AD.
- In Response Timeout (Timeout di risposta), immettere ***the-number-of-seconds***. Questo è il numero di secondi di attesa prima del timeout quando il server IdP restituisce una risposta. Il numero minimo di secondi deve essere 10. Se stabilire la connessione richiede più tempo della soglia prevista, l'operazione viene interrotta. Questa opzione si applica solo al plug-in Browser Azure AD.

Su macOS e Linux, modificare il file `odbc.ini` come segue:

 Note

Tutte le voci non fanno distinzione tra maiuscole e minuscole.

- Per `clusterid`, immettere ***your-cluster-identifier***. Questo è il nome del cluster Amazon Redshift creato.
- Per `region`, immettere ***your-cluster-region***. Questa è la AWS regione del cluster Amazon Redshift creato.
- Per `database`, immettere ***your-database-name***. Questo è il nome del database a cui si sta provando ad accedere nel cluster Amazon Redshift.
- Per `locale`, immettere ***en-us***. Questa è la lingua in cui vengono visualizzati i messaggi di errore.
- Per `iam`, immettere ***1***. Questo valore consente al driver di eseguire l'autenticazione utilizzando le credenziali IAM.
- In `plugin_name` per la configurazione Single Sign-On di Azure AD, immettere ***AzureAD***. Specifica al driver di utilizzare Azure Single Sign-On come metodo di autenticazione.
- In `plugin_name` per la configurazione Single Sign-On di Azure AD con autenticazione a più fattori (MFA), immettere ***BrowserAzureAD***. Indica al driver di utilizzare Azure Single Sign-On con MFA come metodo di autenticazione.
- Per `uid`, immettere ***your-azure-username***. Si tratta del nome utente dell'account Microsoft Azure che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster a cui si sta tentando di autenticarsi. Utilizzare solo per `plugin_name` è `AzureAD`.

- Per PWD, immettere ***your-azure-password***. Utilizzare solo per plugin\_name è AzureAD.
- Per idp\_tenant, immettere ***your-idp-tenant***. Si tratta del nome del tenant della società configurata in IDP (Azure). Questo valore può essere il nome del tenant o l'ID univoco tenant con trattini.
- Per client\_secret, immettere ***your-azure-redshift-application-client-secret***. Questo è il segreto client dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On.
- Per client\_id, immettere ***your-azure-redshift-application-client-id***. Si tratta dell'ID client (con trattini) dell'applicazione Amazon Redshift creata durante la configurazione di Azure Single Sign-On.
- Per listen\_port, immettere ***your-listen-port***. Questa è la porta ascoltata dal server locale. Il valore predefinito è 7890. Questo si applica al plug-in Browser Azure AD.
- In idp\_response\_timeout, immettere ***the-number-of-seconds***. Questo è il periodo di tempo specificato in secondi di attesa della risposta da Azure. Questa opzione si applica al plug-in Browser Azure AD.

Su macOS e Linux, modificare anche le impostazioni del profilo per aggiungere le seguenti esportazioni.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Per risolvere i problemi con il plugin Browser Azure AD

1. Per usare il plugin Browser Azure AD, è necessario impostare l'URL di risposta specificato nella richiesta in modo che corrisponda all'URL di risposta configurato per l'applicazione.

Passare alla pagina Configura Single Sign-On con SAML nel portale di Microsoft Azure. Quindi controllare che l'URL di risposta sia impostato su `http://localhost/redshift/`.

2. Se viene visualizzato un errore tenant IdP, verificare che il nome tenant IdP corrisponda al nome di dominio utilizzato inizialmente per configurare Active Directory in Microsoft Azure.

Su Windows, passa alla sezione Impostazioni connessione della pagina Configurazione DSN ODBC di Amazon Redshift. Verificare quindi che il nome del tenant della società configurata

nell'IdP (Azure) corrisponda al nome di dominio utilizzato inizialmente per configurare Active Directory in Microsoft Azure.

Su macOS e Linux, trova il file `odbc.ini`. Verificare quindi che il nome del tenant della società configurata nell'IdP (Azure) corrisponda al nome di dominio utilizzato inizialmente per configurare Active Directory in Microsoft Azure.

3. Se viene visualizzato un errore che indica che l'URL di risposta specificato nella richiesta non corrisponde agli URL di risposta configurati per l'applicazione, verificare che gli URI di reindirizzamento siano uguali all'URL di risposta.

Passare alla pagina di registrazione app dell'applicazione nel portale di Microsoft Azure. Quindi controllare che gli URI di reindirizzamento corrispondano all'URL di risposta.

4. Se si ottiene la risposta imprevista: errore non autorizzato, verificare di aver completato la configurazione delle applicazioni mobili e desktop.

Passare alla pagina di registrazione app dell'applicazione nel portale di Microsoft Azure. Quindi passare a Autenticazione e verificare di aver configurato le applicazioni mobili e desktop per utilizzare `http://localhost/redshift/` come URI di reindirizzamento.

## Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con AD FS

Puoi utilizzare AD FS come provider di identità (IdP) per accedere al cluster Amazon Redshift. Di seguito, è possibile trovare una procedura che descrive come impostare una relazione di trust per questo scopo. Per ulteriori informazioni sulla configurazione AWS come fornitore di servizi per AD FS, consulta [Configuring Your SAML 2.0 IdP with Relying Party Trust e Adding Claims nella IAM User Guide](#).

Per configurare AD FS e il tuo AWS account in modo che si fidino l'uno dell'altro

1. Crea o utilizza un cluster Amazon Redshift esistente a cui possono connettersi gli utenti di AD FS. Per configurare la connessione, sono necessarie alcune proprietà di questo cluster, ad esempio l'identificatore del cluster. Per ulteriori informazioni, consulta [Creazione di un cluster](#).
2. Configura AD FS per controllare l'accesso di Amazon Redshift nella Console di gestione Microsoft:
  1. Scegliere ADFS 2.0, quindi selezionare Add Relying Party Trust (Aggiungi relazione di trust). Nella pagina Add Relying Party Trust Wizard (Aggiunta guidata relazione di trust), scegliere Start (Avvia).

2. Nella pagina Select Data Source (Seleziona origine dati), scegliere Import data about the relying party published online or on a local network (Importa dati sul relying party pubblicati online o in una rete locale).
3. Per Federation metadata address (host name or URL) (Indirizzo dei metadati della federazione (nome host o URL)), immettere **https://signin.aws.amazon.com/saml-metadata.xml**. Il file XML di metadati è un documento di metadati SAML standard che viene descritto AWS come relying party.
4. Nella pagina Specify Display Name (Specificare nome visualizzato), immettere un valore per Display name (Nome visualizzato).
5. Nella pagina Choose Issuance Authorization Rules (Scegli regole di autorizzazione di emissione), scegliere una regola di autorizzazione di emissione per consentire o rifiutare a tutti gli utenti l'accesso a questo relying party.
6. Nella pagina Ready to Add Trust (Pronto ad aggiungere trust), rivedere le impostazioni.
7. Nella pagina Finish (Termina), scegliere Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (Apri la finestra di dialogo Modifica regole di registrazione per questa relazione di trust quando si chiude la procedura guidata).
8. Nel menu di scelta rapida, scegliere Relying Party Trusts (Relazione di trust).
9. Per il relying party, aprire il menu contestuale e scegliere Edit Claim Rules (Modifica regole di registrazione). Nella pagina Edit Claim Rules (Modifica regole di registrazione), scegliere Add Rule (Aggiungi regola).
10. Per il modello di regola di reclamo, scegli Trasforma un reclamo in entrata, quindi nella Nameld pagina Modifica regola, procedi come segue:
  - Per il nome della regola di reclamo, inserisci Nameld.
  - In Incoming claim name (Nome registrazione in ingresso), scegliere Windows Account Name (Nome account Windows).
  - In Outgoing claim name (Nome registrazione in uscita), scegliere Name ID (ID nome).
  - In Outgoing name ID format (Formato ID nome in uscita), scegliere Persistent Identifier (Identificatore persistente).
  - Scegliere Pass through all claim values (Passaggio di tutti i valori di registrazione).
11. Nella pagina Edit Claim Rules (Modifica regole di registrazione), scegliere Add Rule (Aggiungi regola). Nella pagina Select Rule Template (Seleziona modello regola) per Claim rule template (Modello regola registrazione), scegliere Send LDAP Attributes as Claims (Invia attributi LDAP come registrazioni).

12. Nella pagina Configure Rule (Configura regola), procedere come segue:

- In Claim rule name (Nome regola di attestazione), inserisci RoleSessionName.
- In Attribute store (Archivio attributi), scegliere Active Directory.
- In LDAP Attribute (Attributo LDAP), scegliere Email Addresses (Indirizzi di posta elettronica).
- Per Tipo di attestazione in uscita, scegli <https://aws.amazon.com/SAML/Attributes/RoleSessionName>.

13. Nella pagina Edit Claim Rules (Modifica regole di registrazione), scegliere Add Rule (Aggiungi regola). Nella pagina Select Rule Template (Seleziona modello regola), per Claim rule template (Modello regola di registrazione), scegliere Send Claims Using a Custom Rule (Invia registrazioni utilizzando una regola personalizzata).

14. Nella pagina Edit Rule – Get AD Groups (Modifica regola — Ottieni AD), per Claim rule name (Nome regola registrazione), immettere Get AD Groups (Ottieni gruppi AD).

15. Per Custom rule (Regola personalizzata), immettere quanto segue.

```
c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer == "AD AUTHORITY"] => add(store = "Active Directory",
types = ("http://temp/variable"), query = ";tokenGroups;{0}");
param = c.Value);
```

16. Nella pagina Edit Claim Rules (Modifica regole di registrazione), scegliere Add Rule (Aggiungi regola). Nella pagina Select Rule Template (Seleziona modello regola), per Claim rule template (Modello regola di registrazione), scegliere Send Claims Using a Custom Rule (Invia registrazioni utilizzando una regola personalizzata).

17. Nella pagina Edit Rule – Roles (Modifica regola - Ruoli), in Claim rule name (Nome regola di registrazione), digitare Roles (Ruoli).

18. Per Custom rule (Regola personalizzata), immettere quanto segue.

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-"] =>
issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
RegexReplace(c.Value, "AWS-", "arn:aws:iam::123456789012:saml-provider/ADFS,arn:aws:iam::123456789012:role/ADFS-"));
```

Prendere nota degli ARN del provider SAML e del ruolo da assumere. In questo esempio, `arn:aws:iam:123456789012:saml-provider/ADFS` è l'ARN del provider SAML ed `arn:aws:iam:123456789012:role/ADFS-` è l'ARN del ruolo.

3. Accertarsi di aver scaricato il file `federationmetadata.xml`. Verificare che il documento non contenga caratteri non validi. Questo è il file di metadati con cui configuri la relazione di trust.  
AWS
4. Creare un provider di identità SAML IAM nella console IAM. Il documento dei metadati fornito è il file XML dei metadati di federazione salvato quando si configura l'applicazione Azure Enterprise. Per la procedura dettagliata, consulta [Creazione e gestione di un provider di identità IAM \(console\)](#) nella Guida per l'utente di IAM.
5. Creare un ruolo IAM per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consultare [Creazione di un ruolo per SAML](#) nella Guida per l'utente di IAM.
6. Creare una policy IAM che è possibile collegare al ruolo IAM creato per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM. Per un esempio di Azure AD, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

Per configurare JDBC per l'autenticazione in AD FS

- Configurare il client di database per connettersi al cluster tramite JDBC usando Single Sign-On di Azure AD.

È possibile utilizzare qualsiasi client che utilizza un driver JDBC per connettersi tramite Single Sign-On di AD FS o usare un linguaggio come Java per connettersi mediante uno script. Per informazioni sull'installazione e sulla configurazione, consulta [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).

Ad esempio, è possibile utilizzare SQLWorkBench/j come client. Quando si configura SQLWorkBench/j, l'URL del database utilizza il seguente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se si utilizza SQLWorkBench/j come client, attenersi alla seguente procedura:

- a. Avvia SQL Workbench/J. Nella pagina Seleziona profilo connessione, aggiungi un Gruppo di profili, ad esempio **ADFS**.

- b. In Connection Profile (Profilo connessione), immettere il nome del profilo di connessione, ad esempio **ADFS**.
- c. Selezionare Manage Drivers (Gestisci driver), quindi Amazon Redshift. Scegliere l'icona Open Folder (Apri cartella) accanto a Library (Libreria), quindi scegliere il file JDBC .jar appropriato.
- d. Nella pagina Select Connection Profile (Seleziona profilo connessione), aggiungere informazioni al profilo di connessione come segue:
  - In User (Utente), immettere il nome utente AD FS. Si tratta del nome utente dell'account che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster per il quale si sta tentando di autenticare l'utilizzo.
  - In Password, immettere la password AD FS.
  - Per Drivers (Driver), scegliere Amazon Redshift (com.amazon.comredshift.jdbc.driver).
  - Per URL, immettere **`jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name`**.
- e. Scegli Proprietà estese. Per plugin\_name, immettere **`com.amazon.redshift.plugin.AdfsCredentialsProvider`**. Questo valore indica al driver di utilizzare Single Sign-On di Azure AD come metodo di autenticazione.

Per configurare ODBC per l'autenticazione ad AD FS

- Configurare il client di database per connettersi al cluster tramite ODBC utilizzando Single Sign-On di Azure AD.

Amazon Redshift fornisce driver ODBC per i sistemi operativi Linux, Windows e macOS. Prima di installare un driver ODBC, è necessario determinare se lo strumento client SQL è a 32 o 64 bit. Installare il driver ODBC che soddisfa i requisiti dello strumento client SQL.

Installa e configura il driver ODBC di Amazon Redshift più recente per il sistema operativo in uso nel modo seguente:

- In Windows esegui [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).
- Per macOS, consulta [Installazione del driver ODBC di Amazon Redshift su macOS X](#).
- Per Linux, consulta [Installazione del driver ODBC di Amazon Redshift su Linux](#).

In Windows, nella pagina Amazon Redshift ODBC Driver DSN Setup (Configurazione DSN Driver ODBC Amazon Redshift) in Connection Settings (Impostazioni connessione), immettere le seguenti informazioni:

- Per Data Source Name (Nome origine dati), immettere ***your-DSN***. Specificare il nome dell'origine dati utilizzato come nome del profilo ODBC.
- Per Tipo di autenticazione, scegli Provider di identità: SAML. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per autenticare mediante Single Sign-On di AD FS.
- Per Cluster ID (ID cluster), immettere ***your-cluster-identifier***.
- Per Region (Regione), immettere ***your-cluster-region***.
- Per Database, immettere ***your-database-name***.
- Per User (Utente), immettere ***your-adfs-username***. Si tratta del nome utente dell'account AD FS che si sta utilizzando per l'accesso Single Sign-On con autorizzazioni per il cluster per il quale si sta tentando di autenticare l'utilizzo. Utilizzarlo solo per Auth type (Tipo di autenticazione) è Identity Provider: SAML (Provider di identità: SAML).
- Per Password, immettere ***your-adfs-password***. Utilizzarlo solo per Auth type (Tipo di autenticazione) è Identity Provider: SAML (Provider di identità: SAML).

Su macOS e Linux, modificare il file `odbc.ini` come segue:

 Note

Tutte le voci non fanno distinzione tra maiuscole e minuscole.

- Per `clusterid`, immettere ***your-cluster-identifier***. Questo è il nome del cluster Amazon Redshift creato.
- Per `region`, immettere ***your-cluster-region***. Questa è la AWS regione del cluster Amazon Redshift creato.
- Per `database`, immettere ***your-database-name***. Questo è il nome del database a cui si sta provando ad accedere nel cluster Amazon Redshift.
- Per `locale`, immettere ***en-us***. Questa è la lingua in cui vengono visualizzati i messaggi di errore.

- Per iam, immettere **1**. Questo valore consente al driver di eseguire l'autenticazione utilizzando le credenziali IAM.
- Per plugin\_name, effettuare una delle seguenti operazioni:
  - Per la configurazione di Single Sign-On di AD FS con autenticazione a più fattori (MFA), immettere **BrowserSAML**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per l'autenticazione ad AD FS.
  - Per la configurazione di Single Sign-On di AD FS, immettere **ADFS**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Azure AD.
- Per uid, immettere ***your-adfs-username***. Si tratta del nome utente dell'account Microsoft Azure che si sta utilizzando per Single Sign-On con autorizzazioni per il cluster a cui si sta tentando di autenticarsi. Utilizzare solo se plugin\_name è ADFS.
- Per PWD, immettere ***your-adfs-password***. Utilizzare solo se plugin\_name è ADFS.

Su macOS e Linux, modificare anche le impostazioni del profilo per aggiungere le seguenti esportazioni.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

## Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Ping Identity

Puoi utilizzare Ping Identity come provider di identità (IdP) per accedere al cluster Amazon Redshift. Di seguito, puoi trovare una procedura che descrive come impostare una relazione di fiducia a questo scopo utilizzando il PingOne portale. Per ulteriori informazioni sulla configurazione AWS come fornitore di servizi per Ping Identity, consulta [Configuring Your SAML 2.0 IdP with Relying Party Trust e Adding Claims nella IAM User Guide](#).

Per configurare Ping Identity e il tuo AWS account in modo che si fidino l'uno dell'altro

1. Crea o utilizza un cluster Amazon Redshift esistente a cui possono accedere gli utenti di Ping Identity. Per configurare la connessione, sono necessarie alcune proprietà di questo cluster, ad esempio l'identificatore del cluster. Per ulteriori informazioni, consulta [Creazione di un cluster](#).

2. Aggiungi Amazon Redshift come nuova applicazione SAML sul portale. PingOne Per i passaggi dettagliati, vedere la [documentazione relativa all'identità di ping](#).
  1. Passare a My Applications (Le mie applicazioni).
  2. In Add Application (Aggiungi applicazione), scegliere New SAML Application (Nuova applicazione SAML).
  3. Per Application name (Nome applicazione), immettere **Amazon Redshift**.
  4. Per Protocol Version (Versione protocollo), scegliere SAML v2.0.
  5. Per Category (Categoria), scegliere ***your-application-category***.
  6. Per Assertion Consumer Service (ACS), digitare ***your-redshift-local-host-url***. Questo è l'host locale e la porta verso cui l'asserzione SAML esegue il reindirizzamento.
  7. Per Entity ID (ID entità), inserisci `urn:amazon:webservices`.
  8. Per Signing (Firma), scegliere Sign Assertion (Asserzione firma).
  9. Nella sezione SSO Attribute Mapping (Mappatura degli attributi SSO), creare le registrazioni come illustrato nella tabella seguente.

Attributo Application	Attributo Identity Bridge del valore letterale
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<i>arn:aws:iam:: 123456789012:role/ping, arn:aws:iam:: 123456789012:saml-provider/PingProvider</i>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	e-mail
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	"true"
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	e-mail

Attributo Application	Attributo Identity Bridge del valore letterale
<p><code>https://redshift.amazon.com/SAML/Attributes/ DbGroups</code></p>	<p>I gruppi negli attributi «DbGroups» contengono il prefisso @directory. Per rimuoverlo, in Identità Bridge, specifica memberOf. In Funzione, scegliete ExtractBy RegularExpression. In Espressione, specifica <code>(.*)\[@](?:.*).</code></p>

3. Per Group Access (Accesso di gruppo), impostare il seguente accesso di gruppo, se necessario:
  - `https://aws.amazon.com/SAML/Attributes/Role`
  - `https://aws.amazon.com/SAML/Attributes/RoleSessionName`
  - `https://redshift.amazon.com/SAML/Attributes/AutoCreate`
  - `https://redshift.amazon.com/SAML/Attributes/DbUser`
4. Rivedere la configurazione e apportare modifiche, se necessario.
5. Utilizzare Initiate Single Sign-On (SSO) URL (URL Single Sign-On (SSO) di avvio) come URL di accesso per il plugin Browser SAML.
6. Creare un provider di identità SAML IAM nella console IAM. Il documento dei metadati fornito è il file XML dei metadati di federazione salvato quando si configura l'applicazione Ping Identity. Per la procedura dettagliata, consulta [Creazione e gestione di un provider di identità IAM \(console\)](#) nella Guida per l'utente di IAM.
7. Creare un ruolo IAM per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di un ruolo per SAML](#) nella Guida per l'utente di IAM.
8. Creare una policy IAM che è possibile collegare al ruolo IAM creato per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM. Per un esempio di Azure AD, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

### Come configurare JDBC per l'autenticazione in Ping Identity

- Configura il client di database per connettersi al cluster tramite JDBC utilizzando Single Sign-On di Ping Identity.

È possibile utilizzare qualsiasi client che utilizza un driver JDBC per connettersi tramite Single Sign-On di Ping Identity o usare un linguaggio come Java per connettersi mediante uno script.

Per informazioni sull'installazione e sulla configurazione, consulta [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).

Ad esempio, è possibile utilizzare SQLWorkBench/j come client. Quando si configura SQLWorkBench/j, l'URL del database utilizza il seguente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se si utilizza SQLWorkBench/j come client, attenersi alla seguente procedura:

- a. Avvia SQL Workbench/J. Nella pagina Seleziona profilo connessione, aggiungi un Gruppo di profili, ad esempio **Ping**.
- b. Per Connection Profile (Profilo connessione), immettere ***your-connection-profile-name***, ad esempio **Ping**.
- c. Selezionare Manage Drivers (Gestisci driver), quindi Amazon Redshift. Scegliere l'icona Open Folder (Apri cartella) accanto a Library (Libreria), quindi scegliere il file JDBC .jar appropriato.
- d. Nella pagina Select Connection Profile (Seleziona profilo connessione), aggiungere informazioni al profilo di connessione come segue:
  - Per Utente, inserisci il tuo nome PingOne utente. Questo è il nome utente dell' PingOne account che stai utilizzando per il Single Sign-On che dispone dell'autorizzazione per il cluster che stai cercando di utilizzare per l'autenticazione.
  - Per Password, inserisci la tua password. PingOne
  - Per Drivers (Driver), scegliere Amazon Redshift (com.amazon.comredshift.jdbc.driver).
  - Per URL, immettere ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***.
- e. Scegliere Extended Properties (Proprietà estese) ed effettuare una delle seguenti operazioni:
  - Per login\_url, immettere ***your-ping-ss0-login-url***. Questo valore specifica l'URL per utilizzare Single Sign-On come autenticazione di accesso.
  - Per Ping Identity, in plugin\_name, immetti **com.amazon.redshift.plugin.PingCredentialsProvider**. Questo valore indica al driver di utilizzare Single Sign-On di Ping Identity come metodo di autenticazione.

- Per Ping Identity con Single Sign-On, in `plugin_name` immettere **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**. Questo valore specifica al driver di utilizzare Ping Identity PingOne con Single Sign-on come metodo di autenticazione.

## Come configurare ODBC per l'autenticazione in Ping Identity

- Configura il client del database per la connessione al cluster tramite ODBC utilizzando Ping Identity Single Sign-on. PingOne

Amazon Redshift fornisce driver ODBC per i sistemi operativi Linux, Windows e macOS. Prima di installare un driver ODBC, è necessario determinare se lo strumento client SQL è a 32 o 64 bit. Installare il driver ODBC che soddisfa i requisiti dello strumento client SQL.

Installa e configura il driver ODBC di Amazon Redshift più recente per il sistema operativo in uso nel modo seguente:

- In Windows esegui [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).
- Per macOS, consulta [Installazione del driver ODBC di Amazon Redshift su macOS X](#).
- Per Linux, consulta [Installazione del driver ODBC di Amazon Redshift su Linux](#).

In Windows, nella pagina Amazon Redshift ODBC Driver DSN Setup (Configurazione DSN Driver ODBC Amazon Redshift) in Connection Settings (Impostazioni connessione), immettere le seguenti informazioni:

- Per Data Source Name (Nome origine dati), immettere ***your-DSN***. Specificare il nome dell'origine dati utilizzato come nome del profilo ODBC.
- In Auth type (Tipo di autenticazione), procedere in uno dei seguenti modi:
  - Per la configurazione di Ping Identity, seleziona Provider di identità: federazione Ping. Questo è il metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Ping Identity.
  - Per la configurazione di Ping Identity con Single Sign-On, scegliere Identity Provider: Browser SAML (Provider identità: browser SAML). Questo è il metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Ping Identity con Single Sign-On.

- Per Cluster ID (ID cluster), immettere ***your-cluster-identifier***.
- Per Region (Regione), immettere ***your-cluster-region***.
- Per Database, immettere ***your-database-name***.
- Per User (Utente), immettere ***your-ping-username***. Questo è il nome utente dell' PingOne account che stai utilizzando per il Single Sign-On che dispone dell'autorizzazione per il cluster che stai cercando di utilizzare per l'autenticazione. Usalo solo per il tipo di autenticazione come Identity Provider: PingFederate
- Per Password, immettere ***your-ping-password***. Usalo solo perché il tipo di autenticazione è Identity Provider: PingFederate
- Per Listen Port (Porta di ascolto), immettere ***your-listen-port***. Questa è la porta ascoltata dal server locale. Il valore predefinito è 7890. Questo si applica solo al plugin Browser SAML.
- In Response Timeout (Timeout di risposta), immettere ***the-number-of-seconds***. Questo è il numero di secondi di attesa prima del timeout quando il server IdP restituisce una risposta. Il numero minimo di secondi deve essere 10. Se stabilire la connessione richiede più tempo della soglia prevista, l'operazione viene interrotta. Questo si applica solo al plugin Browser SAML.
- Per Login URL (URL di accesso), immettere ***your-login-url***. Questo si applica solo al plugin Browser SAML.

Su macOS e Linux, modificare il file `odbc.ini` come segue:

 Note

Tutte le voci non fanno distinzione tra maiuscole e minuscole.

- Per `clusterid`, immettere ***your-cluster-identifier***. Questo è il nome del cluster Amazon Redshift creato.
- Per `region`, immettere ***your-cluster-region***. Questa è la AWS regione del cluster Amazon Redshift creato.
- Per `database`, immettere ***your-database-name***. Questo è il nome del database a cui si sta provando ad accedere nel cluster Amazon Redshift.
- Per `locale`, immettere ***en-us***. Questa è la lingua in cui vengono visualizzati i messaggi di errore.

- Per iam, immettere **1**. Questo valore consente al driver di eseguire l'autenticazione utilizzando le credenziali IAM.
- Per plugin\_name, effettuare una delle seguenti operazioni:
  - Per la configurazione di Ping Identity, immetti **BrowserSAML**. Questo è il metodo di autenticazione utilizzato dal driver ODBC per l'autenticazione in Ping Identity.
  - Per la configurazione di Ping Identity con Single Sign-On, immettere **Ping**. Questo è il metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Ping Identity con Single Sign-On.
- Per uid, immettere **your-ping-username**. Si tratta del nome utente dell'account Microsoft Azure che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster a cui si sta tentando di autenticarsi. Utilizzare solo se plugin\_name è Ping.
- Per PWD, immettere **your-ping-password**. Utilizzare solo se plugin\_name è Ping.
- Per login\_url, immettere **your-login-url**. Questo è l'URL Single Sign-On di avvio che restituisce la risposta SAML. Questo si applica solo al plugin Browser SAML.
- In idp\_response\_timeout, immettere **the-number-of-seconds**. Questo è il periodo di tempo specificato, in secondi, per attendere la risposta da PingOne Identity. Questo si applica solo al plugin Browser SAML.
- Per listen\_port, immettere **your-listen-port**. Questa è la porta ascoltata dal server locale. Il valore predefinito è 7890. Questo si applica solo al plugin Browser SAML.

Su macOS e Linux, modificare anche le impostazioni del profilo per aggiungere le seguenti esportazioni.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

## Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Okta

Puoi utilizzare Okta come un provider di identità (IdP) per accedere al cluster Amazon Redshift. Di seguito, è possibile trovare una procedura che descrive come impostare una relazione di trust per questo scopo. Per ulteriori informazioni sulla configurazione AWS come fornitore di servizi per Okta, consulta [Configuring Your SAML 2.0 IdP with Relying Party Trust e Adding Claims nella IAM User Guide](#).

## Per configurare Okta e il tuo account in modo che si fidino l'uno dell'altro AWS

1. Crea o utilizza un cluster Amazon Redshift esistente a cui possono connettersi gli utenti di Okta. Per configurare la connessione, sono necessarie alcune proprietà di questo cluster, ad esempio l'identificatore del cluster. Per ulteriori informazioni, consulta [Creazione di un cluster](#).
2. Aggiungi Amazon Redshift come nuova applicazione sul portale Okta. Per le fasi dettagliate, consultare la [documentazione di Okta](#).
  - Scegliere Add Application (Aggiungi applicazione).
  - In Add Application (Aggiungi applicazione), scegliere Create New App (Crea nuova app).
  - Nella pagina Create a New Add Application Integration (Crea una nuova integrazione di aggiunta applicazioni), per Platform (Piattaforma), scegliere Web.
  - Per Sign on method (Metodo di accesso), scegliere SAML v2.0.
  - Nella pagina General Settings (Impostazioni generali), per App name (Nome app), immettere ***your-redshift-saml-ss0-name***. È il nome dell'applicazione.
  - Nella pagina SAML Settings (Impostazioni SAML) per Single sign on URL (URL Single Sign On), immettere ***your-redshift-local-host-url***. Questo è l'host locale e la porta verso cui l'asserzione SAML esegue il reindirizzamento, ad esempio `http://localhost:7890/redshift/`.
3. Utilizza URL Single Sign On come URL destinatario e URL di destinazione.
4. Per Signing (Firma), scegliere Sign Assertion (Asserzione firma).
5. Per URI del pubblico (ID entità SP), specifica **`urn:amazon:webservicess`** per le attestazioni, come mostrato nella tabella seguente.
6. Nella sezione Advanced Settings (Impostazioni avanzate), per SAML Issuer ID (ID emittente SAML), inserire ***your-Identity-Provider-Issuer-ID***, che puoi trovare nella sezione Visualizza istruzioni di configurazione.
7. Nella sezione Attribute Statements (Istruzioni attributi), creare le registrazioni come illustrato nella tabella seguente.

Nome di registrazione	Valore
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<code>arn:aws:iam::<b><i>123456789012</i></b> :role/<i>Okta</i>,arn:aws:iam::<b><i>123456789012</i></b> :saml-provider/<i>Okta</i></code>

Nome di registrazione	Valore
<a href="https://aws.amazon.com/SAML/Attributes/RoleSessionName">https://aws.amazon.com/SAML/Attributes/RoleSessionName</a>	user.email
<a href="https://redshift.amazon.com/SAML/Attributes/AutoCreate">https://redshift.amazon.com/SAML/Attributes/AutoCreate</a>	"true"
<a href="https://redshift.amazon.com/SAML/Attributes/DbUser">https://redshift.amazon.com/SAML/Attributes/DbUser</a>	user.email

8. Nella sezione App Embed Link (Collegamento incorporamento app), trovare l'URL che è possibile utilizzare come URL di accesso per il plugin SAML Browser.
9. Creare un provider di identità SAML IAM nella console IAM. Il documento dei metadati fornito è il file XML dei metadati di federazione salvato quando durante la configurazione di Okta. Per la procedura dettagliata, consulta [Creazione e gestione di un provider di identità IAM \(console\)](#) nella Guida per l'utente di IAM.
10. Creare un ruolo IAM per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di un ruolo per SAML](#) nella Guida per l'utente di IAM.
11. Creare una policy IAM che è possibile collegare al ruolo IAM creato per la federazione SAML 2.0 nella console IAM. Per la procedura dettagliata, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM. Per un esempio di Azure AD, consulta [Configurazione dell'autenticazione Single Sign-On JDBC o ODBC con Microsoft Azure AD](#).

Per configurare JDBC per l'autenticazione in Okta

- Configurare il client di database per connettersi al cluster tramite JDBC usando Single Sign-On di Okta.

È possibile utilizzare qualsiasi client che utilizza un driver JDBC per connettersi tramite Single Sign-On di Okta o usare un linguaggio come Java per connettersi mediante uno script. Per informazioni sull'installazione e sulla configurazione, consulta [Configurazione di una connessione per la versione 2.1 del driver JDBC per Amazon Redshift](#).

Ad esempio, è possibile utilizzare SQLWorkBench/j come client. Quando si configura SQLWorkBench/j, l'URL del database utilizza il seguente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Se si utilizza SQLWorkBench/j come client, attenersi alla seguente procedura:

- a. Avvia SQL Workbench/J. Nella pagina Seleziona profilo connessione, aggiungi un Gruppo di profili, ad esempio **Okta**.
- b. Per Connection Profile (Profilo connessione), immettere ***your-connection-profile-name***, ad esempio **Okta**.
- c. Selezionare Manage Drivers (Gestisci driver), quindi Amazon Redshift. Scegliere l'icona Open Folder (Apri cartella) accanto a Library (Libreria), quindi scegliere il file JDBC .jar appropriato.
- d. Nella pagina Select Connection Profile (Seleziona profilo connessione), aggiungere informazioni al profilo di connessione come segue:
  - Per User (Utente), immettere il nome utente Okta. Si tratta del nome utente dell'account Okta che si sta utilizzando per Single Sign-On che dispone delle autorizzazioni per il cluster per il quale si sta tentando di autenticare l'utilizzo.
  - Per Password, immettere la password Okta.
  - Per Drivers (Driver), scegliere Amazon Redshift (com.amazon.comredshift.jdbc.driver).
  - Per URL, immettere ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***.
- e. Scegliere Extended Properties (Proprietà estese) ed effettuare una delle seguenti operazioni:
  - Per login\_url, immettere ***your-okta-ssso-login-url***. Questo valore specifica l'URL per utilizzare Single Sign-On come autenticazione per accedere a Okta.
  - Per l'autenticazione Single Sign-On di Okta, in plugin\_name immettere **com.amazon.redshift.plugin.OktaCredentialsProvider**. Questo valore consente al driver di utilizzare l'autenticazione Single Sign-On di Okta come metodo di autenticazione.
  - Per l'autenticazione Single Sign-On di Okta con autenticazione a più fattori (MFA), in plugin\_name immettere **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Questo valore indica al driver di utilizzare Single Sign-On di Okta con autenticazione a più fattori (MFA) come metodo di autenticazione.

## Per configurare ODBC per l'autenticazione in Okta

- Configurare il client di database per connettersi al cluster tramite ODBC mediante Single Sign-On di Azure AD.

Amazon Redshift fornisce driver ODBC per i sistemi operativi Linux, Windows e macOS. Prima di installare un driver ODBC, è necessario determinare se lo strumento client SQL è a 32 o 64 bit. Installare il driver ODBC che soddisfa i requisiti dello strumento client SQL.

Installa e configura il driver ODBC di Amazon Redshift più recente per il sistema operativo in uso nel modo seguente:

- In Windows esegui [Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows](#).
- Per macOS, consulta [Installazione del driver ODBC di Amazon Redshift su macOS X](#).
- Per Linux, consulta [Installazione del driver ODBC di Amazon Redshift su Linux](#).

In Windows, nella pagina Amazon Redshift ODBC Driver DSN Setup (Configurazione DSN Driver ODBC Amazon Redshift) in Connection Settings (Impostazioni connessione), immettere le seguenti informazioni:

- Per Data Source Name (Nome origine dati), immettere ***your-DSN***. Specificare il nome dell'origine dati utilizzato come nome del profilo ODBC.
- In Auth type (Tipo di autenticazione), procedere in uno dei seguenti modi:
  - Per la configurazione Single Sign-On di Okta, scegliere **Identity Provider: Okta**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Okta.
  - Per la configurazione Single Sign-On di Okta con autenticazione a più fattori (MFA), scegliere **Identity Provider: Browser SAML**. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Okta con autenticazione a più fattori (MFA).
- Per Cluster ID (ID cluster), immettere ***your-cluster-identifier***.
- Per Region (Regione), immettere ***your-cluster-region***.
- Per Database, immettere ***your-database-name***.
- Per User (Utente), immettere ***your-okta-username***. Si tratta del nome utente dell'account Okta che si sta utilizzando per Single Sign-On con autorizzazioni per il cluster per il quale si

sta tentando di autenticare l'utilizzo. Utilizzarlo solo per Auth type (Tipo di autenticazione) è Identity Provider: Okta (Provider identità: Okta).

- Per Password, immettere ***your-okta-password***. Utilizzarlo solo per Auth type (Tipo di autenticazione) è Identity Provider: Okta (Provider identità: Okta).

Su macOS e Linux, modificare il file `odbc.ini` come segue:

#### Note

Tutte le voci non fanno distinzione tra maiuscole e minuscole.

- Per `clusterid`, immettere ***your-cluster-identifier***. Questo è il nome del cluster Amazon Redshift creato.
- Per `region`, immettere ***your-cluster-region***. Questa è la AWS regione del cluster Amazon Redshift creato.
- Per `database`, immettere ***your-database-name***. Questo è il nome del database a cui si sta provando ad accedere nel cluster Amazon Redshift.
- Per `locale`, immettere ***en-us***. Questa è la lingua in cui vengono visualizzati i messaggi di errore.
- Per `iam`, immettere ***1***. Questo valore consente al driver di eseguire l'autenticazione utilizzando le credenziali IAM.
- Per `plugin_name`, effettuare una delle seguenti operazioni:
  - Per la configurazione di Single Sign-On di Okta con autenticazione a più fattori (MFA), immettere ***BrowserSAML***. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Okta con autenticazione a più fattori (MFA).
  - Per la configurazione di Single Sign-On di Okta, immettere ***Okta***. Si tratta del metodo di autenticazione utilizzato dal driver ODBC per eseguire l'autenticazione mediante Single Sign-On di Okta.
- Per `uid`, immettere ***your-okta-username***. Si tratta del nome utente dell'account Okta che si sta utilizzando per Single Sign-On con autorizzazioni per il cluster a cui si sta tentando di autenticarsi. Utilizzare solo se `plugin_name` è Okta.
- Per `PWD`, immettere ***your-okta-password***. Utilizzare solo se `plugin_name` è Okta.

- Per `login_url`, immettere ***your-login-url***. Questo è l'URL Single Sign-On di avvio che restituisce la risposta SAML. Questo si applica solo al plugin Browser SAML.
- In `idp_response_timeout`, immettere ***the-number-of-seconds***. Questo è il periodo di tempo specificato, in secondi, da PingOne cui attendere la risposta. Questo si applica solo al plugin Browser SAML.
- Per `listen_port`, immettere ***your-listen-port***. Questa è la porta ascoltata dal server locale. Il valore predefinito è 7890. Questo si applica solo al plugin Browser SAML.

Su macOS e Linux, modificare anche le impostazioni del profilo per aggiungere le seguenti esportazioni.

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

## Opzioni JDBC e ODBC per la creazione di credenziali utente di database

Per creare credenziali utente di database con il driver JDBC o ODBC di Amazon Redshift, devi fornire il nome utente di database come opzione JDBC o ODBC. Facoltativamente, il driver può creare un nuovo utente di database se questo non esiste e puoi specificare un elenco di gruppi di utenti di database a cui l'utente viene aggiunto all'accesso.

Se utilizzi un provider di identità (IdP), collabora con l'amministratore IdP per determinare i valori corretti per queste opzioni. L'amministratore IdP può anche configurare l'IdP per fornire tali opzioni, nel qual caso non devi fornirle come opzioni JDBC o ODBC. Per ulteriori informazioni, consulta [Configurazione di asserzioni SAML per l'IdP](#).

### Note

Se si utilizza una variabile di policy IAM `${redshift:DbUser}`, come descritto in [Politiche relative alle risorse per GetClusterCredentials](#), il valore per `DbUser` è sostituito con il valore recuperato dal contesto della richiesta dell'operazione API. I driver Amazon Redshift utilizzano il valore per la variabile `DbUser` fornito dalla connessione URL, piuttosto che il valore fornito come attributo SAML.

Per proteggere questa configurazione, consigliamo di utilizzare una condizione nella policy IAM per convalidare il valore `DbUser` con il codice `RoleSessionName`. È possibile trovare

esempi di come impostare una condizione utilizzando una policy IAM in [Esempio di politica per l'utilizzo GetClusterCredentials](#).

La tabella seguente elenca le opzioni per la creazione di credenziali utente di database.

Opzione	Descrizione
DbUser	Il nome di un utente di database. Se nel database DbUser esiste un utente denominato, le credenziali utente temporanee dispongono delle stesse autorizzazioni dell'utente esistente. Se DbUser non esiste nel database ed AutoCreate è vero, viene creato un nuovo utente denominato DbUser . Se lo desideri, puoi disabilitare la password di un utente esistente. Per ulteriori informazioni, consultare <a href="#">ALTER_USER</a> .
AutoCreate	true Specificare di creare un utente del database con il nome specificato DbUser se non ne esiste uno. Il valore predefinito è false.
DbGroups	Un elenco delimitato da virgola dei nomi di uno o più dei gruppi di database esistenti a cui viene aggiunto l'utente di database per la sessione corrente. Per impostazione predefinita, il nuovo utente viene aggiunto solo a PUBLIC.

Generazione di credenziali di database per un'identità IAM utilizzando la CLI o l'API di Amazon Redshift

Per generare in modo programmatico credenziali utente temporanee del database, Amazon Redshift fornisce il [get-cluster-credentials](#) comando per il funzionamento AWS Command Line Interface (AWS CLI) e dell'API. [GetClusterCredentials](#) In alternativa, puoi configurare il tuo client SQL con i driver JDBC o ODBC di Amazon Redshift, che gestiscono il processo di chiamata dell'operazione `GetClusterCredentials`, di recupero delle credenziali utente di database e di connessione tra il client SQL e il database Amazon Redshift. Per ulteriori informazioni, consulta [Opzioni JDBC e ODBC per la creazione di credenziali utente di database](#).

#### Note

Consigliamo di utilizzare i driver JDBC o ODBC di Amazon Redshift per generare credenziali utente di database.

In questa sezione, puoi trovare i passaggi per richiamare a livello di codice l'operazione `GetClusterCredentials` o il `get-cluster-credentials` comando, recuperare le credenziali utente del database e connetterti al database.

Per generare e utilizzare credenziali di database temporanee

1. Crea o modifica un utente o un ruolo con le autorizzazioni necessarie. Per ulteriori informazioni sulle autorizzazioni IAM, consultare [Crea un ruolo IAM con le autorizzazioni per la chiamata `GetClusterCredentials`](#).
2. Come utente o ruolo che hai autorizzato nel passaggio precedente, esegui il comando `get-cluster-credentials` CLI o chiama l'operazione `GetClusterCredentials` API e fornisci i seguenti valori:
  - Identificatore del cluster: il nome del cluster contenente il database.
  - Nome utente del database: il nome di un utente del database esistente o nuovo.
    - Se l'utente non esiste nel database ed `AutoCreate` è vero, viene creato un nuovo utente con `PASSWORD` disattivata.
    - Se l'utente non esiste ed `AutoCreate` è falso, la richiesta ha esito negativo.
    - Per questo esempio, il nome utente di database è `temp_creds_user`.
  - `Autocreate`: (facoltativo) crea un nuovo utente se il nome utente di database non esiste.
  - Nome database: il nome del database a cui l'utente è autorizzato ad accedere. Se il nome di database non è specificato, l'utente può accedere a qualsiasi database del cluster.
  - Gruppi di database: (facoltativo) un elenco di gruppi di utenti di database esistenti. Se l'accesso va a buon fine, l'utente di database viene aggiunto al gruppo di utenti specificato. Se non viene specificato alcun gruppo, l'utente dispone solo di autorizzazioni `PUBLIC`. I nomi dei gruppi di utenti devono corrispondere agli ARN delle risorse `dbgroup` specificati nella policy IAM collegata all'utente o al ruolo.
  - Tempo scadenza: (facoltativo) il tempo, in secondi, fino alla scadenza delle credenziali temporanee. È possibile specificare un valore compreso tra 900 secondi (15 minuti) e 3600 secondi (60 minuti). Il valore predefinito è 900 secondi.
3. Amazon Redshift verifica che l'utente disponga dell'autorizzazione per chiamare l'operazione `GetClusterCredentials` con le risorse specificate.
4. Amazon Redshift restituisce una password temporanea e il nome utente di database.

L'esempio seguente utilizza la CLI di Amazon Redshift per generare credenziali di database temporanee per un utente esistente denominato `temp_creds_user`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
temp_creds_user --db-name exampledb --duration-seconds 3600
```

Il risultato è illustrato di seguito.

```
{
  "DbUser": "IAM:temp_creds_user",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDM/
gqX2Eeaq6P3DgTzgPg=="
}
```

L'esempio seguente utilizza la CLI di Amazon Redshift con `autocreate` per generare credenziali di database temporanee per un nuovo utente e per aggiungere l'utente al gruppo `example_group`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user
temp_creds_user --auto-create --db-name exampledb --db-groups example_group --
duration-seconds 3600
```

Il risultato è illustrato di seguito.

```
{
  "DbUser": "IAMA:temp_creds_user:example_group",
  "Expiration": "2016-12-08T21:12:53Z",
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM80yxpDHwXVPyJYBDM/
gqX2Eeaq6P3DgTzgPg=="
}
```

5. Stabilisci una connessione di autenticazione Secure Sockets Layer (SSL) con il cluster Amazon Redshift e invia una richiesta di accesso con il nome utente e la password contenuti nella risposta `GetClusterCredentials`. Includere il prefisso `IAM:` o `IAMA:` con il nome utente, ad esempio `IAM:temp_creds_user` o `IAMA:temp_creds_user`.

#### Important

Configurare il client SQL per richiedere SSL. Se non si esegue questa operazione e il client SQL tenta automaticamente di connettersi con SSL, può utilizzare di nuovo una connessione non SSL in caso di problemi. In tal caso, il primo tentativo di connessione

può non riuscire in quanto le credenziali sono scadute o invalide e il secondo non riesce perché la connessione non è SSL. Se ciò si verifica, è possibile non vedere il primo messaggio di errore. Per ulteriori informazioni sulla connessione al cluster mediante SSL, consultare [Configurazione delle opzioni di sicurezza per le connessioni](#).

6. Se la connessione non utilizza SSL, il tentativo di connessione non riesce.
7. Il cluster invia una richiesta authentication al client SQL.
8. Il client SQL invia quindi la password temporanea al cluster.
9. Se la password è valida e non è scaduta, il cluster completa la connessione.

## Autorizzazione di Amazon Redshift ad accedere ad AWS altri servizi per tuo conto

Alcune funzionalità di Amazon Redshift richiedono che Amazon Redshift acceda ad AWS altri servizi per tuo conto. Ad esempio, i comandi [COPY](#) e [UNLOAD](#) possono caricare o scaricare dati nel cluster Amazon Redshift usando un bucket Amazon S3. Il comando [CREATE EXTERNAL FUNCTION](#) può richiamare una funzione AWS Lambda utilizzando una funzione scalare Lambda definita dall'utente (UDF). Amazon Redshift Spectrum può utilizzare un catalogo di dati in Amazon AWS Glue Athena o. Affinché i cluster Amazon Redshift possano agire per tuo conto, devi fornire le credenziali di sicurezza ai tuoi cluster. Il metodo preferito per fornire le credenziali di sicurezza consiste nello specificare un ruolo AWS Identity and Access Management (IAM). Per i comandi COPY e UNLOAD, puoi fornire le credenziali temporanee.

Gli utenti hanno bisogno di un accesso programmatico se vogliono interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>Per la AWS CLI, consulta <a href="#">Configurazione dell'uso</a></li> </ul>

Quale utente necessita dell'accesso programmatico?	Per	Come
		<p><a href="#">AWS IAM Identity Center</a> nella Guida <a href="#">AWS CLI per l'utente</a>.AWS Command Line Interface</p> <ul style="list-style-type: none"><li>• Per AWS SDK, strumenti e AWS API, consulta <a href="#">l'autenticazione IAM Identity Center</a> nella Guida di riferimento agli AWS SDK e agli strumenti.</li></ul>
IAM	Utilizza credenziali temporane e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in <a href="#">Uso delle credenziali temporanee con AWS risorse</a> nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface</a></li> <li>• Per gli AWS SDK e gli strumenti, consulta <a href="#">Autenticazione tramite credenziali a lungo termine</a> nella Guida di riferimento agli SDK e agli AWS strumenti.</li> <li>• Per le AWS API, consulta <a href="#">Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.</a></li> </ul>

Di seguito, scopri come creare un ruolo IAM con le autorizzazioni appropriate per accedere ad altri servizi. AWS Devi anche associare il ruolo al cluster e specificare l'Amazon Resource Name (ARN) del ruolo quando esegui il comando Amazon Redshift. Per ulteriori informazioni, consulta [Autorizzazione di operazioni COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA utilizzando ruoli IAM.](#)

Inoltre, un utente con privilegi avanzati può concedere il privilegio ASSUMEROLE a utenti e gruppi specifici per fornire l'accesso a un ruolo per le operazioni COPY e UNLOAD. Per ulteriori informazioni, consultare [GRANT](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Creazione di un ruolo IAM per consentire al cluster Amazon Redshift di accedere ai servizi AWS

Per creare un ruolo IAM che consenta al cluster Amazon Redshift di comunicare con altri servizi AWS per tuo conto, completa la procedura riportata di seguito. I valori utilizzati in questa sezione sono esempi, è possibile scegliere i valori in base alle proprie esigenze.

Creare un ruolo IAM per consentire ad Amazon Redshift di accedere ai servizi AWS

1. Aprire la [console IAM](#).
2. Nel pannello di navigazione, selezionare Ruoli.
3. Selezionare Create role (Crea ruolo).
4. Seleziona Servizio AWS e quindi Redshift.
5. In Select your use case (Seleziona il tuo caso d'uso) scegliere Redshift - Customizable (Redshift - Personalizzabile) e quindi scegliere Next: Permissions (Successivo: Autorizzazioni). Verrà visualizzata la pagina Attach permissions policy (Collega policy di autorizzazioni).
6. Per l'accesso ad Amazon S3 tramite COPY, ad esempio, è possibile utilizzare **AmazonS3ReadOnlyAccess** e append. Per l'accesso ad Amazon S3 utilizzando COPY o UNLOAD, consigliamo di creare policy gestite che limitino di conseguenza l'accesso al bucket desiderato e al prefisso. Per le operazioni di lettura e scrittura, consigliamo di applicare i privilegi minimi e di limitare solo i bucket Amazon S3 e i prefissi chiave richiesti da Amazon Redshift.

Per accedere alle funzioni Lambda per il comando CREATE EXTERNAL FUNCTION, aggiungi **AWSLambdaRole**.

Per Redshift Spectrum, oltre all'accesso ad Amazon S3, aggiungere **AWSGlueConsoleFullAccess** o **AmazonAthenaFullAccess**.

Scegli Successivo: Tag.

7. Viene visualizzata la pagina Aggiungi tag. È inoltre possibile aggiungere i tag. Scegli Prossimo: Rivedi.
8. Per Role name (Nome ruolo), digitare un nome per il ruolo, ad esempio **RedshiftCopyUnload**. Scegliere Crea ruolo.
9. Il nuovo ruolo è disponibile per tutti gli utenti nei cluster che usano il ruolo. Per limitare l'accesso solo a utenti specifici in cluster specifici oppure a cluster in regioni specifiche, modificare la relazione di trust per il ruolo. Per ulteriori informazioni, consulta [Limitazione dell'accesso a ruoli IAM](#).

10. Associare il ruolo al cluster. È possibile associare un ruolo IAM a un cluster quando si crea il cluster oppure quando si aggiunge il ruolo a un cluster esistente. Per ulteriori informazioni, consulta [Associazione di ruoli IAM ai cluster](#).

#### Note

Per limitare l'accesso a dati specifici, utilizza un ruolo IAM che concede il minor numero di privilegi richiesti.

## Limitazione dell'accesso a ruoli IAM

Per impostazione predefinita, i ruoli IAM disponibili per un cluster Amazon Redshift sono disponibili per tutti gli utenti del cluster. Puoi decidere di limitare i ruoli IAM a utenti del database Amazon Redshift specifici in cluster specifici oppure a regioni specifiche.

Per permettere solo a utenti del database specifici di usare un ruolo IAM, segui queste fasi.

Per identificare gli utenti del database specifici con accesso a un ruolo IAM

1. Identifica l'Amazon Resource Name (ARN) per gli utenti del database nel cluster Amazon Redshift. L'ARN per un utente del database ha il formato:  
`arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name.`

Per Amazon Redshift serverless utilizza il seguente formato ARN.

`arn:aws:redshift:region:account-id:dbuser:workgroup-name/user-name`

2. Aprire la [console IAM](#).
3. Nel pannello di navigazione, selezionare Ruoli.
4. Scegli il ruolo IAM per limitare a utenti del database Amazon Redshift specifici.
5. Selezionare la scheda Trust Relationships (Relazioni di trust) e quindi scegliere Edit Trust Relationship (Modifica relazione di trust). Un nuovo ruolo IAM che consente ad Amazon Redshift di accedere ad altri AWS servizi per tuo conto ha una relazione di fiducia come segue:

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

```

    "Service": "redshift.amazonaws.com"
  },
  "Action": "sts:AssumeRole"
}
]
}

```

6. Aggiungere una condizione nella sezione dell'operazione `sts:AssumeRole` della relazione di trust che limita il campo `sts:ExternalId` ai valori specificati. Includere un ARN per ogni utente del database a cui si vuole concedere l'accesso al ruolo. L'ID esterno può essere qualsiasi stringa univoca.

Ad esempio, la relazione di trust seguente specifica che solo gli utenti del database `user1` e `user2` nel cluster `my-cluster` nella regione `us-west-2` hanno l'autorizzazione per usare questo ruolo IAM.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": [
            "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user1",
            "arn:aws:redshift:us-west-2:123456789012:dbuser:my-cluster/user2"
          ]
        }
      }
    }
  ]
}

```

7. Scegli `Update Trust Policy` (Aggiorna policy di trust).

## Limitazione di un ruolo IAM a una regione AWS

Puoi limitare l'accessibilità di un ruolo IAM solo in una determinata AWS regione. Per impostazione predefinita, i ruoli IAM per Amazon Redshift non sono limitati a una singola regione.

Per limitare l'uso di un ruolo IAM in base alla regione, segui queste fasi.

Per identificare le regioni permesse per un ruolo IAM

1. Apri la [console IAM](https://console.aws.amazon.com/) all'indirizzo <https://console.aws.amazon.com/>.
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Scegliere il ruolo da modificare con regioni specifiche.
4. Selezionare la scheda Trust Relationships (Relazioni di trust) e quindi scegliere Edit Trust Relationship (Modifica relazione di trust). Un nuovo ruolo IAM che consente ad Amazon Redshift di accedere ad altri AWS servizi per tuo conto ha una relazione di fiducia come segue:

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

5. Modificare l'elenco Service per Principal con l'elenco delle regioni specifiche in cui si vuole permettere l'uso del ruolo. Ogni regione nell'elenco Service deve avere il formato seguente: `redshift.region.amazonaws.com`.

Ad esempio, la relazione di trust modificata seguente permette l'uso del ruolo IAM solo nelle regioni `us-east-1` e `us-west-2`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift.us-east-1.amazonaws.com",
          "redshift.us-west-2.amazonaws.com"
        ]
      }
    }
  ]
}
```

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

6. Scegliere Update Trust Policy (Aggiorna policy di trust).

## Concatenazione di ruoli IAM in Amazon Redshift

Quando associ un ruolo al cluster, quest'ultimo può assumere quel ruolo per accedere ad Amazon S3, Amazon Athena AWS Glue AWS Lambda e per tuo conto. Se un ruolo collegato al cluster non ha accesso alle risorse necessarie, è possibile concatenare un altro ruolo, possibilmente appartenente a un altro account. Il cluster quindi può assumere temporaneamente il ruolo concatenato per accedere ai dati. Concatenando i ruoli è anche possibile concedere l'accesso a più account. Ogni ruolo nella catena assume il ruolo successivo nella catena, fino a quando il cluster non assume il ruolo alla fine della catena. Il numero massimo di ruoli IAM che è possibile associare è soggetto a una quota. Per ulteriori informazioni, consulta la quota «Cluster IAM roles for Amazon Redshift to access other AWS services» in [Quote per gli oggetti Amazon Redshift](#)

Ad esempio, supponiamo che l'azienda A desideri accedere ai dati in un bucket Amazon S3 appartenente all'azienda B. La società A AWS crei un ruolo di servizio RoleA denominato per Amazon Redshift e lo alleggi al proprio cluster. L'Azienda B crea un ruolo denominato RoleB autorizzato ad accedere ai dati nel bucket dell'Azienda B. Per accedere ai dati nel bucket dell'Azienda B, l'Azienda A esegue un comando COPY con un parametro `iam_role` che concatena RoleA e RoleB. Per l'intera durata dell'operazione COPY, RoleA assume temporaneamente RoleB per accedere al bucket Amazon S3.

Per concatenare i ruoli, stabilisci una relazione di trust tra di essi. Un ruolo che assume un altro ruolo (ad esempio, RoleA) deve avere una policy di autorizzazioni che gli permette di assumere il ruolo concatenato successivo (ad esempio, RoleB). A sua volta, il ruolo che passa le autorizzazioni (RoleB) deve avere una policy di trust che gli permette di passare le autorizzazioni al ruolo concatenato precedente (RoleA). Per ulteriori informazioni, consultare [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

Il primo ruolo nella catena deve essere un ruolo collegato al cluster. Il primo ruolo e ogni ruolo successivo che assume il ruolo seguente nella catena devono avere una policy che include un'istruzione specifica. Questa istruzione ha l'effetto Allow sull'operazione `sts:AssumeRole` e l'Amazon Resource Name (ARN) del ruolo successivo in un elemento `Resource`. Nell'esempio,

RoleA ha la policy di autorizzazione seguente che gli permette di assumere RoleB, di proprietà dell'account AWS 210987654321.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1487639602000",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ],
      "Resource": "arn:aws:iam::210987654321:role/RoleB"
    }
  ]
}
```

Un ruolo che passa a un altro ruolo deve stabilire una relazione di fiducia con il ruolo che assume il ruolo o con l'account che possiede il AWS ruolo. Nell'esempio, RoleB ha la policy di trust seguente per stabilire una relazione di trust con RoleA.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": "arn:aws:iam::role/RoleA"
      }
    }
  ]
}
```

La seguente politica di fiducia stabilisce una relazione di fiducia con il proprietario dell'account RoleA. AWS 123456789012

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

```

    "Action": "sts:AssumeRole",
    "Principal": {
      "AWS": "arn:aws:iam::123456789012:root"
    }
  }
]
}

```

### Note

Per limitare l'autorizzazione del concatenamento dei ruoli a utenti specifici, puoi definire una condizione. Per ulteriori informazioni, consulta [Limitazione dell'accesso a ruoli IAM](#).

Quando esegui un comando UNLOAD, COPY, CREATE EXTERNAL FUNCTION o CREATE EXTERNAL SCHEMA, i ruoli vengono concatenati includendo un elenco di ARN di ruoli separati da virgole nel parametro `iam_role`. Di seguito è illustrata la sintassi per la concatenazione di ruoli nel parametro `iam_role`.

```

unload ('select * from venue limit 10')
to 's3://acmedata/redshift/venue_pipe_'
IAM_ROLE 'arn:aws:iam::<aws-account-id-1>:role/<role-name-1>[,arn:aws:iam::<aws-
account-id-2>:role/<role-name-2>][,...]';

```

### Note

L'intera catena di ruoli è racchiusa tra virgolette singole e non deve contenere spazi.

Negli esempi seguenti, RoleA è collegato al cluster che appartiene all'account AWS 123456789012. RoleB, che appartiene all'account 210987654321, dispone dell'autorizzazione per accedere al bucket denominato `s3://companyb/redshift/`. L'esempio seguente concatena RoleA e RoleB per eseguire il comando UNLOAD per scaricare i dati nel bucket `s3://companyb/redshift/`.

```

unload ('select * from venue limit 10')
to 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';

```

L'esempio seguente usa il comando COPY per caricare i dati scaricati nell'esempio precedente.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Nell'esempio seguente CREATE EXTERNAL SCHEMA usa ruoli concatenati per assumere il ruolo RoleB.

```
create external schema spectrumexample from data catalog
database 'exampledb' region 'us-west-2'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

Nell'esempio seguente CREATE EXTERNAL FUNCTION usa ruoli concatenati per assumere il ruolo RoleB.

```
create external function lambda_example(varchar)
returns varchar
volatile
lambda 'exampleLambdaFunction'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

## Informazioni aggiuntive

Per ulteriori informazioni, consultare anche [Autorizzazione di operazioni COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA utilizzando ruoli IAM](#).

## Autorizzazione di operazioni COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA utilizzando ruoli IAM

Puoi usare il comando [COPY](#) per caricare (o importare) i dati in Amazon Redshift e il comando [UNLOAD](#) per scaricare (o esportare) i dati da Amazon Redshift. È possibile utilizzare il comando CREATE EXTERNAL FUNCTION per creare funzioni definite dall'utente che richiamano funzioni da AWS Lambda

Quando usi Amazon Redshift Spectrum, viene utilizzato il comando [CREATE EXTERNAL SCHEMA](#) per specificare la posizione di un bucket Amazon S3 contenente i dati. Quando si eseguono i comandi COPY, UNLOAD o CREATE EXTERNAL SCHEMA vengono fornite le credenziali di sicurezza. Tali credenziali autorizzano il cluster Amazon Redshift a leggere o scrivere dati da e verso la destinazione obiettivo, come ad esempio un bucket Amazon S3.

Quando si esegue `CREATE EXTERNAL FUNCTION`, si forniscono le credenziali di sicurezza utilizzando il parametro del ruolo IAM. Queste credenziali autorizzano il tuo cluster Amazon Redshift a richiamare funzioni Lambda. AWS Lambda Il metodo preferito per fornire le credenziali di sicurezza consiste nello specificare un ruolo (IAM). AWS Identity and Access Management Per i comandi `COPY` e `UNLOAD`, puoi fornire le credenziali temporanee. Per informazioni su come creare un ruolo IAM, consultare [Autorizzazione di Amazon Redshift ad accedere ad AWS altri servizi per tuo conto](#).

Gli utenti necessitano dell'accesso programmatico se desiderano interagire con l' AWS esterno di. AWS Management Console Il modo per concedere l'accesso programmatico dipende dal tipo di utente che accede. AWS

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporanee e per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>Per la AWS CLI, consulta <a href="#">Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'utente</a>. AWS Command Line Interface</li> <li>Per AWS SDK, strumenti e AWS API, consulta <a href="#">l'autenticazione IAM Identity Center</a> nella Guida di riferimento agli AWS SDK e agli strumenti.</li> </ul>
IAM	Utilizza credenziali temporanee e per firmare le richieste programmatiche agli SDK o alle API AWS CLI. AWS AWS	Segui le istruzioni in <a href="#">Uso delle credenziali temporanee con AWS risorse</a> nella Guida per l'utente IAM.

Quale utente necessita dell'accesso programmatico?	Per	Come
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare le richieste programmatiche agli AWS CLI AWS SDK o alle API. AWS	<p>Segui le istruzioni per l'interfaccia che desideri utilizzare.</p> <ul style="list-style-type: none"> <li>• Per la AWS CLI, consulta <a href="#">Autenticazione tramite credenziali utente IAM nella Guida per l'utente.AWS Command Line Interface</a></li> <li>• Per gli AWS SDK e gli strumenti, consulta <a href="#">Autenticazione tramite credenziali a lungo termine</a> nella Guida di riferimento agli SDK e agli AWS strumenti.</li> <li>• Per le AWS API, consulta <a href="#">Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente IAM.</a></li> </ul>

Le fasi per l'uso di un ruolo IAM sono le seguenti:

- Crea un ruolo IAM da utilizzare con il cluster Amazon Redshift.
- Associazione del ruolo IAM al cluster.
- Includi l'ARN del ruolo IAM nella chiamata al comando COPY, UNLOAD, CREATE EXTERNAL SCHEMA o CREATE EXTERNAL FUNCTION.

In questa sezione viene descritto come associare un ruolo IAM a un cluster Amazon Redshift.

## Associazione di ruoli IAM ai cluster

Dopo aver creato un ruolo IAM che autorizza Amazon Redshift ad accedere ad altri servizi AWS per tuo conto, è necessario associare il ruolo a un cluster Amazon Redshift. È necessario eseguire questa azione prima di poter utilizzare il ruolo per caricare o scaricare i dati.

### Autorizzazioni necessarie per associare un ruolo IAM a un cluster

Per associare un ruolo IAM a un cluster, un utente deve avere l'autorizzazione `iam:PassRole` per il ruolo IAM. Questa autorizzazione permette a un amministratore di limitare i ruoli IAM che un utente può associare ai cluster Amazon Redshift. Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

L'esempio seguente illustra una policy IAM che può essere collegata a un utente, consentendogli di eseguire le operazioni seguenti:

- Ottieni i dettagli per tutti i cluster Amazon Redshift di proprietà dell'account dell'utente.
- Associa uno dei tre ruoli IAM a uno dei due cluster Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "redshift:DescribeClusters",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "redshift:ModifyClusterIamRoles",
        "redshift:CreateCluster"
      ],
      "Resource": [
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-cluster",
        "arn:aws:redshift:us-east-1:123456789012:cluster:my-second-redshift-
cluster"
      ]
    }
  ],
  {
```

```
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::123456789012:role/MyRedshiftRole",
        "arn:aws:iam::123456789012:role/SecondRedshiftRole",
        "arn:aws:iam::123456789012:role/ThirdRedshiftRole"
    ]
  }
]
```

Una volta acquisite le autorizzazioni appropriate, l'utente può associare un ruolo IAM a un cluster Amazon Redshift. Il ruolo IAM è quindi pronto per l'uso con i comandi COPY o UNLOAD o con altri comandi Amazon Redshift.

Per ulteriori informazioni sulle policy IAM, consultare [Panoramica delle policy IAM](#) nella Guida per l'utente IAM.

#### Gestione dell'associazione di un ruolo IAM a un cluster

Durante la creazione del cluster, è possibile associare un ruolo IAM a un cluster Amazon Redshift. Oppure è possibile modificare un cluster esistente e aggiungere o rimuovere una o più associazioni di ruoli IAM.

Ricorda quanto segue:

- Il numero massimo di ruoli IAM che è possibile associare è soggetto a una quota.
- Un ruolo IAM può essere associato a più cluster Amazon Redshift.
- Un ruolo IAM può essere associato a un cluster Amazon Redshift solo se sia il ruolo IAM che il cluster sono di proprietà dello stesso AWS account.

#### Uso della console per gestire le associazioni dei ruoli IAM

Puoi gestire le associazioni dei ruoli IAM per un cluster con la console usando la procedura seguente.

Per gestire le associazioni dei ruoli IAM

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster da aggiornare.

3. Alla voce **Actions (Operazioni)**, scegli **Manage IAM roles (Gestisci ruoli IAM)** per visualizzare l'elenco corrente dei ruoli IAM associati al cluster.
4. Nella pagina **Manage IAM roles (Gestisci ruoli IAM)**, scegli i ruoli IAM disponibili da aggiungere e quindi scegli **Add IAM role (Aggiungi ruolo IAM)**.
5. Scegli **Save (Salva)** per salvare le modifiche.

### Utilizzo di AWS CLI per gestire le associazioni di ruoli IAM

È possibile gestire le associazioni di ruoli IAM per un cluster AWS CLI utilizzando i seguenti approcci.

#### Associazione di un ruolo IAM a un cluster utilizzando il AWS CLI

Per associare un ruolo IAM a un cluster al momento della creazione del cluster, specifica l'Amazon Resource Name (ARN) del ruolo IAM per il parametro `--iam-role-arns` del comando `create-cluster`. Il numero massimo di ruoli IAM che è possibile aggiungere quando si chiama il comando `create-cluster` è soggetto a una quota.

L'associazione e la dissociazione di ruoli IAM ai cluster Amazon Redshift sono processi asincroni. Per ottenere lo stato di tutte le associazioni ai cluster dei ruoli IAM, chiama il comando `describe-clusters`.

L'esempio seguente associa due ruoli IAM al cluster appena creato denominato `my-redshift-cluster`.

```
aws redshift create-cluster \  
  --cluster-identifier "my-redshift-cluster" \  
  --node-type "ra3.4xlarge" \  
  --number-of-nodes 16 \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \  
                 "arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Per associare un ruolo IAM a un cluster Amazon Redshift esistente, specifica l'Amazon Resource Name (ARN) del ruolo IAM per il parametro `--add-iam-roles` del comando `modify-cluster-iam-roles`. Il numero massimo di ruoli IAM che è possibile aggiungere quando si chiama il comando `modify-cluster-iam-roles` è soggetto a una quota.

L'esempio seguente associa un ruolo IAM a un cluster esistente denominato `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier "my-redshift-cluster" \  
  --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

## Dissociazione di un ruolo IAM da un cluster utilizzando il AWS CLI

Per eliminare l'associazione di un ruolo IAM da un cluster, specifica l'ARN del ruolo IAM per il parametro `--remove-iam-roles` del comando `modify-cluster-iam-roles`. `modify-cluster-iam-roles` Il numero massimo di ruoli IAM che è possibile rimuovere quando si chiama il comando `modify-cluster-iam-roles` è soggetto a una quota.

L'esempio seguente rimuove l'associazione per un ruolo IAM per l'123456789012 AWS account da un cluster denominato `my-redshift-cluster`

```
aws redshift modify-cluster-iam-roles \  
  --cluster-identifier "my-redshift-cluster" \  
  --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

## Elenco delle associazioni di ruoli IAM per un cluster utilizzando il AWS CLI

Per elencare tutti i ruoli IAM associati a un cluster Amazon Redshift con lo stato dell'associazione del ruolo IAM, chiama il comando `describe-clusters`. L'ARN per ogni ruolo IAM associato al cluster viene restituito nell'elenco `IamRoles`, come illustrato nell'output di esempio seguente.

I ruoli che sono stati associati al cluster hanno uno stato `in-sync`. I ruoli di cui è in corso l'associazione al cluster hanno uno stato `adding`. I ruoli di cui è in corso l'eliminazione dell'associazione al cluster hanno uno stato `removing`.

```
{  
  "Clusters": [  
    {  
      "ClusterIdentifier": "my-redshift-cluster",  
      "NodeType": "ra3.4xlarge",  
      "NumberOfNodes": 16,  
      "IamRoles": [  
        {  
          "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",  
          "IamRoleApplyStatus": "in-sync"  
        }  
      ],  
    },  
  ],  
}
```

```
        {
            "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
            "IamRoleApplyStatus": "in-sync"
        }
    ],
    ...
},
{
    "ClusterIdentifier": "my-second-redshift-cluster",
    "NodeType": "ra3.4xlarge",
    "NumberOfNodes": 10,
    "IamRoles": [
        {
            "IamRoleArn": "arn:aws:iam::123456789012:role/MyRedshiftRole",
            "IamRoleApplyStatus": "in-sync"
        },
        {
            "IamRoleArn": "arn:aws:iam::123456789012:role/SecondRedshiftRole",
            "IamRoleApplyStatus": "in-sync"
        },
        {
            "IamRoleArn": "arn:aws:iam::123456789012:role/ThirdRedshiftRole",
            "IamRoleApplyStatus": "in-sync"
        }
    ],
    ...
}
]
```

Per ulteriori informazioni sull'utilizzo di AWS CLI, consulta la [Guida AWS CLI per l'utente](#).

## Creazione di un ruolo IAM come predefinito per Amazon Redshift

Quando crei ruoli IAM tramite la console Redshift, Amazon Redshift crea i ruoli nel Account AWS tuo sistema a livello di codice e ad essi AWS allega automaticamente le policy gestite esistenti. Questo approccio significa che puoi rimanere all'interno della console Redshift senza dover passare alla console IAM per la creazione di ruoli. Per un controllo più dettagliato delle autorizzazioni per un ruolo IAM esistente creato nella console Amazon Redshift, puoi allegare una policy gestita personalizzata al ruolo IAM.

## Panoramica dei ruoli IAM creati nella console

Quando utilizzi la console Amazon Redshift per creare ruoli IAM, Amazon Redshift tiene traccia di tutti i ruoli IAM creati tramite la console. Amazon Redshift preseleziona il ruolo IAM predefinito più recente per la creazione di tutti i nuovi cluster e il ripristino dei cluster dalle istantanee.

È possibile creare un ruolo IAM attraverso la console che ha una policy con autorizzazioni per eseguire comandi SQL. Questi comandi includono COPIA, SCARICARE, CREA FUNZIONE ESTERNA, CREA TABELLA ESTERNA, CREA SCHEMA ESTERNO, CREA MODELLO o CREA LIBRERIA. Facoltativamente, puoi ottenere un controllo più dettagliato dell'accesso dell'utente alle tue risorse AWS creando e collegando policy personalizzate al ruolo IAM.

Quando si crea un ruolo IAM e lo si imposta come predefinito per il cluster utilizzando la console, non è necessario fornire l'Amazon Resource Name (ARN) del ruolo IAM per eseguire autenticazione e autorizzazione.

### Utilizzo del ruolo IAM creato nella console

Il ruolo IAM creato tramite la console per il cluster ha la policy gestita da `AmazonRedshiftAllCommandsFullAccess` allegata automaticamente. Questo ruolo IAM consente ad Amazon Redshift di copiare, scaricare, interrogare e analizzare i dati alla ricerca di AWS risorse nel tuo account IAM. La policy gestita fornisce l'accesso alle operazioni [COPY](#) (COPIA), [UNLOAD](#) (SCARICA), [CREATE EXTERNAL FUNCTION](#) (CREAZIONE FUNZIONE ESTERNA), [CREATE EXTERNAL SCHEMA](#) (CREAZIONE SCHEMA ESTERNO), [CREATE MODEL](#) (CREAZIONE MODELLO) e [CREATE LIBRARY](#) (CREAZIONE LIBRERIA). La policy concede inoltre le autorizzazioni per eseguire istruzioni SELECT per AWS servizi correlati, come Amazon S3, Amazon Logs, CloudWatch SageMaker Amazon e. AWS Glue

I comandi CREAZIONE FUNZIONE ESTERNA, CREAZIONE SCHEMA ESTERNO, CREAZIONE MODELLO e CREAZIONE LIBRERIA hanno la parola chiave default `Per` questa parola chiave per questi comandi, Amazon Redshift usa il ruolo IAM che è impostato come predefinito e associato al cluster quando il comando viene eseguito. È anche possibile eseguire il [RUOLO\\_IAM\\_PREDEFINITO](#) per controllare il ruolo IAM predefinito corrente associato al cluster.

Per controllare i privilegi di accesso del ruolo IAM creato e impostato come predefinito per il tuo cluster Redshift, usa il privilegio ASSUMEROLE. Questo controllo di accesso si applica agli utenti e ai gruppi del database quando eseguono comandi come quelli elencati in precedenza. Dopo aver concesso il privilegio ASSUMEROLE a un utente o a un gruppo per il ruolo IAM, l'utente o il gruppo può assumere tale ruolo durante l'esecuzione dei comandi. Il privilegio ASSUMEROLE consente di concedere l'accesso ai comandi appropriati in base alle esigenze.

Utilizzando la console Amazon Redshift, puoi effettuare le seguenti operazioni:

- [Creazione di un ruolo IAM come predefinito](#)
- [Rimozione di ruoli IAM dal cluster](#)
- [Associazione di ruoli IAM al cluster](#)
- [Impostazione di un ruolo IAM come predefinito](#)
- [Rendere un ruolo IAM non più predefinito per il cluster](#)

### Autorizzazioni della politica gestita AmazonRedshiftAllCommandsFullAccess

L'esempio seguente mostra le autorizzazioni nella policy gestita da AmazonRedshiftAllCommandsFullAccess che consentono determinate operazioni per il ruolo IAM impostato come predefinito per il cluster. Il ruolo IAM con policy di autorizzazione allegati autorizza ciò che un utente o un gruppo può e non può fare. Date queste autorizzazioni, puoi eseguire il comando COPIA da Amazon S3, eseguire SCARICA e utilizzare il comando CREAZIONE MODELLO.

```
{
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:GetBucketAcl",
    "s3:GetBucketCors",
    "s3:GetEncryptionConfiguration",
    "s3:GetBucketLocation",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:ListMultipartUploadParts",
    "s3:ListBucketMultipartUploads",
    "s3:PutObject",
    "s3:PutBucketAcl",
    "s3:PutBucketCors",
    "s3:DeleteObject",
    "s3:AbortMultipartUpload",
    "s3:CreateBucket"
  ],
  "Resource": [
    "arn:aws:s3:::redshift-downloads",
    "arn:aws:s3:::redshift-downloads/*",
    "arn:aws:s3::*redshift*",
  ]
}
```

```

        "arn:aws:s3:::*redshift*/*"
    ]
}

```

L'esempio seguente mostra le autorizzazioni nella policy gestita da `AmazonRedshiftAllCommandsFullAccess` che consentono determinate operazioni per il ruolo IAM impostato come predefinito per il cluster. Il ruolo IAM con policy di autorizzazione allegati autorizza ciò che un utente o un gruppo può e non può fare. In base alle seguenti autorizzazioni, è possibile eseguire il comando **CREAZIONE FUNZIONE ESTERNA**.

```

{
  "Action": [
    "lambda:InvokeFunction"
  ],
  "Resource": "arn:aws:lambda:*:*:function:*redshift*"
}

```

L'esempio seguente mostra le autorizzazioni nella policy gestita da `AmazonRedshiftAllCommandsFullAccess` che consentono determinate operazioni per il ruolo IAM impostato come predefinito per il cluster. Il ruolo IAM con policy di autorizzazione allegati autorizza ciò che un utente o un gruppo può e non può fare. In base alle seguenti autorizzazioni, è possibile eseguire i comandi **CREAZIONE SCHEMA ESTERNO** e **CREAZIONE TABELLA ESTERNA** necessari per Amazon Redshift Spectrum.

```

{
  "Effect": "Allow",
  "Action": [
    "glue:CreateDatabase",
    "glue>DeleteDatabase",
    "glue:GetDatabase",
    "glue:GetDatabases",
    "glue:UpdateDatabase",
    "glue:CreateTable",
    "glue>DeleteTable",
    "glue:BatchDeleteTable",
    "glue:UpdateTable",
    "glue:GetTable",
    "glue:GetTables",
    "glue:BatchCreatePartition",
    "glue:CreatePartition",
    "glue>DeletePartition",

```

```

        "glue:BatchDeletePartition",
        "glue:UpdatePartition",
        "glue:GetPartition",
        "glue:GetPartitions",
        "glue:BatchGetPartition"
    ],
    "Resource": [
        "arn:aws:glue:*:*:table/*redshift*/*",
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/*redshift*"
    ]
}

```

L'esempio seguente mostra le autorizzazioni nella policy gestita da `AmazonRedshiftAllCommandsFullAccess` che consentono determinate operazioni per il ruolo IAM impostato come predefinito per il cluster. Il ruolo IAM con policy di autorizzazione allegati autorizza ciò che un utente o un gruppo può e non può fare. In base alle seguenti autorizzazioni, è possibile eseguire il comando `CREAZIONE SCHEMA ESTERNO` utilizzando query federate.

```

{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetResourcePolicy",
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret",
        "secretsmanager:ListSecretVersionIds"
    ],
    "Resource": [
        "arn:aws:secretsmanager:*:*:secret:*Redshift*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetRandomPassword",
        "secretsmanager:ListSecrets"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "secretsmanager:ResourceTag/Redshift": "true"
        }
    }
}

```

```
},
```

## Gestione dei ruoli IAM creati per un cluster tramite la console

Per creare, modificare e rimuovere i ruoli IAM creati dalla console di Amazon Redshift, utilizzare la sezione Cluster nella console.

### Creazione di un ruolo IAM come predefinito

Nella console, puoi creare un ruolo IAM per il tuo cluster che ha la policy `AmazonRedshiftAllCommandsFullAccess` automaticamente allegata. Ciò consente ad Amazon Redshift di copiare, scaricare, analizzare i dati ed eseguire query su di essi dalle risorse Amazon nel tuo account IAM.

Può esserci un solo set di ruoli IAM predefinito per un cluster. Se si crea un altro ruolo IAM come predefinito del cluster quando un ruolo IAM esistente è attualmente assegnato come predefinito, il nuovo ruolo IAM sostituisce l'altro come predefinito.

Per creare un nuovo cluster e un set di ruoli IAM come predefinito per il nuovo cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Per creare un cluster, scegli Create cluster (Crea cluster).
4. Segui le istruzioni sulla pagina della console per inserire le proprietà della Cluster configuration (Configurazione del cluster). Per ulteriori informazioni su questa fase, consultare [Creazione di un cluster](#).
5. (Facoltativo) Scegliere Caricare dati campione per caricare il set di dati di esempio nel cluster Amazon Redshift per iniziare a utilizzare l'editor di query per interrogare i dati.

Se è abilitata la protezione di un firewall, è necessario specificare una porta del database aperta che accetti connessioni in entrata.

6. Segui le istruzioni sulla pagina della console per inserire le proprietà delle Database configurations (Configurazioni del database).
7. In Autorizzazioni cluster, per Gestisci i ruoli IAM, scegliere Creazione di ruolo IAM.
8. Specificare un bucket Amazon S3 per l'accesso al ruolo IAM scegliendo uno dei seguenti metodi:

- Scegliere Nessun bucket Amazon S3 aggiuntivo per creare il ruolo IAM senza specificare bucket Amazon S3 specifici.
  - Scegliere Qualsiasi bucket Amazon S3 per consentire agli utenti che hanno accesso al cluster Amazon Redshift di accedere anche a qualsiasi bucket Amazon S3 e ai relativi contenuti nel tuo Account AWS.
  - Scegliere Bucket Amazon S3 specifico per specificare uno o più bucket Amazon S3 a cui il ruolo IAM creato ha l'autorizzazione per accedere. Quindi scegliere uno o più bucket Amazon S3 dalla tabella.
9. Scegliere Creazione di ruolo IAM come predefinito. Amazon Redshift crea e imposta automaticamente il ruolo IAM come predefinito per il cluster.
  10. Per creare il cluster, scegli Create cluster (Crea cluster). Potrebbero essere necessari diversi minuti prima che il cluster sia pronto per l'utilizzo.

### Rimozione di ruoli IAM dal cluster

È possibile rimuovere uno o più ruoli IAM dal cluster.

Per rimuovere ruoli IAM dal cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Selezionare il nome del cluster da cui desideri rimuovere il ruolo IAM.
4. In Autorizzazioni cluster, scegliere uno o più ruoli IAM che si desidera rimuovere dal cluster.
5. Da Gestisci i ruoli IAM, scegliere Rimuovere i ruoli IAM.

### Associazione di ruoli IAM al cluster

È possibile associare uno o più ruoli IAM al cluster.

Per associare ruoli IAM al cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione, scegliere Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegliere il cluster a cui si desidera associare il ruolo IAM..
4. In Autorizzazioni cluster, scegliere uno o più ruoli IAM che si desidera associare al cluster.
5. Da Gestisci i ruoli IAM, scegliere Associare ruoli IAM.
6. Scegliere uno o più ruoli IAM da associare al cluster.
7. Quindi scegliere Associa ruoli IAM.

### Impostazione di un ruolo IAM come predefinito

È possibile impostare un ruolo IAM come predefinito per il cluster.

Per rendere un ruolo IAM come predefinito per il cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegliere il cluster per il quale si desidera impostare un ruolo IAM predefinito.
4. In Autorizzazioni cluster, da Ruoli IAM associati, scegliere un ruolo IAM che si desidera rendere come predefinito per il cluster.
5. In Impostazione predefinita, scegliere Rendi predefinito.
6. Quando richiesto, scegliere Impostazione predefinita per confermare l'impostazione predefinita del ruolo IAM specificato.

### Rendere un ruolo IAM non più predefinito per il cluster

Puoi rendere un ruolo IAM non più predefinito per il tuo cluster.

Per cancellare un ruolo IAM come predefinito per il tuo cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione, scegliere Clusters (Cluster). Regione AWS Sono elencati i cluster del tuo account nella versione corrente. Nelle colonne dell'elenco è visualizzato un sottoinsieme delle proprietà di ciascun cluster.
3. Scegliere il cluster a cui si desidera associare il ruolo IAM..
4. In Autorizzazioni cluster, da Ruoli IAM associati, scegliere il ruolo IAM predefinito.
5. In Impostazione predefinita, scegliere Annulla predefinito.
6. Quando richiesto, scegliere Annulla predefinito per confermare l'impostazione predefinita del ruolo IAM specificato.

## Gestione dei ruoli IAM creati nel cluster utilizzando il AWS CLI

Puoi gestire dei ruoli IAM creati per un cluster tramite la AWS CLI.

Per creare un cluster Amazon Redshift con un set di ruoli IAM come predefinito

Per creare un cluster Amazon Redshift con un ruolo IAM impostato come predefinito per il cluster, usa il `aws redshift create-cluster` AWS CLI comando.

Il AWS CLI comando seguente crea un cluster Amazon Redshift e il ruolo IAM denominato `myrole1`. Il AWS CLI comando imposta anche `myrole1` come impostazione predefinita per il cluster.

```
aws redshift create-cluster \  
  --node-type dc2.large \  
  --number-of-nodes 2 \  
  --master-username adminuser \  
  --master-user-password TopSecret1 \  
  --cluster-identifier mycluster \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole1'  
'arn:aws:iam::012345678910:role/myrole2' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

Il seguente frammento è un esempio della risposta.

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
```

```

    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "ApplyStatus": "adding"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "ApplyStatus": "adding"
      }
    ]
    ...
  }
}

```

Per aggiungere uno o più ruoli IAM a un cluster Amazon Redshift

Per aggiungere uno o più ruoli IAM associati al cluster, usa il comando `aws redshift modify-cluster-iam-roles` AWS CLI

Il AWS CLI comando seguente aggiunge `myrole3` e `myrole4` al cluster.

```

aws redshift modify-cluster-iam-roles \
  --cluster-identifier mycluster \
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
'arn:aws:iam::012345678910:role/myrole4'

```

Il seguente frammento è un esempio della risposta.

```

{
  "Cluster": {
    "ClusterIdentifier": "mycluster",
    "NodeType": "dc2.large",
    "MasterUsername": "adminuser",
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "ApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "ApplyStatus": "in-sync"
      }
    ]
  }
}

```

```

    },
    {
      "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
      "ApplyStatus": "adding"
    },
    {
      "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
      "ApplyStatus": "adding"
    }
  ],
  ...
}

```

Per rimuovere uno o più ruoli IAM da un cluster Amazon Redshift

Per rimuovere uno o più ruoli IAM associati al cluster, usa il `aws redshift modify-cluster-iam-roles` AWS CLI comando.

Il AWS CLI comando seguente rimuove `myrole3` e `myrole4` dal cluster.

```

aws redshift modify-cluster-iam-roles \
  --cluster-identifier mycluster \
  --remove-iam-roles 'arn:aws:iam::012345678910:role/myrole3'
  'arn:aws:iam::012345678910:role/myrole4'

```

Il seguente frammento è un esempio della risposta.

```

{
  "Cluster": {
    "ClusterIdentifier": "mycluster",
    "NodeType": "dc2.large",
    "MasterUsername": "adminuser",
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "ApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "ApplyStatus": "in-sync"
      }
    ]
  }
}

```

```

    },
    {
      "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
      "ApplyStatus": "removing"
    },
    {
      "IamRoleArn": "arn:aws:iam::012345678910:role/myrole4",
      "ApplyStatus": "removing"
    }
  ],
  ...
}

```

Per impostare un ruolo IAM associato come predefinito per il cluster

Per impostare un ruolo IAM associato come predefinito per il cluster, usa il `aws redshift modify-cluster-iam-roles` AWS CLI comando.

Il AWS CLI comando seguente viene impostato `myrole2` come predefinito per il cluster.

```

aws redshift modify-cluster-iam-roles \
  --cluster-identifier mycluster \
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole2'

```

Il seguente frammento è un esempio della risposta.

```

{
  "Cluster": {
    "ClusterIdentifier": "mycluster",
    "NodeType": "dc2.large",
    "MasterUsername": "adminuser",
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "ApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "ApplyStatus": "in-sync"
      }
    ]
  }
}

```

```

    ],
    ...
  }
}

```

Per impostare un ruolo IAM non associato come predefinito per il cluster

Per impostare un ruolo IAM non associato come predefinito per il cluster, usa il `aws redshift modify-cluster-iam-roles` AWS CLI comando.

Il AWS CLI comando seguente aggiunge `myrole2` al cluster Amazon Redshift e lo imposta come predefinito per il cluster.

```

aws redshift modify-cluster-iam-roles \
  --cluster-identifier mycluster \
  --add-iam-roles 'arn:aws:iam::012345678910:role/myrole3' \
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole3'

```

Il seguente frammento è un esempio della risposta.

```

{
  "Cluster": {
    "ClusterIdentifier": "mycluster",
    "NodeType": "dc2.large",
    "MasterUsername": "adminuser",
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
    "IamRoles": [
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",
        "ApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",
        "ApplyStatus": "in-sync"
      },
      {
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole3",
        "ApplyStatus": "adding"
      }
    ],
    ...
  }
}

```

```
}
```

Per ripristinare un cluster da uno snapshot e impostare un ruolo IAM come predefinito

Quando si ripristina il cluster da uno snapshot, è possibile associare un ruolo IAM esistente o crearne uno nuovo e impostarlo come predefinito per il cluster.

Per ripristinare un cluster Amazon Redshift da uno snapshot e impostare un ruolo IAM come cluster predefinito, usa il comando `aws redshift restore-from-cluster-snapshot` AWS CLI

Il AWS CLI comando seguente ripristina il cluster da uno snapshot e lo imposta `myrole2` come predefinito per il cluster.

```
aws redshift restore-from-cluster-snapshot \  
  --cluster-identifier mycluster-clone \  
  --snapshot-identifier my-snapshot-id \  
  --iam-roles 'arn:aws:iam::012345678910:role/myrole1' \  
  'arn:aws:iam::012345678910:role/myrole2' \  
  --default-iam-role-arn 'arn:aws:iam::012345678910:role/myrole1'
```

Il seguente frammento è un esempio della risposta.

```
{  
  "Cluster": {  
    "ClusterIdentifier": "mycluster-clone",  
    "NodeType": "dc2.large",  
    "MasterUsername": "adminuser",  
    "DefaultIamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
    "IamRoles": [  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole1",  
        "ApplyStatus": "adding"  
      },  
      {  
        "IamRoleArn": "arn:aws:iam::012345678910:role/myrole2",  
        "ApplyStatus": "adding"  
      }  
    ],  
    ...  
  }  
}
```

## Utilizzo di un'identità federata per gestire l'accesso di Amazon Redshift alle risorse locali e alle tabelle esterne di Amazon Redshift Spectrum

L'utilizzo della federazione delle identità AWS con le credenziali fornite da `GetDatabaseCredentials` può semplificare l'autorizzazione e l'accesso ai dati locali e ai dati esterni. Attualmente, per consentire agli utenti di accedere a dati esterni che risiedono in Amazon S3, è necessario creare un ruolo IAM con le autorizzazioni definite in una policy di autorizzazioni. Quindi, gli utenti con il ruolo associato possono accedere ai dati esterni. Funziona, ma se si desidera fornire regole granulari, ad esempio rendere non disponibili colonne specifiche per un determinato utente, potrebbe essere necessario eseguire una configurazione aggiuntiva sullo schema esterno. In questo argomento, mostriamo come fornire l'accesso alle risorse con la federazione delle AWS identità, anziché utilizzare un ruolo IAM specifico. La federazione delle identità, con credenziali fornite da `GetDatabaseCredentials`, può fornire l'accesso alle risorse di Redshift Spectrum tramite regole IAM granulari più facili da specificare AWS Glue e modificare. In questo modo è più facile applicare un accesso conforme alle regole aziendali.

I vantaggi dell'utilizzo di credenziali federate sono i seguenti:

- Non è necessario gestire i ruoli IAM collegati al cluster per Redshift Spectrum.
- Gli amministratori dei cluster possono creare uno schema esterno accessibile ai consumatori con diversi contesti IAM. Ciò è utile, ad esempio, per eseguire il filtraggio delle colonne su una tabella, in cui utenti diversi eseguono query sullo stesso schema esterno e ottengono campi diversi nei record restituiti.
- È possibile eseguire query su Amazon Redshift utilizzando un utente con autorizzazioni IAM, anziché solo con un ruolo.

### Preparazione di un'identità per l'accesso con un'identità federata

Prima di accedere con un'identità federata, è necessario eseguire diverse fasi preliminari. Queste istruzioni presuppongono che si disponga di uno schema esterno Redshift Spectrum esistente che fa riferimento a un file di dati archiviato in un bucket Amazon S3 e che il bucket si trovi nello stesso account del proprio cluster Amazon Redshift o del data warehouse di Amazon Redshift Serverless.

1. Creazione di un'identità IAM. Può trattarsi di un utente o di un ruolo IAM. Utilizzare qualsiasi nome supportato da IAM.
2. Collegare le policy di autorizzazione all'identità. Specificare uno dei seguenti:

- `redshift:GetClusterCredentialsWithIAM` (per un cluster con provisioning di Amazon Redshift)
- `redshift-serverless:GetCredentials` (per Amazon Redshift Serverless)

È possibile aggiungere autorizzazioni con l'editor delle policy, utilizzando la console IAM.

L'identità IAM necessita anche delle autorizzazioni per accedere ai dati esterni. Concedi l'accesso ad Amazon S3 aggiungendo direttamente le seguenti policy AWS gestite:

- `AmazonS3ReadOnlyAccess`
- `AWSGlueConsoleFullAccess`

L'ultima policy gestita è necessaria se utilizzi AWS Glue per preparare i tuoi dati esterni. Per ulteriori informazioni sulle fasi richieste per concedere l'accesso ad Amazon Redshift Spectrum, consulta [Creare un ruolo IAM per Amazon Redshift](#), che fa parte della guida introduttiva per Amazon Redshift e Redshift Spectrum. Illustra le fasi richieste per aggiungere le policy IAM per accedere a Redshift Spectrum.

3. Configurare il client SQL per la connessione ad Amazon Redshift. Usa il driver JDBC di Amazon Redshift e aggiungi le credenziali dell'utente alle proprietà delle credenziali dello strumento. Per questa operazione, si consiglia in client come SQL Workbench/J. Impostare le seguenti proprietà estese della connessione client:
  - `AccessKeyID`: il tuo identificatore della chiave di accesso.
  - `SecretAccessChiave`: la tua chiave di accesso segreta. (Si noti il rischio di sicurezza legato alla trasmissione della chiave segreta se non si utilizza la crittografia.)
  - `SessionToken`— Un set di credenziali temporanee per un ruolo IAM.
  - `GroupFederation`: impostare su `true` se si sta configurando l'identità federata per un cluster con provisioning. Non impostare questo parametro se si utilizza Amazon Redshift Serverless.
  - `LogLevel`— Valore intero a livello di log. Si tratta di un'opzione facoltativa.
4. Impostare l'URL sull'endpoint JDBC che si trova nella console Amazon Redshift o Amazon Redshift Serverless. Sostituire lo schema URL con `jdbc:redshift:iam:` e utilizzare questo formato:
  - Formato per un cluster con provisioning di Amazon Redshift: `jdbc:redshift:iam://<cluster_id>.<unique_suffix>.<region>.redshift.amazonaws.com:<port>/<database_name>`

Esempio: `jdbc:redshift:iam://test1.12345abcdefg.us-east-1.redshift.amazonaws.com:5439/dev`

- Formato per Amazon Redshift Serverless: `jdbc:redshift:iam://<workgroup-name>.<account-number>.<aws-region>.redshift-serverless.amazonaws.com:5439:<port>/<database_name>`

Esempio: `jdbc:redshift:iam://default.123456789012.us-east-1.redshift-serverless.amazonaws.com:5439/dev`

Dopo la prima connessione al database, utilizzando un'identità IAM, Amazon Redshift crea automaticamente un'identità Amazon Redshift con lo stesso nome e il prefisso IAM: per un utente o IAMR: per un ruolo IAM. Le fasi rimanenti di questo argomento mostrano esempi per un utente.

Se un utente Redshift non viene creato automaticamente, puoi crearne uno eseguendo un'istruzione `CREATE USER`, utilizzando un account amministratore, specificando il nome utente nel formato `IAM:<user name>`.

5. In qualità di amministratore del cluster Amazon Redshift, concedi all'utente Redshift le autorizzazioni necessarie per accedere allo schema esterno.

```
GRANT ALL ON SCHEMA my_schema to "IAM:my_user";
```

Per concedere la possibilità all'utente Redshift di creare tabelle nello schema esterno, esso deve essere un proprietario dello schema. Per esempio:

```
ALTER SCHEMA my_schema owner to "IAM:my_user";
```

6. Per verificare la configurazione, esegui una query come utente, utilizzando il client SQL, dopo aver assegnato le autorizzazioni. Questo esempio di query recupera i dati da una tabella esterna.

```
SELECT * FROM my_schema.my_table;
```

## Guida introduttiva alla propagazione di identità e autorizzazioni su Redshift Spectrum

Per passare un'identità federata per eseguire query su tabelle esterne, impostare SESSION come valore per il parametro di query IAM\_ROLE di CREATE EXTERNAL SCHEMA. La procedura seguente mostra come configurare e utilizzare SESSION per autorizzare le query sullo schema esterno.

1. Creazione di tabelle locali e di tabelle esterne. Tabelle esterne catalogate con documenti a tal fine. AWS Glue
2. Connessione ad Amazon Redshift con la propria identità IAM. Come indicato nella sezione precedente, quando l'identità si connette ad Amazon Redshift, viene creato un utente del database Redshift. L'utente viene creato se non esisteva in precedenza. Se l'utente è nuovo, l'amministratore deve concedere le autorizzazioni per eseguire attività in Amazon Redshift, come l'esecuzione di query o la creazione di tabelle.
3. Connessione a Redshift con il proprio account amministratore. Eseguire il comando per creare uno schema esterno, utilizzando il valore SESSION.

```
create external schema spectrum_schema from data catalog
database '<my_external_database>'
region '<my_region>'
iam_role 'SESSION'
catalog_id '<my_catalog_id>;'
```

In questo caso, si noti che è impostato catalog\_id. Questa è una nuova impostazione aggiunta con la caratteristica, perché SESSION sostituisce un ruolo specifico.

In questo esempio, i valori della query simulano il modo in cui vengono visualizzati i valori reali.

```
create external schema spectrum_schema from data catalog
database 'spectrum_db'
region 'us-east-1'
iam_role 'SESSION'
catalog_id '123456789012'
```

Il catalog\_id valore in questo caso è l'ID del tuo AWS account.

4. Eseguire le query per accedere ai dati esterni, utilizzando l'identità IAM a cui ti sei connesso nella fase 2. Ad esempio:

```
select * from spectrum_schema.table1;
```

In questo caso, `table1` può essere, ad esempio, dati in formato JSON in un file in un bucket Amazon S3.

5. Se disponi già di uno schema esterno che utilizza un ruolo IAM collegato al cluster, che punta al database o schema esterno, puoi sostituire lo schema esistente e utilizzare un'identità federata come descritto in queste fasi, o crearne una nuova.

`SESSION` indica che le credenziali dell'identità federata vengono utilizzate per eseguire query sullo schema esterno. Quando si utilizza il parametro di query `SESSION`, assicurarsi di impostare `catalog_id`. È obbligatorio perché punta al catalogo dati utilizzato per lo schema. In precedenza, `catalog_id` veniva recuperato dal valore assegnato a `iam_role`. Quando si configura la propagazione dell'identità e delle autorizzazioni in questo modo, ad esempio, su Redshift Spectrum, utilizzando credenziali federate per eseguire query su uno schema esterno, non è richiesta l'autorizzazione tramite un ruolo IAM.

#### Note per l'utilizzo

Un errore di connessione comune è il seguente: `IAM error retrieving temp credentials: Unable to unmarshall exception response with the unmarshallers provided`. Questo errore è il risultato di un driver JDBC obsoleto. La versione minima del driver richiesta per l'identità federata è la 2.1.0.9. Puoi scaricare il driver JDBC da [Scarica il driver JDBC Amazon Redshift, versione 2.1](#).

#### Risorse aggiuntive

Questi collegamenti forniscono informazioni aggiuntive per la gestione degli accessi ai dati esterni.

- È comunque possibile accedere ai dati di Redshift Spectrum utilizzando un ruolo IAM. Per ulteriori informazioni, consulta [Autorizzazione di Amazon Redshift ad accedere ad AWS altri servizi per tuo conto](#).
- Quando gestisci l'accesso a tabelle esterne con AWS Lake Formation, puoi interrogarle utilizzando Redshift Spectrum con identità IAM federate. Non è più necessario gestire i ruoli IAM collegati al cluster per Redshift Spectrum con cui interrogare i dati registrati. AWS Lake Formation Per ulteriori informazioni, consulta [Using AWS Lake Formation with Amazon Redshift Spectrum](#).

# Gestione delle password di amministrazione di Amazon Redshift tramite AWS Secrets Manager

Amazon Redshift può integrarsi con AWS Secrets Manager per generare e gestire le credenziali di amministratore all'interno di un segreto crittografato. Con AWS Secrets Manager, puoi sostituire le password di amministratore con una chiamata API per recuperare programmaticamente il segreto quando è necessario. L'uso di credenziali segrete anziché a codifica fissa riduce il rischio che le credenziali vengano esposte o compromesse. [Per ulteriori informazioni in merito AWS Secrets Manager, consulta la Guida per l'utente AWS Secrets Manager](#)

Puoi specificare che Amazon Redshift gestisca la tua password di amministratore utilizzando AWS Secrets Manager quando esegui una delle seguenti operazioni:

- Creazione di un cluster con provisioning o uno spazio dei nomi serverless
- Ripristino di un cluster o uno spazio dei nomi serverless da uno snapshot

Quando specifichi che Amazon Redshift gestisce la password di amministratore in AWS Secrets Manager, Amazon Redshift genera la password e la archivia in Secrets Manager. Puoi accedere al segreto direttamente in AWS Secrets Manager per recuperare le credenziali dell'utente amministratore. Facoltativamente, puoi specificare una chiave gestita dal cliente per crittografare il segreto se devi accedere al segreto da un altro account. AWS Inoltre, puoi utilizzare la chiave KMS fornita da AWS Secrets Manager .

Amazon Redshift gestisce le impostazioni del segreto e lo ruota ogni 30 giorni per impostazione predefinita, ma puoi ruotare manualmente il segreto in qualsiasi momento. Se si elimina un cluster o uno spazio dei nomi serverless fornito che gestisce un indirizzo segreto in AWS Secrets Manager, vengono eliminati anche il segreto e i metadati associati.

Per connetterti a un cluster o a uno spazio dei nomi serverless con le credenziali gestite da segreti, puoi recuperare il segreto da AWS Secrets Manager usando la console Secrets Manager o la chiamata API `GetSecretValue` di Secrets Manager. Per ulteriori informazioni, consulta [Recupera segreti da AWS Secrets Manager](#) e [Connettiti a un database SQL con credenziali in un AWS Secrets Manager segreto nella Guida](#) per l'AWS Secrets Manager utente.

## Autorizzazioni necessarie per l'integrazione AWS Secrets Manager

Gli utenti devono disporre delle autorizzazioni necessarie per eseguire operazioni relative all' AWS Secrets Manager integrazione. Crea le policy IAM che forniscono l'autorizzazione per eseguire

operazioni API specifiche sulle risorse indicate necessarie. Quindi collega tali policy ai ruoli o ai set di autorizzazioni IAM che richiedono le autorizzazioni. Per ulteriori informazioni, consulta [Identity and Access Management in Amazon Redshift](#).

L'utente che specifica che Amazon Redshift gestisce la password AWS Secrets Manager di amministratore deve disporre delle autorizzazioni per eseguire le seguenti operazioni:

- `secretsmanager:CreateSecret`
- `secretsmanager:RotateSecret`
- `secretsmanager:DescribeSecret`
- `secretsmanager:UpdateSecret`
- `secretsmanager>DeleteSecret`
- `secretsmanager:GetRandomPassword`
- `secretsmanager:TagResource`

Se l'utente desidera passare una chiave KMS nel parametro `MasterPasswordSecretKmsKeyId` per i cluster con provisioning o il parametro `AdminPasswordSecretKmsKeyId` per gli spazi dei nomi serverless, sono necessarie le seguenti autorizzazioni oltre a quelle sopra elencate.

- `kms:Decrypt`
- `kms:GenerateDataKey`
- `kms:CreateGrant`
- `kms:RetireGrant`

## Rotazione del segreto della password dell'amministratore

Per impostazione predefinita, Amazon Redshift ruota automaticamente il segreto ogni 30 giorni per garantire che le credenziali non rimangano invariate per periodi prolungati. Quando Amazon Redshift rende segreta una password di amministratore, AWS Secrets Manager aggiorna la segreta esistente per contenere una nuova password di amministratore. Amazon Redshift modifica la password dell'amministratore per il cluster in modo che corrisponda alla password presente nel segreto aggiornato.

Con AWS Secrets Manager puoi ruotare un segreto immediatamente invece di aspettare la rotazione programmata. Per ulteriori informazioni sulla rotazione dei segreti, consulta [Ruotare i AWS Secrets Manager segreti](#) nella Guida per l'utente AWS Secrets Manager

## Recupero del nome della risorsa Amazon (ARN) del segreto in Amazon Redshift

Puoi visualizzare il nome della risorsa Amazon (ARN) per tutti i segreti gestiti da AWS Secrets Manager utilizzando la console Amazon Redshift. Una volta ottenuto l'ARN del segreto, puoi visualizzare i dettagli sul tuo segreto e sui dati crittografati contenuti nel tuo utilizzo segreto. AWS Secrets Manager Per ulteriori informazioni sul recupero dei segreti utilizzando l'ARN, consulta [Recuperare segreti](#) nella Guida per l'utente di AWS Secrets Manager .

### Visualizzazione dei dettagli di un segreto per un cluster con provisioning Amazon Redshift

Visualizza il nome della risorsa Amazon (ARN) per il segreto del cluster utilizzando la console Amazon Redshift con la seguente procedura:

1. Accedi AWS Management Console e apri la console Amazon Redshift.
2. Nel riquadro Panoramica del cluster seleziona il cluster di cui desideri visualizzare il segreto.
3. Scegliere la scheda Properties (Proprietà).
4. Visualizza l'ARN del segreto sotto ARN delle credenziali dell'amministratore. Questo ARN è l'identificatore del segreto, che puoi utilizzare AWS Secrets Manager per visualizzarne i dettagli.

### Visualizzazione dei dettagli di un segreto per uno spazio dei nomi Amazon Redshift serverless

Visualizza il nome della risorsa Amazon (ARN) per il segreto dello spazio dei nomi serverless utilizzando la console Amazon Redshift con la seguente procedura:

1. Accedi AWS Management Console e apri la console Amazon Redshift.
2. Dal Pannello di controllo dei cluster con provisioning scegli Vai a Serverless nella parte superiore destra della pagina.
3. Dal Pannello di controllo serverless, scorri fino al riquadro Spazi dei nomi/Gruppi di lavoro e scegli lo spazio dei nomi di cui desideri visualizzare il segreto.
4. Nel riquadro Informazioni generali visualizza l'ARN del segreto in ARN delle credenziali dell'amministratore. Questo ARN è l'identificatore del segreto, che puoi utilizzare AWS Secrets Manager per visualizzarne i dettagli.

## Creazione di un segreto per le credenziali di connessione al database

Puoi creare un segreto di Secrets Manager per archiviare le credenziali utilizzate per connetterti a un cluster con provisioning di Amazon Redshift o allo spazio dei nomi e al gruppo di lavoro Redshift

Serverless. Puoi utilizzare questo segreto anche per pianificare una query nell'editor di query di Amazon Redshift v2.

Per creare un segreto per un database in un cluster con provisioning di Amazon Redshift utilizzando la console Secrets Manager

1. Aprire la console Secrets Manager (<https://console.aws.amazon.com/secretsmanager/>).
2. Vai all'elenco dei segreti e scegli Memorizza un nuovo segreto.
3. Scegli Credentials for Amazon Redshift data warehouse. Inserisci le tue informazioni nei passaggi per creare un segreto come segue:
  - In Credenziali per il nome utente, inserisci il nome dell'utente amministrativo del data warehouse.
  - In Credenziali per password, immettere la password per il nome utente.
  - Per Chiave di crittografia, scegli la tua chiave di crittografia.
  - Per il data warehouse, scegli il cluster con provisioning di Amazon Redshift che contiene i tuoi dati.
  - Per Nome segreto, inserisci un nome per il segreto.
  - In Descrizione, inserisci una descrizione del segreto.
  - Per Tag, inserisci una chiave Tag con la parola **Redshift**. Questa chiave di tag è necessaria per elencare i segreti quando tenti di connetterti al tuo data warehouse utilizzando Amazon Redshift query editor v2. Il segreto deve avere una chiave di tag che inizi con la stringa in cui **Redshift** il segreto deve essere elencato nella console AWS Secrets Manager di gestione.
4. Continua a inserire le informazioni sul tuo segreto seguendo diversi passaggi fino a quando non memorizzi le modifiche nella fase di revisione.

I valori specifici delle credenziali, del motore, dell'host, della porta e dell'identificatore del cluster sono archiviati nel segreto. Inoltre, il segreto è contrassegnato con la chiave tag. **Redshift**

Per creare un segreto per un database in uno spazio dei nomi Redshift Serverless utilizzando la console Redshift Serverless

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Scegli Redshift serverless e accedi alla configurazione del namespace.
3. Scegli uno spazio dei nomi per il quale creare credenziali segrete.

4. Apri Azioni, Modifica le credenziali di amministratore.
5. Per la password di amministratore, scegli Gestisci le credenziali di amministratore in. AWS Secrets Manager
6. Per salvare le modifiche, scegliere Salva modifiche.

Conferma che venga visualizzato un messaggio che indica che la password è stata modificata correttamente. Puoi anche visualizzare il segreto nella console Secrets Manager. Puoi utilizzare questo segreto per connetterti a un database in un gruppo di lavoro nella console Redshift Serverless e nell'editor di query di Amazon Redshift v2, utilizzando il metodo di connessione. AWS Secrets Manager Il segreto deve avere una chiave di tag che inizi con la stringa «Redshift» affinché il segreto venga elencato nell'applicazione web Query Editor v2. Il segreto deve avere una chiave di tag che inizi con la stringa in cui **Redshift** il segreto deve essere elencato nella console AWS Secrets Manager di gestione.

Per creare un segreto per un database in uno spazio dei nomi Redshift Serverless utilizzando la console Secrets Manager

1. Aprire la console Secrets Manager (<https://console.aws.amazon.com/secretsmanager/>).
2. Vai all'elenco dei segreti e scegli Memorizza un nuovo segreto.
3. Scegli Credentials for Amazon Redshift data warehouse. Inserisci le tue informazioni nei passaggi per creare un segreto come segue:
  - In Credenziali per il nome utente, inserisci il nome dell'utente amministrativo del data warehouse.
  - In Credenziali per password, immettere la password per il nome utente.
  - Per Chiave di crittografia, scegli la tua chiave di crittografia.
  - Per Data warehouse, scegli lo spazio dei nomi Redshift Serverless che contiene i tuoi dati.
  - Per Nome segreto, inserisci un nome per il segreto.
  - In Descrizione, inserisci una descrizione del segreto.
  - Per Tag, inserisci una chiave Tag con la parola **Redshift**. Questa chiave di tag è necessaria per elencare i segreti quando tenti di connetterti al tuo data warehouse utilizzando Amazon Redshift query editor v2. Il segreto deve avere una chiave di tag che inizi con la stringa in cui **Redshift** il segreto deve essere elencato nella console AWS Secrets Manager di gestione.
4. Continua a inserire le informazioni sul tuo segreto seguendo diversi passaggi fino a quando non memorizzi le modifiche nella fase di revisione.

I valori specifici delle credenziali, del nome del database, dell'host, della porta, dello spazio dei nomi e del motore sono archiviati nel segreto. Inoltre, il segreto è contrassegnato con la chiave tag. Redshift

Per creare un segreto per un database in uno spazio dei nomi Redshift Serverless utilizzando AWS CLI

È possibile utilizzare il per creare un segreto AWS CLI . Un metodo consiste nell' AWS CloudShell eseguire il AWS CLI comando Secrets Manager come segue. È necessario disporre delle autorizzazioni appropriate per eseguire i AWS CLI comandi illustrati nella procedura seguente.

1. Sulla AWS console, aprire il prompt dei AWS CloudShell comandi. Per ulteriori informazioni AWS CloudShell, consulta [Cosa c'è AWS CloudShell](#) nella Guida per l'AWS CloudShell utente.
2. Ad esempio, per il segreto, MyTestSecret inserisci un comando Secrets Manager per memorizzare il segreto utilizzato per connettersi a un database o pianificare una query Amazon Redshift Query Editor v2. Sostituisci i seguenti valori nel comando con valori per il tuo ambiente:
  - *admin* è il nome utente dell'amministratore per il data warehouse.
  - *passwd0rd* è la password dell'amministratore.
  - *dev* è il nome iniziale del database nel data warehouse.
  - la *regione* è Regione AWS quella che contiene il data warehouse. Ad esempio us-east-1.
  - *123456789012* è il. Account AWS
  - *namespace-id* è l'identificatore dello spazio dei nomi simile a. c3928f0e-c889-4d2b-97a5-5738324d5d3e Puoi trovare questo identificatore nella pagina dei dettagli della console Amazon Redshift per lo spazio dei nomi serverless.

```
aws secretsmanager create-secret \  
--name MyTestSecret \  
--description "My test secret created with the CLI." \  
--secret-string "{\"username\":\"admin\",\"password\":\"passwd0rd\",\"dbname\":\  
\"dev\",\"engine\":\"redshift\"}" \  
--tags "[{\"Key\":\"redshift-serverless:namespaceArn\",\"Value\":\  
\"arn:aws:redshift-serverless:region:123456789012:namespace/namespace-id\"}]"
```

## Considerazioni sull'utilizzo AWS Secrets Manager con Amazon Redshift

Quando lo utilizzi AWS Secrets Manager per gestire le credenziali di amministratore del cluster o dello spazio dei nomi serverless fornito, considera quanto segue:

- Quando metti in pausa un cluster le cui credenziali di amministratore sono gestite da AWS Secrets Manager, il segreto del cluster non verrà eliminato e continuerai a ricevere la fattura per il segreto. I segreti vengono eliminati solo quando elimini il cluster.
- Se il cluster è sospeso quando Amazon Redshift tenta di ruotare il segreto associato, la rotazione avrà esito negativo. In questo caso, Amazon Redshift interrompe la rotazione automatica e non la ritenta, neanche dopo la ripresa del cluster. È necessario riavviare la pianificazione di rotazione automatica utilizzando la chiamata `secretsmanager:RotateSecret` API per continuare a far ruotare AWS Secrets Manager automaticamente il segreto.
- Se lo spazio dei nomi serverless non ha un gruppo di lavoro associato quando Amazon Redshift tenta di ruotare il segreto collegato, la rotazione avrà esito negativo e viene più ritentata, neanche dopo aver collegato un gruppo di lavoro. È necessario riavviare la pianificazione di rotazione automatica utilizzando la chiamata `secretsmanager:RotateSecret` API per continuare a far ruotare AWS Secrets Manager automaticamente il segreto.

## Registrazione e monitoraggio in Amazon Redshift

Il monitoraggio è importante per garantire l'affidabilità, la disponibilità e le prestazioni di Amazon Redshift e delle soluzioni AWS. È possibile raccogliere dati di monitoraggio da tutte le parti della soluzione AWS per eseguire più facilmente il debug nel caso si verificano guasti in più punti.

AWS fornisce diversi strumenti per il monitoraggio delle risorse di Amazon Redshift e per rispondere a potenziali incidenti.

### Allarmi di Amazon CloudWatch

Utilizzando gli allarmi di Amazon CloudWatch, è possibile osservare un singolo parametro per il periodo di tempo specificato. Se il parametro supera una determinata soglia, viene inviata una notifica a un argomento Amazon SNS o alla policy AWS Auto Scaling. Gli allarmi CloudWatch non richiamano le operazioni perché si trovano in uno stato particolare. È necessario invece cambiare lo stato e mantenerlo per un numero di periodi specificato. Per ulteriori informazioni, consultare [Gestione degli allarmi](#). Per un elenco di parametri, consultare [Monitoraggio di Amazon Redshift tramite metriche CloudWatch](#).

## AWS CloudTrailLog di

CloudTrail fornisce un record di operazioni API eseguite da un utente, un ruolo IAM o un servizio AWS in Amazon Redshift. L'uso delle informazioni raccolte da CloudTrail consente di determinare la richiesta effettuata ad Amazon Redshift, 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 con CloudTrail](#).

## Logging di controllo dei database

Amazon Redshift registra informazioni su connessioni e attività degli utenti nel database. Questi log ti aiutano a monitorare il database per scopi di sicurezza e risoluzione dei problemi, un processo noto con il nome di controllo dei database. I registri possono essere archiviati in:

- Bucket Amazon S3: offrono un accesso con caratteristiche di sicurezza dei dati per gli utenti responsabili delle attività di monitoraggio nel database.
- Amazon CloudWatch: puoi visualizzare i dati di registrazione dei controlli utilizzando le funzionalità integrate CloudWatch, come le funzioni di visualizzazione e le azioni di impostazione.

### Note

[SYS\\_CONNECTION\\_LOG](#) raccoglie i dati di log delle connessioni per Amazon Redshift Serverless. Tieni presente che quando raccogli dati di audit logging per Amazon Redshift Serverless, non possono essere inviati ai file di log, ma solo a CloudWatch

## Argomenti

- [Log di Amazon Redshift](#)
- [Abilitazione della registrazione](#)
- [Invio di registri di controllo ad Amazon CloudWatch](#)
- [Gestione dei file di log in Simple Storage Service \(Amazon S3\)](#)
- [Risoluzione dei problemi relativi alla registrazione di verifica di Amazon Redshift in Simple Storage Service \(Amazon S3\)](#)
- [Registrazione delle chiamate API Amazon Redshift con AWS CloudTrail](#)
- [Configurazione del controllo tramite la console](#)

- [Configurazione della registrazione utilizzando l'API Amazon AWS CLI Redshift](#)

## Log di Amazon Redshift

Amazon Redshift registra informazioni nei file di log seguenti:

- Log di connessione: registra i tentativi di autenticazione, connessioni e disconnessioni.
- Log degli utenti: registra le informazioni sulle modifiche apportate alle definizioni degli utenti del database.
- Log attività utente: registra ogni query prima che venga eseguita nel database.

I log delle connessioni e degli utenti sono utili prevalentemente per scopi di sicurezza. Puoi utilizzare il registro delle connessioni per monitorare le informazioni sugli utenti che si connettono al database e le relative informazioni di connessione. Queste informazioni potrebbero essere il loro indirizzo IP, il momento in cui hanno effettuato la richiesta, quale tipo di autenticazione hanno usato e così via. Puoi usare il log degli utenti per monitorare le modifiche apportate alle definizioni degli utenti di database.

Il log delle attività degli utenti è utile prevalentemente per scopi di risoluzione dei problemi e tiene traccia delle informazioni sui tipi di query eseguite dagli utenti e dal sistema nel database.

Le informazioni del log delle connessioni e del log degli utenti corrispondono a quelle archiviate nelle tabelle di sistema nel database. È possibile usare le tabelle di sistema per ottenere le stesse informazioni, ma i file di log offrono un meccanismo più semplice per il recupero e l'analisi. Per eseguire query sulle tabelle, i file di log si basano sulle autorizzazioni di Amazon S3 piuttosto che sulle autorizzazioni del database. Inoltre, visualizzando le informazioni nei file di log invece di eseguire query sulle tabelle di sistema, puoi ridurre l'impatto dell'interazione con il database.

### Note

I file di log non sono aggiornati quanto le tabelle dei log di sistema che sono [STL\\_USERLOG](#) e [STL\\_CONNECTION\\_LOG](#). Nei file di log vengono copiati i record più vecchi del record più recente (questo escluso).

**Note**

[SYS\\_CONNECTION\\_LOG](#) raccoglie i dati del log delle connessioni per Amazon Redshift Serverless. Quando raccogli dati di audit logging per Amazon Redshift Serverless, non possono essere inviati ai file di log, ma solo a CloudWatch

## Log delle connessioni

Registra i tentativi di autenticazione, insieme alle connessioni e disconnessioni. La tabella seguente descrive le informazioni incluse nel log delle connessioni. Per ulteriori informazioni su questi campi, consultare [STL\\_CONNECTION\\_LOG](#) nella Guida per gli sviluppatori di database di Amazon Redshift. Per ulteriori informazioni sui dati di log delle connessioni raccolti per Amazon Redshift Serverless, consulta [SYS\\_CONNECTION\\_LOG](#).

Nome colonna	Descrizione
evento	Evento di connessione o autenticazione.
recordtime	Ora in cui l'evento si è verificato.
remotehost	Nome o indirizzo IP dell'host remoto.
remoteport	Numero di porta per l'host remoto.
pid	ID di processo associato all'istruzione.
dbname	Nome del database.
username	Nome dell'utente.
authmethod	Metodo di autenticazione.
durata	Durata di connessione in microsecondi.
sslversion	Versione Secure Sockets Layer (SSL).
sslcipher	Crittografia SSL.
mtu	Unità di trasmissione massima (MTU).

Nome colonna	Descrizione
sslcompression	Tipo di compressione SSL.
sslexpansion	Tipo di espansione SSL.
iamauthguid	L'ID di autenticazione AWS Identity and Access Management (IAM) per la richiesta. AWS CloudTrail Questo è l'identificatore della chiamata <a href="#">GetClusterCredentials</a> API per creare le credenziali utilizzate per una determinata connessione.
application_name	Il nome iniziale o aggiornato dell'applicazione per una sessione.
os_version	La versione del sistema operativo presente sul client che si connette al cluster Amazon Redshift.
driver_version	La versione del driver ODBC o JDBC che si connette al cluster Amazon Redshift dagli strumenti client SQL di terze parti.
plugin_name	Il nome del plug-in utilizzato per connettersi al cluster Amazon Redshift.
protocol_version	La versione del protocollo interno utilizzato dal driver Amazon Redshift per stabilire la connessione con il server.
sessionid	L'identificatore univoco globale per la sessione attuale.
compression	L'algoritmo di compressione utilizzato per la connessione.

## Log degli utenti

Registra i dettagli per le seguenti modifiche a un utente di database:

- Create user (Crea utente)
- Rimozione dell'utente
- Modifica di un utente (assegnazione di un nuovo nome)
- Modifica di un utente (modifica delle proprietà)

Nome colonna	Descrizione
userid	ID dell'utente interessato dalla modifica.
username	Nome utente dell'utente interessato dalla modifica.
oldusername	Per un'operazione di assegnazione di un nuovo nome, il nome utente originale. Per ogni altra operazione, questo campo è vuoto.
action	Operazione che si è verificata. Valori validi: <ul style="list-style-type: none"> <li>• Alter</li> <li>• Crea</li> <li>• Drop (E-mail eliminata)</li> <li>• Assegnazione di un nuovo nome</li> </ul>
usecreatedb	Se true (1), indica che l'utente ha creato delle autorizzazioni del database.
usesuper	Se true (1), indica che l'utente è un utente con privilegi avanzati.
usecatupd	Se true (1), indica che l'utente può aggiornare i cataloghi di sistema.
valuntil	Data di scadenza della password.
pid	ID processo.
xid	ID transazione.
recordtime	Ora in UTC in cui è stata avviata la query.

Interroga la visualizzazione del sistema [SYS\\_USERLOG](#) per trovare informazioni aggiuntive sulle modifiche apportate agli utenti. Questa visualizzazione include i dati di log di Amazon Redshift Serverless.

Log delle attività degli utenti

Registra ogni query prima che venga eseguita nel database.

Nome colonna	Descrizione
recordtime	Ora in cui l'evento si è verificato.
db	Nome del database.
Utente	Nome dell'utente.
pid	ID di processo associato all'istruzione.
userid	ID utente.
xid	ID transazione.
query	Prefisso LOG: seguito dal testo della query, incluse le nuove righe.

## Abilitazione della registrazione

La registrazione di verifica non è abilitata in Amazon Redshift, per impostazione predefinita. Quando attivi la registrazione sul cluster, Amazon Redshift esporta i log su Amazon oppure crea e carica i log su CloudWatch Amazon S3, che acquisiscono i dati dal momento in cui la registrazione di audit è abilitata fino a oggi. Ogni aggiornamento di registrazione è una continuazione delle registrazioni precedenti.

La registrazione di audit su CloudWatch o su Amazon S3 è un processo facoltativo. La registrazione nelle tabelle di sistema non è facoltativa e avviene automaticamente. Per ulteriori informazioni sulla registrazione con le tabelle di sistema, consultare [Riferimento alle tabelle di sistema](#) nella Guida per gli sviluppatori di Amazon Redshift.

Il log di connessione, il log utente e il log delle attività degli utenti vengono abilitati insieme utilizzando Amazon Redshift API Reference o AWS Command Line Interface (AWS CLI). AWS Management Console Per il log delle attività degli utenti, devi anche abilitare il parametro di database `enable_user_activity_logging`. Se abiliti solo la funzionalità di logging di controllo, ma non il parametro associato, i log di controllo dei database registrano informazioni solo per il log delle connessioni e il log degli utenti, ma non per il log delle attività degli utenti. Per impostazione predefinita, il parametro `enable_user_activity_logging` non è abilitato (`false`). Puoi impostarlo al valore `true` per abilitare il log delle attività degli utenti. Per ulteriori informazioni, consulta [Gruppi di parametri di Amazon Redshift](#).

## Invio di registri di controllo ad Amazon CloudWatch

Quando abiliti la registrazione a CloudWatch, Amazon Redshift esporta i dati dei log di connessione del cluster, utenti e attività degli utenti in un gruppo di log CloudWatch Amazon Logs. I dati di log non cambiano, in termini di schema. CloudWatch è progettato per il monitoraggio delle applicazioni e può essere utilizzato per eseguire analisi in tempo reale o impostarlo per eseguire azioni. Puoi anche utilizzare Amazon CloudWatch Logs per archiviare i tuoi record di registro in uno spazio di archiviazione durevole.

L'uso CloudWatch per visualizzare i log è un'alternativa consigliata all'archiviazione dei file di registro in Amazon S3. Non richiede molta configurazione e può soddisfare i requisiti di monitoraggio, soprattutto se lo si utilizza già per monitorare altri servizi e applicazioni.

### Gruppi di log ed eventi di log in Amazon CloudWatch

Dopo aver selezionato i log di Amazon Redshift da esportare, puoi monitorare gli eventi di log in Amazon Logs. CloudWatch Un nuovo gruppo di registri viene creato automaticamente per Amazon Redshift Serverless con il seguente prefisso, in cui `log_type` rappresenta il tipo di registro.

```
/aws/redshift/cluster/<cluster_name>/<log_type>
```

Ad esempio, se scegli di esportare il log di connessione, i dati di log vengono archiviati nel seguente gruppo di log.

```
/aws/redshift/cluster/cluster1/connectionlog
```

Il registro eventi viene esportato in un gruppo di registri utilizzando il flusso di log. Per cercare informazioni all'interno degli eventi di registro per il tuo endpoint serverless, usa la console Amazon CloudWatch Logs, o l' AWS CLI API Amazon CloudWatch Logs. Per informazioni sulla ricerca e l'applicazione di filtri per i dati di registro, consulta [Creazione di parametri da registro eventi mediante filtri](#).

In CloudWatch, puoi cercare i dati di log con una sintassi di query che garantisce granularità e flessibilità. Per ulteriori informazioni, consulta la sintassi delle query di [CloudWatch Logs Insights](#).

### Migrazione alla registrazione di CloudWatch controllo di Amazon

In ogni caso, quando si inviano log ad Amazon S3 e si modifica la configurazione, ad esempio per inviare log a, i log CloudWatch che rimangono in Amazon S3 non subiscono alcuna modifica. È comunque possibile eseguire query sui dati di registro nei bucket Amazon S3 in cui risiedono.

## Gestione dei file di log in Simple Storage Service (Amazon S3)

Il numero e le dimensioni dei file di log di Amazon Redshift in Amazon S3 dipendono in larga misura dall'attività nel cluster. Se il cluster è attivo e sta generando un numero elevato di log, Amazon Redshift può generare i file di log più spesso. Può essere generata una serie di file di log per lo stesso tipo di attività, ad esempio più log delle connessioni nella stessa ora.

Poiché Amazon Redshift utilizza Simple Storage Service (Amazon S3) per archiviare i registri, verranno addebitati i costi dell'archiviazione utilizzata in Simple Storage Service (Amazon S3). Prima di configurare la registrazione in Simple Storage Service (Amazon S3), è necessario disporre di un piano per determinare per quanto tempo è necessario archiviare i file di log. Inoltre, è necessario determinare quando è possibile eliminare o archiviare i file di log in base alle proprie esigenze di verifica. Il piano creato dipende in larga misura dal tipo di dati archiviati, ad esempio dati soggetti a requisiti normativi o di conformità. Per ulteriori informazioni sui prezzi di Amazon S3, consultare [Prezzi di Amazon Simple Storage Service \(S3\)](#).

### Limitazioni dell'abilitazione della registrazione su Amazon S3

La registrazione dei log di verifica ha i seguenti vincoli:

- Puoi utilizzare solo la crittografia delle chiavi gestite da Amazon S3 (SSE-S3) (AES-256).
- I bucket Amazon S3 devono avere la funzionalità Blocco oggetti di S3 disattivata.

### Autorizzazioni del bucket per la registrazione di verifica di Amazon Redshift

Quando si abilita la registrazione in Simple Storage Service (Amazon S3), Amazon Redshift raccoglie informazioni di registrazione e le carica in file di log archiviati in Simple Storage Service (Amazon S3). È possibile creare un nuovo bucket o utilizzare un bucket esistente. Amazon Redshift richiede le autorizzazioni IAM seguenti per il bucket:

- `s3:GetBucketAc1`: il servizio richiede autorizzazioni di lettura per il bucket Amazon S3 per poter identificare il proprietario del bucket.
- `s3:PutObject`: il servizio richiede autorizzazioni di inserimento di oggetti per caricare i log. Inoltre, l'utente o il ruolo IAM che attiva la registrazione deve disporre dell'autorizzazione `s3:PutObject` per il bucket Amazon S3. Ogni volta che vengono caricati log, il servizio determina se il proprietario corrente del bucket corrisponde al proprietario del bucket al momento dell'abilitazione del logging. Se questi proprietari non corrispondono, verrà ricevuto un errore.

Quando abiliti la registrazione di controllo, selezionando l'opzione per creare un nuovo bucket, ad esso verranno applicate le corrette autorizzazioni. Tuttavia, se il bucket viene creato personalmente in Amazon S3 o si utilizza un bucket esistente, aggiungere una policy di bucket che includa il nome del bucket. I registri vengono consegnati utilizzando le credenziali principali del servizio. *Per la maggior parte Regioni AWS, aggiungi il nome principale del servizio Redshift, `redshift.amazonaws.com`.*

La policy del bucket utilizza il formato seguente. *ServiceName* e *BucketName* sono segnaposto dei tuoi valori. Specificare inoltre le azioni e le risorse associate nella policy del bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "Service": "ServiceName"
      },
      "Action": [
        "s3:PutObject",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::BucketName",
        "arn:aws:s3:::BucketName/*"
      ]
    }
  ]
}
```

L'esempio seguente mostra una policy del bucket per la regione Stati Uniti orientali (Virginia settentrionale) e un bucket denominato AuditLogs.

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "Service": "redshift.amazonaws.com"
      }
    }
  ]
}
```

```
    },
    "Action": [
      "s3:PutObject",
      "s3:GetBucketAcl"
    ],
    "Resource": [
      "arn:aws:s3:::AuditLogs",
      "arn:aws:s3:::AuditLogs/*"
    ]
  }
]
```

Le Regioni che non sono abilitate di default, conosciute anche come regioni "scelte", richiedono un nome del principale di servizio specifico per la Regione. Per questi, il nome principale del servizio include la regione, nel formato `redshift.region.amazonaws.com`. Ad esempio: `redshift.ap-east-1.amazonaws.com` per la regione Asia Pacifico (Hong Kong). Per un elenco di regioni che non sono abilitate per impostazione predefinita, consulta [Gestione delle Regioni AWS](#) in Riferimenti generali di AWS.

#### Note

Il nome del principale del servizio specifico della Regione corrisponde alla Regione in cui si trova il cluster.

### Best practice per i file di registro

Quando Redshift carica i file di registro su Amazon S3, è possibile caricare file di grandi dimensioni in parti. Se un caricamento in più parti non ha esito positivo, è possibile che parti di un file rimangano nel bucket Amazon S3. Ciò può comportare costi di storage aggiuntivi, quindi è importante capire cosa si verifica quando un caricamento in più parti fallisce. Per una spiegazione dettagliata sul caricamento in più parti per i registri di controllo, vedere [Caricamento e copia di oggetti utilizzando il caricamento in più parti](#) e [Interruzione di un caricamento in più parti](#).

Per ulteriori informazioni sulla creazione di bucket S3 e sull'aggiunta di policy di bucket, consultare [Creazione di un bucket](#) e [Modifica delle autorizzazioni del bucket](#) nella Guida per l'utente della console di Amazon Simple Storage Service.

## Struttura del bucket per il logging di verifica in Amazon Redshift

Per impostazione predefinita, Amazon Redshift organizza i file di log nel bucket Amazon S3 utilizzando il bucket e la struttura di oggetti seguenti:

`AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region`

Un esempio è: `AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Se si specifica un prefisso della chiave di Amazon S3, posizionare il prefisso all'inizio della chiave.

Ad esempio, se specifichi il prefisso `myprefix`: `myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz`

Il prefisso della chiave di Amazon S3 non può contenere più di 512 caratteri e non può contenere spazi ( ), virgolette doppie ("), virgolette singole (') né una barra rovesciata (\). C'è anche un numero non consentito di caratteri speciali e caratteri di controllo. I codici esadecimali per questi caratteri sono i seguenti:

- Da `x00` a `x20`
- `x22`
- `x27`
- `x5c`
- `x7f` o maggiore

## Risoluzione dei problemi relativi alla registrazione di verifica di Amazon Redshift in Simple Storage Service (Amazon S3)

La registrazione di verifica in Amazon Redshift può essere interrotta per i motivi seguenti:

- Amazon Redshift non dispone dell'autorizzazione necessaria per caricare i log nel bucket Amazon S3. Verifica che il bucket sia configurato con la policy IAM corretta. Per ulteriori informazioni, consultare [Autorizzazioni del bucket per la registrazione di verifica di Amazon Redshift](#).
- Il proprietario del bucket è cambiato. Quando Amazon Redshift carica i log, verifica che il proprietario del bucket sia lo stesso di quello al momento dell'abilitazione della registrazione. Se

il proprietario del bucket è cambiato, Amazon Redshift non potrà caricare i log finché non viene configurato un altro bucket da usare per la registrazione di verifica.

- Non è possibile trovare il bucket. Se il bucket è stato eliminato in Amazon S3, Amazon Redshift non può caricare i log. Per il caricamento dei registri in un bucket diverso sarà necessario creare nuovamente il bucket oppure configurare di conseguenza Amazon Redshift.

## Registrazione delle chiamate API Amazon Redshift con AWS CloudTrail

Amazon Redshift è integrato con AWS CloudTrail un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon Redshift. CloudTrail acquisisce tutte le chiamate API per Amazon Redshift come eventi. Per ulteriori informazioni sull'integrazione di Amazon Redshift con AWS CloudTrail, consulta [Logging](#) with. CloudTrail

Puoi utilizzarlo CloudTrail indipendentemente o in aggiunta alla registrazione di audit del database Amazon Redshift.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'[AWS CloudTrail utente](#).

## Configurazione del controllo tramite la console

Configurazione di Amazon Redshift per esportare i dati di registro di verifica. I log possono essere esportati o come file in bucket Amazon S3. CloudWatch

Abilitazione del logging di controllo tramite la console

Passaggi della console

Per abilitare il logging di controllo per un cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere il cluster da aggiornare.
3. Scegliere la scheda Properties (Proprietà). Nel pannello Database configurations (Configurazioni dei database), scegliere Edit (Modifica), quindi Edit audit logging (Modifica dei registri di verifica).
4. Nella pagina Modifica registrazione di controllo, scegli Attiva e seleziona S3 bucket o. CloudWatch Ti consigliamo di utilizzarlo CloudWatch perché l'amministrazione è semplice e offre funzioni utili per la visualizzazione dei dati.
5. Scegliere i registri da esportare.
6. Per salvare le modifiche, scegliere Save changes (Salva modifiche).

## Configurazione della registrazione utilizzando l'API Amazon AWS CLI Redshift

Per configurare la registrazione di verifica, è possibile utilizzare la seguente CLI di Amazon Redshift:

- [describe-logging-status](#)
- [disable-logging](#)
- [enable-logging](#)

Per configurare la registrazione di verifica, è possibile utilizzare le seguenti operazioni API di Amazon Redshift:

- [DescribeLoggingStatus](#)
- [DisableLogging](#)
- [EnableLogging](#)

## Registrazione con CloudTrail

### Registrazione delle chiamate con AWS CloudTrail

Amazon Redshift, la condivisione dei dati, Amazon Redshift Serverless, Amazon Redshift Data API e l'editor di query v2 sono tutti integrati con AWS CloudTrail. CloudTrail è un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon Redshift. CloudTrail acquisisce tutte le chiamate API per Amazon Redshift come eventi. Le chiamate acquisite includono le chiamate dalla console Amazon Redshift e le chiamate di codice alle operazioni di Redshift.

Se crei un CloudTrail trail, puoi disporre di una distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Redshift. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare determinate cose. Sono inclusi la richiesta effettuata a Redshift, l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, la data/ora in cui è stata effettuata e altri dettagli.

Puoi utilizzarlo CloudTrail indipendentemente o in aggiunta alla registrazione di audit del database Amazon Redshift.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'[AWS CloudTrail utente](#).

## Utilizzo delle informazioni in CloudTrail

CloudTrail è attivata nel tuo AWS account quando crei l'account. Quando si verifica un'attività, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#) nella Guida AWS CloudTrail per l'utente.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Redshift, crea un percorso. CloudTrail utilizza trail per inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il trail registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consultare gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail:

- [Panoramica della creazione di un trail](#)
- [CloudTrail Servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte le azioni di Amazon Redshift, Amazon Redshift Serverless, Data API, condivisione dei dati e Query Editor v2 vengono registrate da CloudTrail. Ad esempio, le chiamate a `AuthorizeDatashare`, `CreateNamespace`, `ExecuteStatement`, e le `CreateConnection` azioni generano voci nei file di registro. 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 credenziali utente o root.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta [CloudTrail UserIdentity Element nella Guida](#) per l'AWS CloudTrail utente.

## Descrizione delle voci dei file di log

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

## Esempio di unità di condivisione dati per Amazon Redshift

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'AuthorizeDataShareoperazione.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::111122223333:user/janedoe",
    "accountId": "111122223333",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
        "arn": "arn:aws:sts::111122223333:user/janedoe",
        "accountId": "111122223333",
        "userName": "janedoe"
      },
      "attributes": {
        "creationDate": "2021-08-02T23:40:45Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2021-08-02T23:40:58Z",
  "eventSource": "redshift.amazonaws.com",
  "eventName": "AuthorizeDataShare",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "3.227.36.75",
```

```

    "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto-core/1.17.41",
    "requestParameters": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "consumerIdentifier": "555555555555"
    },
    "responseElements": {
        "dataShareArn": "arn:aws:redshift:us-
east-1:111122223333:datashare:4c64c6ec-73d5-42be-869b-b7f7c43c7a53/testshare",
        "producerNamespaceArn": "arn:aws:redshift:us-
east-1:123456789012:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "producerArn": "arn:aws:redshift:us-
east-1:111122223333:namespace:4c64c6ec-73d5-42be-869b-b7f7c43c7a53",
        "allowPubliclyAccessibleConsumers": true,
        "dataShareAssociations": [
            {
                "consumerIdentifier": "555555555555",
                "status": "AUTHORIZED",
                "createdDate": "Aug 2, 2021 11:40:56 PM",
                "statusChangeDate": "Aug 2, 2021 11:40:57 PM"
            }
        ]
    },
    "requestID": "87ee1c99-9e41-42be-a5c4-00495f928422",
    "eventID": "03a3d818-37c8-46a6-aad5-0151803bdb09",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}

```

## Esempio per Amazon Redshift Serverless

Amazon Redshift Serverless è integrato con AWS CloudTrail per fornire un registro delle azioni intraprese in Amazon Redshift Serverless. CloudTrail acquisisce tutte le chiamate API per Amazon Redshift Serverless come eventi. Per ulteriori informazioni sulle caratteristiche di Amazon Redshift Serverless, consulta [Panoramica delle funzionalità di Amazon Redshift Serverless](#).

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione. CreateNamespace

```
{
```

```

"eventVersion": "1.08",
"userIdentity": {
  "type": "AssumedRole",
  "principalId": "AAKEOFPINEXAMPLE",
  "arn": "arn:aws:sts::111111111111:assumed-role/admin/admin",
  "accountId": "111111111111",
  "accessKeyId": "AAKEOFPINEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AAKEOFPINEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/admin",
      "accountId": "111111111111",
      "userName": "admin"
    },
    "webIdFederationData": {},
    "attributes": {
      "creationDate": "2022-03-21T20:51:58Z",
      "mfaAuthenticated": "false"
    }
  }
},
"eventTime": "2022-03-21T23:15:40Z",
"eventSource": "redshift-serverless.amazonaws.com",
"eventName": "CreateNamespace",
"awsRegion": "us-east-1",
"sourceIPAddress": "56.23.155.33",
"userAgent": "aws-cli/2.4.14 Python/3.8.8 Linux/5.4.181-109.354.amzn2int.x86_64
exe/x86_64.amzn.2 prompt/off command/redshift-serverless.create-namespace",
"requestParameters": {
  "adminUserPassword": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
  "dbName": "dev",
  "namespaceName": "testnamespace"
},
"responseElements": {
  "namespace": {
    "adminUsername": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "creationDate": "Mar 21, 2022 11:15:40 PM",
    "defaultIamRoleArn": "",
    "iamRoles": [],
    "logExports": [],
    "namespaceArn": "arn:aws:redshift-serverless:us-
east-1:111111111111:namespace/befa5123-16c2-4449-afca-1d27cb40fc99",

```

```

        "namespaceId": "8b726a0c-16ca-4799-acca-1d27cb403599",
        "namespaceName": "testnamespace",
        "status": "AVAILABLE"
    }
},
"requestID": "ed4bb777-8127-4dae-aea3-bac009999163",
"eventID": "1dbee944-f889-4beb-b228-7ad0f312464",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "111111111111",
"eventCategory": "Management",
}

```

## Esempi per l'API di dati di Amazon Redshift

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ExecuteStatementazione.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn": "arn:aws:sts::123456789012:user/janedoe",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime": "2020-08-19T17:55:59Z",
  "eventSource": "redshift-data.amazonaws.com",
  "eventName": "ExecuteStatement",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 botocore/1.17.41",
  "requestParameters": {
    "clusterIdentifier": "example-cluster-identifier",
    "database": "example-database-name",
    "dbUser": "example_db_user_name",
    "sql": "****OMITTED****"
  },
  "responseElements": {
    "clusterIdentifier": "example-cluster-identifier",

```

```

    "createdAt":"Aug 19, 2020 5:55:58 PM",
    "database":"example-database-name",
    "dbUser":"example_db_user_name",
    "id":"5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID":"00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID":"c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly":false,
  "eventType":"AwsApiCall",
  "recipientAccountId":"123456789012"
}

```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'ExecuteStatementazione che mostra l'clientTokenuso per l'idempotenza.

```

{
  "eventVersion":"1.05",
  "userIdentity":{
    "type":"IAMUser",
    "principalId":"AKIAIOSFODNN7EXAMPLE:janedoe",
    "arn":"arn:aws:sts::123456789012:user/janedoe",
    "accountId":"123456789012",
    "accessKeyId":"AKIAI44QH8DHBEXAMPLE",
    "userName": "janedoe"
  },
  "eventTime":"2020-08-19T17:55:59Z",
  "eventSource":"redshift-data.amazonaws.com",
  "eventName":"ExecuteStatement",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"192.0.2.0",
  "userAgent":"aws-cli/1.18.118 Python/3.6.10
Linux/4.9.217-0.1.ac.205.84.332.metal1.x86_64 boto3/1.17.41",
  "requestParameters":{
    "clusterIdentifier":"example-cluster-identifier",
    "database":"example-database-name",
    "dbUser":"example_db_user_name",
    "sql":"***OMITTED***",
    "clientToken":"32db2e10-69ac-4534-b3fc-a191052616ce"
  },
  "responseElements":{
    "clusterIdentifier":"example-cluster-identifier",
    "createdAt":"Aug 19, 2020 5:55:58 PM",
    "database":"example-database-name",

```

```

    "dbUser": "example_db_user_name",
    "id": "5c52b37b-9e07-40c1-98de-12ccd1419be7"
  },
  "requestID": "00c924d3-652e-4939-8a7a-cd0612eeb8ac",
  "eventID": "c1fb7076-102f-43e5-9ec9-40820bcc1175",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

## Editor di query v2 di Amazon Redshift

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'azione. CreateConnection

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAKE0FPINEXAMPLE:session",
    "arn": "arn:aws:sts::123456789012:assumed-role/MyRole/session",
    "accountId": "123456789012",
    "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAKE0FPINEXAMPLE",
        "arn": "arn:aws:iam::123456789012:role/MyRole",
        "accountId": "123456789012",
        "userName": "MyRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-09-21T17:19:02Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-09-21T22:22:05Z",
  "eventSource": "sqlworkbench.amazonaws.com",
  "eventName": "CreateConnection",
  "awsRegion": "ca-central-1",
  "sourceIPAddress": "192.2.0.2",

```

```

"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0)
Gecko/20100101 Firefox/102.0",
"requestParameters": {
  "password": "****",
  "databaseName": "****",
  "isServerless": false,
  "name": "****",
  "host": "redshift-cluster-2.c8robpbxvbf9.ca-central-1.redshift.amazonaws.com",
  "authenticationType": "****",
  "clusterId": "redshift-cluster-2",
  "username": "****",
  "tags": {
    "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
  }
},
"responseElements": {
  "result": true,
  "code": "",
  "data": {
    "id": "arn:aws:sqlworkbench:ca-central-1:123456789012:connection/ce56b1be-
dd65-4bfb-8b17-12345123456",
    "name": "****",
    "authenticationType": "****",
    "databaseName": "****",
    "secretArn": "arn:aws:secretsmanager:ca-
central-1:123456789012:secret:sqlworkbench!7da333b4-9a07-4917-b1dc-12345123456-qTCoFm",
    "clusterId": "redshift-cluster-2",
    "dbUser": "****",
    "userSettings": "****",
    "recordDate": "2022-09-21 22:22:05",
    "updatedAt": "2022-09-21 22:22:05",
    "accountId": "123456789012",
    "tags": {
      "sqlworkbench-resource-owner": "AAKEOFPINEXAMPLE:session"
    },
    "isServerless": false
  }
},
"requestID": "9b82f483-9c03-4cdd-bb49-a7009e7da714",
"eventID": "a7cdd442-e92f-46a2-bc82-2325588d41c3",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",

```

```
"eventCategory": "Management"
}
```

## ID account di Amazon Redshift nei log AWS CloudTrail

Quando Amazon Redshift chiama un altro servizio AWS per tuo conto, la chiamata è registrata con un ID account che appartiene ad Amazon Redshift. Non è registrata con il tuo ID account. Ad esempio, supponiamo che Amazon Redshift chiami le operazioni AWS Key Management Service (AWS KMS) come `CreateGrant`, `Decrypt`, `Encrypt`, e `RetireGrant` per gestire la crittografia sul cluster. In questo caso, le chiamate sono registrate da AWS CloudTrail utilizzando l'ID account di Amazon Redshift.

Quando richiama altri servizi AWS, Amazon Redshift usa gli ID account inclusi nella tabella seguente.

Regione	Regione	ID account
Stati Uniti orientali (Virginia settentrionale)	us-east-1	368064434614
Stati Uniti orientali (Ohio)	us-east-2	790247189693
Regione Stati Uniti occidentali (California settentrionale)	us-west-1	703715109447
Stati Uniti occidentali (Oregon)	us-west-2	473191095985
Regione Africa (Città del Capo)	af-south-1	420376844563
Regione Asia Pacifico (Hong Kong)	ap-east-1	651179539253
Regione Asia Pacifico (Hyderabad)	ap-south-2	297058826802
Regione Asia Pacifico (Giacarta)	ap-southeast-3	623197973179
Regione Asia Pacifico (Melbourne)	ap-southeast-4	945512339897
Regione Asia Pacifico (Mumbai)	ap-south-1	408097707231

Regione	Regione	ID account
Regione Asia Pacifico (Osaka-Locale)	ap-northeast-3	398671365691
Regione Asia Pacifico (Seoul)	ap-northeast-2	713597048934
Asia Pacifico (Singapore)	ap-southeast-1	960118270566
Asia Pacifico (Sydney)	ap-southeast-2	485979073181
Asia Pacifico (Tokyo)	ap-northeast-1	615915377779
Regione Canada (Centrale)	ca-central-1	764870610256
Regione Canada occidentale (Calgary)	ca-west-1	830903446466
Regione Europa (Francoforte)	eu-central-1	434091160558
Europa (Irlanda)	eu-west-1	246478207311
Regione Europa (Londra)	eu-west-2	885798887673
Regione Europa (Milano)	eu-south-1	041313461515
Regione Europa (Parigi)	eu-west-3	694668203235
Regione Europa (Spagna)	eu-south-2	028811157404
Regione Europa (Stoccolma)	eu-north-1	553461782468
Regione Europa (Zurigo)	eu-central-2	668912161003
Regione di Israele (Tel Aviv)	il-central-1	901883065212
Regione Medio Oriente (Bahrein)	me-south-1	051362938876
Regione Medio Oriente (EAU)	me-central-1	595013617770
Sud America (San Paolo)	sa-east-1	392442076723

L'esempio seguente mostra una voce di CloudTrail registro per l'operazione AWS KMS Decrypt chiamata da Amazon Redshift.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAI5QPCMKLTL4VHFCYY:i-0f53e22dbe5df8a89",
    "arn": "arn:aws:sts::790247189693:assumed-role/prod-23264-role-wp/i-0f53e22dbe5df8a89",
    "accountId": "790247189693",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-03T16:24:54Z"
      },
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAI5QPCMKLTL4VHFCYY",
        "arn": "arn:aws:iam::790247189693:role/prod-23264-role-wp",
        "accountId": "790247189693",
        "userName": "prod-23264-role-wp"
      }
    }
  },
  "eventTime": "2017-03-03T17:16:51Z",
  "eventSource": "kms.amazonaws.com",
  "eventName": "Decrypt",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "52.14.143.61",
  "userAgent": "aws-internal/3",
  "requestParameters": {
    "encryptionContext": {
      "aws:redshift:createtime": "20170303T1710Z",
      "aws:redshift:arn": "arn:aws:redshift:us-east-2:123456789012:cluster:my-dw-instance-2"
    }
  },
  "responseElements": null,
  "requestID": "30d2fe51-0035-11e7-ab67-17595a8411c8",
  "eventID": "619bad54-1764-4de4-a786-8898b0a7f40c",
}
```

```
"readOnly": true,
"resources": [
  {
    "ARN": "arn:aws:kms:us-east-2:123456789012:key/f8f4f94f-e588-4254-
b7e8-078b99270be7",
    "accountId": "123456789012",
    "type": "AWS::KMS::Key"
  }
],
"eventType": "AwsApiCall",
"recipientAccountId": "123456789012",
"sharedEventID": "c1daefea-a5c2-4fab-b6f4-d8eaa1e522dc"
}
```

## Convalida della conformità per Amazon Redshift

Revisori di terze parti valutano la sicurezza e la conformità di Amazon Redshift come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco di servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consultare [Servizi AWS coperti dal programma di compliance](#). Per informazioni generali, consultare [Programmi per la conformità di AWS](#).

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consultare [Download dei report in AWS Artifact](#).

La responsabilità di conformità durante l'utilizzo di Amazon Redshift è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e normative applicabili. Se l'utilizzo di Amazon Redshift è soggetto alla conformità con standard come HIPAA, PCI o FedRAMP, AWS fornisce alcune risorse utili:

- [Guide Quick Start sulla sicurezza e la conformità](#), che forniscono considerazioni relative all'architettura e alle fasi per la distribuzione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.
- Il whitepaper [Progettazione per la sicurezza e la conformità HIPAA](#), che descrive il modo in cui le aziende possono utilizzare AWS per creare applicazioni conformi a HIPAA.
- [Risorse per la conformità AWS](#), raccolta di cartelle di lavoro e guide che potrebbero essere utili per il settore e la posizione.

- [AWS Config](#), un servizio AWS, è in grado di valutare il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti di settore.
- [AWS Security Hub](#), un servizio AWS, fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con standard industriali e best practice di sicurezza. Security Hub utilizza controlli di sicurezza per valutare le configurazioni delle risorse e gli standard di sicurezza per aiutarti a rispettare vari framework di conformità. Per ulteriori informazioni sull'utilizzo di Security Hub volto a valutare le risorse Amazon Redshift, consulta [Controlli di Amazon Redshift](#) nella Guida per l'utente di AWS Security Hub.

I seguenti documenti per la conformità e la sicurezza trattano Amazon Redshift e sono disponibili on demand tramite AWS Artifact. Per ulteriori informazioni, consultare [AWS Artifact](#).

- Cloud Computing Compliance Controls Catalogue (C5)
- ISO 27001:2013 Statement of Applicability (SoA)
- Certificazione ISO 27001:2013
- ISO 27017:2015 Statement of Applicability (SoA)
- Certificazione ISO 27017:2015
- ISO 27018:2015 Statement of Applicability (SoA)
- Certificazione ISO 27018:2014
- Certificazione ISO 9001:2015
- Attestazione di conformità allo standard DSS PCI e riepilogo delle responsabilità
- Service Organization Controls (SOC) 1 Report
- Service Organization Controls (SOC) 2 Report
- Service Organization Controls (SOC) 2 Report For Confidentiality

## Resilienza in Amazon Redshift

L'infrastruttura globale di AWS è basata su regioni AWS e zone di disponibilità (AZ) AWS. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. 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 tradizionali.

Quasi tutte le regioni AWS hanno più zone di disponibilità e datacenter. Puoi distribuire le applicazioni tra più zone di disponibilità nella stessa regione per avere maggiore tolleranza ai guasti e una bassa latenza.

Per spostare un cluster in un'altra zona di disponibilità senza perdere i dati o modificare le applicazioni, è possibile configurare il trasferimento del cluster. Con la rilocalizzazione, è possibile continuare le operazioni in caso di interruzione del servizio nel cluster con un impatto minimo. Quando il trasferimento dei cluster è abilitato, Amazon Redshift potrebbe scegliere di trasferire i cluster in alcune situazioni. Per ulteriori informazioni sul trasferimento in Amazon Redshift, consulta [Trasferimento del cluster](#).

Negli scenari di errore in cui si verifica un evento imprevisto in una zona di disponibilità, puoi configurare un'implementazione multi-AZ (di più zone di disponibilità) per garantire che il data warehouse di Amazon Redshift continui a funzionare. Amazon Redshift distribuisce risorse di calcolo uguali in due zone di disponibilità a cui è possibile accedere tramite un singolo endpoint. In caso di errore dell'intera zona di disponibilità, le risorse di calcolo rimanenti nella seconda zona di disponibilità saranno disponibili per continuare l'elaborazione dei carichi di lavoro. Per ulteriori informazioni sulle implementazioni Multi-AZ, consulta [Configurazione dell'implementazione multi-AZ](#).

Per ulteriori informazioni sulle regioni e le zone di disponibilità AWS, consultare [Infrastruttura globale di AWS](#).

## Sicurezza dell'infrastruttura in Amazon Redshift

Come servizio gestito, Amazon Redshift è protetto dalla sicurezza di rete globale di AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina [Sicurezza del cloud AWS](#). Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina [Protezione dell'infrastruttura](#) nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizzare le chiamate all'API pubblicate da AWS per accedere ad Amazon Redshift 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.

## Isolamento di rete

Un Virtual Private Cloud (VPC) basato sul servizio Amazon VPC è la rete privata, isolata logicamente in AWS Cloud. È possibile distribuire un cluster Amazon Redshift all'interno di un VPC seguendo questa procedura:

- Creare un VPC in una regione AWS. Per ulteriori informazioni, consultare [Che cos'è Amazon VPC?](#) nella Guida per l'utente di Amazon VPC
- Creare due o più sottoreti VPC private. Per ulteriori informazioni, consultare [VPC e sottoreti](#) nella Guida per l'utente di Amazon VPC.
- Distribuire un cluster Amazon Redshift. Per ulteriori informazioni, consultare [Gruppi di sottoreti dei cluster Amazon Redshift](#).

Un cluster Amazon Redshift è bloccato per impostazione predefinita sul provisioning. Per consentire il traffico di rete in entrata dai client Amazon Redshift, associare un gruppo di sicurezza VPC in un cluster Amazon Redshift. Per ulteriori informazioni, consultare [Gruppi di sottoreti dei cluster Amazon Redshift](#).

Per abilitare il solo traffico a o da intervalli di indirizzi IP specifici, aggiornare i gruppi di sicurezza con il VPC. Un esempio consiste nel consentire il traffico solo da o alla rete aziendale.

Durante la configurazione delle liste di controllo degli accessi di rete associati alle sottoreti con cui è taggato il cluster Amazon Redshift, assicurati che i rispettivi intervalli CIDR S3 della regione AWS siano aggiunti all'elenco degli elementi consentiti per le regole di ingresso e uscita. In questo modo potrai eseguire operazioni basate su S3 come Redshift Spectrum, COPY e UNLOAD senza interruzioni.

Nel seguente comando di esempio viene analizzata la risposta JSON per tutti gli indirizzi IPv4 utilizzati in Amazon S3 nella regione us-east-1.

```
curl https://ip-ranges.amazonaws.com/ip-ranges.json | jq -r '.prefixes[] |
  select(.region=="us-east-1") | select(.service=="S3") | .ip_prefix'
```

```
54.231.0.0/17
```

```
52.92.16.0/20
```

```
52.216.0.0/15
```

Per le istruzioni su come ottenere intervalli IP S3 per una determinata regione, consulta [Intervalli di indirizzi IP AWS](#).

Amazon Redshift supporta la distribuzione dei cluster in VPC con istanza dedicata a tenant singolo. Per ulteriori informazioni, consultare [Istanze dedicate](#) nella Guida per l'utente di Amazon EC2.

## Gruppi di sicurezza dei cluster Amazon Redshift

Quando si effettua il provisioning di un cluster Amazon Redshift, questo è bloccato per impostazione predefinita perché nessuno possa accedervi. Per concedere ad altri utenti l'accesso in ingresso a un cluster ad Amazon Redshift, è necessario associare il cluster a un gruppo di sicurezza. Se si utilizza la piattaforma EC2-VPC, è possibile usare un gruppo di sicurezza Amazon VPC esistente o definirne uno nuovo e quindi associarlo a un cluster. Per ulteriori informazioni sulla gestione di un cluster nella piattaforma EC2-VPC, consultare [Gestione dei cluster in un VPC](#).

## Connessione ad Amazon Redshift utilizzando un endpoint VPC di interfaccia

È possibile connettersi direttamente al servizio API Amazon Redshift utilizzando un endpoint VPC di interfaccia (AWS PrivateLink) nel Virtual Private Cloud (VPC) invece di connettersi tramite Internet. Per ulteriori informazioni sulle operazioni API di Amazon Redshift, consultare [Operazioni](#) nella Documentazione di riferimento dell'API Amazon Redshift. Per ulteriori informazioni AWS PrivateLink, consulta [Interface VPC endpoints \(AWS PrivateLink\)](#) nella Amazon VPC User Guide. Tenere presente che la connessione JDBC/ODBC al cluster non fa parte del servizio API di Amazon Redshift.

Quando utilizzi un endpoint VPC di interfaccia, la comunicazione tra il tuo VPC e Amazon Redshift avviene interamente all'interno della rete, AWS il che può fornire una maggiore sicurezza. Ogni endpoint VPC è rappresentato da una o più interfacce di rete elastiche con indirizzi IP privati nelle sottoreti del VPC. Per maggiori informazioni sulle interfacce di rete elastiche, consulta le [interfacce di rete elastiche](#) nella Guida dell'utente di Amazon EC2.

Un endpoint VPC di interfaccia collega il VPC direttamente ad Amazon Redshift. Non utilizza un gateway Internet, un dispositivo NAT (Network Address Translation), una connessione di rete

privata virtuale (VPN) o una connessione. AWS Direct Connect Le istanze presenti nel tuo VPC non richiedono indirizzi IP pubblici per comunicare con l'API di Amazon Redshift.

Per utilizzare Amazon Redshift tramite il VPC, sono disponibili due opzioni. Una è quella di connettersi da un'istanza che si trova all'interno del VPC. L'altro è connettere la rete privata al VPC utilizzando un' AWS VPN opzione o. AWS Direct Connect Per ulteriori informazioni sulle AWS VPN opzioni, consulta le [connessioni VPN](#) nella Amazon VPC User Guide. Per informazioni su AWS Direct Connect, consultare [Creazione di una connessione](#) nella Guida per l'utente di AWS Direct Connect .

Puoi creare un endpoint VPC di interfaccia per connetterti ad Amazon Redshift utilizzando i AWS Management Console comandi or (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consultare [Creazione di un endpoint di interfaccia](#).

Una volta creato un endpoint VPC di interfaccia, è possibile abilitare nomi host DNS privati per l'endpoint. Quando si fa, l'endpoint Amazon Redshift predefinito (`https://redshift.Region.amazonaws.com`) restituisce l'endpoint VPC.

Se non si abilitano nomi host DNS privati, Amazon VPC fornisce un nome di endpoint DNS che può essere utilizzato nel formato seguente:

```
VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com
```

Per ulteriori informazioni, consultare [Endpoint VPC di interfaccia \(AWS PrivateLink\)](#) nella Guida per l'utente di Amazon VPC.

Amazon Redshift supporta l'esecuzione di chiamate a tutte le [operazioni API](#) all'interno del VPC.

È possibile collegare le policy di endpoint VPC a un endpoint VPC per controllare l'accesso per i principal AWS Identity and Access Management (IAM). È inoltre possibile associare i gruppi di sicurezza a un endpoint VPC per controllare l'accesso in ingresso e in uscita in base all'origine e alla destinazione del traffico di rete. Un esempio è un intervallo di indirizzi IP. Per ulteriori informazioni, consultare [Controllo degli accessi ai servizi con endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

## Creazione di una policy per l'endpoint VPC per Amazon Redshift

È possibile creare una policy per gli endpoint VPC per Amazon Redshift in cui specificare quanto segue:

- Il principal che può o non può eseguire operazioni

- Le azioni che possono essere eseguite
- Le risorse sui cui si possono eseguire le azioni

Per ulteriori informazioni, consultare [Controllo degli accessi ai servizi con endpoint VPC](#) in Guida per l'utente di Amazon VPC.

Di seguito sono riportati alcuni esempi di policy di endpoint VPC.

### Argomenti

- [Esempio: policy degli endpoint VPC per negare tutti gli accessi da un account specificato AWS](#)
- [Esempio: policy di endpoint VPC per consentire l'accesso VPC solo a un ruolo IAM specificato](#)
- [Esempio: policy di endpoint VPC per consentire l'accesso VPC solo a un principal IAM specificato \(utente\)](#)
- [Esempio: policy di endpoint VPC per consentire operazioni Amazon Redshift di sola lettura](#)
- [Esempio: policy di endpoint VPC che nega l'accesso a un cluster specificato](#)

Esempio: policy degli endpoint VPC per negare tutti gli accessi da un account specificato AWS

La seguente politica degli endpoint VPC nega all' AWS account **123456789012** tutto l'accesso alle risorse che utilizzano questo endpoint.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

```

    }
  ]
}

```

Esempio: policy di endpoint VPC per consentire l'accesso VPC solo a un ruolo IAM specificato

*La seguente policy degli endpoint VPC consente l'accesso completo solo al ruolo IAM `redshiftrolenell' AWS account 123456789012`. A tutte le altre entità principali IAM viene negato l'accesso utilizzando l'endpoint.*

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/redshiftrole"
        ]
      }
    }
  ]
}

```

Si tratta solo di un esempio, nella maggior parte dei casi d'uso ti consigliamo di collegare le autorizzazioni per operazioni specifiche in modo da limitare l'ambito delle autorizzazioni.

Esempio: policy di endpoint VPC per consentire l'accesso VPC solo a un principal IAM specificato (utente)

*La seguente policy sugli endpoint VPC consente l'accesso completo solo all'utente IAM `redshiftadminnell' AWS account 123456789012`. A tutte le altre entità principali IAM viene negato l'accesso utilizzando l'endpoint.*

```

{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",

```

```
    "Resource": "*",
    "Principal": {
      "AWS": [
        "arn:aws:iam::123456789012:user/redshiftadmin"
      ]
    }
  ]
}
```

Si tratta solo di un esempio, nella maggior parte dei casi d'uso ti consigliamo di collegare le autorizzazioni a un ruolo prima di assegnarlo a un utente. Inoltre, suggeriamo di utilizzare operazioni specifiche in modo da limitare l'ambito delle autorizzazioni.

Esempio: policy di endpoint VPC per consentire operazioni Amazon Redshift di sola lettura

La seguente policy sugli endpoint VPC consente solo **123456789012** all' AWS account di eseguire le azioni Amazon Redshift specificate.

Le operazioni specificate forniscono l'equivalente dell'accesso di sola lettura per Amazon Redshift. Tutte le altre azioni sul VPC vengono negate per l'account specificato. Inoltre, a tutti gli altri account viene negato l'accesso. Per visualizzare un elenco delle operazioni Amazon Redshift, consultare [Operazioni, risorse e chiavi di condizione per Amazon Redshift](#) nella Guida per l'utente di IAM.

```
{
  "Statement": [
    {
      "Action": [
        "redshift:DescribeAccountAttributes",
        "redshift:DescribeClusterParameterGroups",
        "redshift:DescribeClusterParameters",
        "redshift:DescribeClusterSecurityGroups",
        "redshift:DescribeClusterSnapshots",
        "redshift:DescribeClusterSubnetGroups",
        "redshift:DescribeClusterVersions",
        "redshift:DescribeDefaultClusterParameters",
        "redshift:DescribeEventCategories",
        "redshift:DescribeEventSubscriptions",
        "redshift:DescribeHsmClientCertificates",
        "redshift:DescribeHsmConfigurations",
        "redshift:DescribeLoggingStatus",
        "redshift:DescribeOrderableClusterOptions",
```

```

        "redshift:DescribeQuery",
        "redshift:DescribeReservedNodeOfferings",
        "redshift:DescribeReservedNodes",
        "redshift:DescribeResize",
        "redshift:DescribeSavedQueries",
        "redshift:DescribeScheduledActions",
        "redshift:DescribeSnapshotCopyGrants",
        "redshift:DescribeSnapshotSchedules",
        "redshift:DescribeStorage",
        "redshift:DescribeTable",
        "redshift:DescribeTableRestoreStatus",
        "redshift:DescribeTags",
        "redshift:FetchResults",
        "redshift:GetReservedNodeExchangeOfferings"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Principal": {
        "AWS": [
            "123456789012"
        ]
    }
}
]
}

```

Esempio: policy di endpoint VPC che nega l'accesso a un cluster specificato

La seguente policy di endpoint VPC consente l'accesso completo a tutti gli account e principal. Allo stesso tempo, nega qualsiasi accesso AWS dell'account *123456789012* alle azioni eseguite sul cluster Amazon Redshift con l'ID del cluster. *my-redshift-cluster* Le altre operazioni Amazon Redshift che non supportano le autorizzazioni a livello di risorsa per i cluster sono comunque consentite. Per un elenco delle operazioni Amazon Redshift e dei tipi di risorse corrispondenti, consultare [Operazioni, risorse e chiavi di condizione per Amazon Redshift](#) nella Guida per l'utente di IAM.

```

{
  "Statement": [
    {
      "Action": "*",

```

```
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "arn:aws:redshift:us-east-1:123456789012:cluster:my-redshift-
cluster",
        "Principal": {
            "AWS": [
                "123456789012"
            ]
        }
    }
]
```

## Analisi della configurazione e delle vulnerabilità in Amazon Redshift

AWS gestisce le attività di sicurezza di base, ad esempio la protezione del sistema operativo, l'applicazione di patch ai database, la configurazione dei firewall e il ripristino di emergenza (DR). Queste procedure sono state riviste e certificate da terze parti certificate. Per ulteriori informazioni, consultare [Convalida della conformità per Amazon Redshift](#), [Modello di responsabilità condivisa](#) e [Best practice per sicurezza, identità e conformità](#).

Amazon Redshift applica automaticamente aggiornamenti e patch al data warehouse, consentendo di concentrarsi sull'applicazione anziché sulla sua amministrazione. Le patch e gli aggiornamenti vengono applicati durante una finestra di manutenzione configurabile. Per ulteriori informazioni, consulta [Finestre di manutenzione](#).

Il query editor v2 di Amazon Redshift è un'applicazione gestita da AWS. Tutte le patch e gli aggiornamenti vengono applicati da AWS in base alle esigenze.

# Attività di rete

È possibile eseguire attività di rete come personalizzare la connessione a un database Redshift. Puoi anche eseguire attività relative al DNS, come la configurazione di un nome di dominio personalizzato. Queste attività di configurazione sono disponibili se disponi di un cluster con provisioning di Amazon Redshift o se utilizzi un gruppo di lavoro Serverless Amazon Redshift.

## Argomenti

- [Utilizzo di un nome di dominio personalizzato per le connessioni client](#)
- [Utilizzo degli endpoint VPC gestiti da RedShift](#)
- [Routing VPC avanzato in Amazon Redshift](#)

## Utilizzo di un nome di dominio personalizzato per le connessioni client

Puoi creare un nome di dominio personalizzato, noto anche come URL personalizzato, per il cluster Amazon Redshift e il gruppo di lavoro Amazon Redshift serverless. È un record easy-to-read DNS che indirizza le connessioni client SQL al tuo endpoint. Puoi configurarlo in qualsiasi momento per un cluster o un gruppo di lavoro esistente. Fornisce diversi vantaggi:

- Il nome di dominio personalizzato è una stringa più semplice dell'URL predefinito che in genere include il nome del cluster o il nome del gruppo di lavoro e la regione. È più facile da richiamare e utilizzare.
- Puoi indirizzare rapidamente il traffico verso un nuovo cluster o un nuovo gruppo di lavoro, ad esempio in caso di failover. In questo modo i client non devono apportare modifiche alla configurazione quando si riconnettono. Le connessioni possono essere reindirizzate centralmente, con interruzioni minime.
- È possibile evitare di condividere informazioni private come il nome di un server in un URL di connessione. Puoi nascondere in un URL personalizzato.

Quando configuri un nome di dominio personalizzato, utilizzando un CNAME, Amazon Redshift non prevede costi aggiuntivi. Potresti ricevere una fattura dal tuo provider DNS per un nome di dominio, se ne crei uno nuovo, ma questo costo è in genere basso. Per ulteriori informazioni, consulta l'argomento relativo alla [creazione di un nome di dominio personalizzato](#).

## Sicurezza per un nome di dominio personalizzato

Amazon Redshift o Amazon Redshift serverless richiede un certificato SSL (Secure Sockets Layer) convalidato per un endpoint personalizzato per proteggere le comunicazioni e verificare la proprietà del nome di dominio. Puoi utilizzare il tuo AWS Certificate Manager account con un AWS KMS key per una gestione sicura dei certificati. La convalida della sicurezza include la verifica completa del nome host (`sslmode=verify-full`).

### Rinnovo di un certificato

I rinnovi dei certificati sono gestiti da Amazon Redshift solo quando scegli la convalida DNS anziché la convalida via e-mail. Se utilizzi la convalida via e-mail, puoi utilizzare il certificato, ma è necessario effettuare personalmente il rinnovo prima della scadenza. Consigliamo di scegliere la convalida DNS per il certificato. Puoi monitorare le date di scadenza dei certificati importati in AWS Certificate Manager.

## Configurazione di un nome di dominio personalizzato

La configurazione del nome di dominio personalizzato include diverse attività, tra cui la registrazione del nome di dominio nel provider DNS e la creazione di un certificato. Dopo aver eseguito queste operazioni, configuri il nome di dominio personalizzato nella console Amazon Redshift o nella console Amazon Redshift Serverless oppure configuralo con i comandi. AWS CLI Le diverse fasi vengono approfondite nelle sezioni seguenti.

### Registrazione di un nome di dominio e selezione di un certificato

Devi disporre di un nome di dominio Internet registrato per configurare un nome di dominio personalizzato in Amazon Redshift. Puoi registrare un dominio Internet usando Route 53 oppure un provider di registrazione di dominio di terze parti. Queste attività vengono eseguite all'esterno della console Amazon Redshift. Un dominio registrato è un prerequisito per completare le procedure rimanenti per la creazione di un dominio personalizzato.

#### Note

Se utilizzi un cluster con provisioning, prima di eseguire i passaggi per configurare il nome di dominio personalizzato, è necessario abilitarne il trasferimento. Per ulteriori informazioni, consulta [Trasferimento del cluster](#). Questo passaggio non è necessario per Amazon Redshift serverless.

Il nome di dominio personalizzato include in genere il dominio root e un sottodominio, ad esempio `mycluster.example.com`. Per configurarlo, esegui la procedura seguente:

Crea una voce DNS CNAME per il nome di dominio personalizzato

1. Registra un dominio root, ad esempio `example.com`. Facoltativamente, puoi utilizzare un dominio esistente. Il nome personalizzato può essere limitato da restrizioni su caratteri particolari o da altre convalide dei nomi. Per ulteriori informazioni sulla registrazione di un dominio, con Route 53, consulta [Registering a new domain](#) (Registrazione di un nuovo dominio).
2. Aggiungi un record DNS CNAME che indirizzi il nome di dominio personalizzato all'endpoint Redshift per il cluster o il gruppo di lavoro. L'endpoint è disponibile nelle proprietà del cluster o del gruppo di lavoro nella console Redshift o nella console Amazon Redshift Serverless. Copia l'URL JDBC disponibile nelle proprietà del cluster o del gruppo di lavoro in Informazioni generali. Gli URL hanno il seguente formato:
  - Per un cluster Amazon Redshift: `redshift-cluster-sample.abc123456.us-east-1.redshift.amazonaws.com`
  - Per un gruppo di lavoro Amazon Redshift serverless: `endpoint-name.012345678901.us-east-1-dev.redshift-serverless-dev.amazonaws.com`

Se l'URL include un prefisso JDBC, rimuovilo.

#### Note

I record DNS sono soggetti a disponibilità, poiché ogni nome deve essere univoco e disponibile per l'uso all'interno dell'organizzazione.

## Limitazioni

Sono previste un paio di restrizioni relative alla creazione di record CNAME per un dominio personalizzato:

- La creazione di più nomi di dominio personalizzato per lo stesso cluster con provisioning o lo stesso gruppo di lavoro Amazon Redshift serverless non è supportata. Puoi associare un solo record CNAME.
- L'associazione di un record CNAME a più di un cluster o gruppo di lavoro non è supportata. Il record CNAME di ogni risorsa Redshift deve essere univoco.

Dopo aver registrato il dominio e creato il record CNAME, selezioni un certificato nuovo o esistente. Esegui questo passaggio utilizzando: AWS Certificate Manager

Richiesta di un certificato fornito da ACM per un nome di dominio

1. Accedi AWS Management Console e apri la console ACM all'[indirizzo https://console.aws.amazon.com/acm/](https://console.aws.amazon.com/acm/).
2. Scegli Request a certificate (Richiedi un certificato).
3. Immetti il nome del dominio personalizzato nel campo Nome dominio.

#### Note

Puoi specificare molti prefissi, oltre al dominio del certificato, per utilizzare un singolo certificato per più record di dominio personalizzati. Per maggiore chiarezza, puoi utilizzare record aggiuntivi come `one.example.com` e `two.example.com` oppure un record DNS jolly come `*.example.com` con lo stesso certificato.

4. Seleziona Review and request (Riconsulta e richiedi).
5. Seleziona Confirm and request (Conferma e richiedi).
6. Per una richiesta valida, un proprietario registrato del dominio Internet deve accettare la richiesta prima che ACM emetta il certificato. Assicurati che lo stato appaia come Emesso nella console ACM, al termine delle fasi.

Ti consigliamo di creare un [certificato DNS convalidato](#) che soddisfi l'idoneità per il rinnovo gestito, disponibile con AWS Certificate Manager. Rinnovo gestito significa che ACM rinnova automaticamente i certificati o ti invia avvisi tramite e-mail quando si avvicina la scadenza. Per ulteriori informazioni, consulta [Rinnovo gestito per i certificati ACM](#).

## Creazione del dominio personalizzato

Puoi utilizzare la console Amazon Redshift o Amazon Redshift serverless per creare l'URL del dominio personalizzato. Se non l'hai configurata, la proprietà Nome dominio personalizzato viene visualizzata come un trattino (-) in Informazioni generali. Dopo aver creato il record CNAME e il certificato, associ il nome del dominio personalizzato al cluster o al gruppo di lavoro.

Per creare un'associazione di dominio personalizzato, sono necessarie le seguenti autorizzazioni IAM:

- `redshift:CreateCustomDomainAssociation`: è possibile limitare l'autorizzazione a un cluster specifico aggiungendo il relativo ARN.
- `redshiftServerless:CreateCustomDomainAssociation`: è possibile limitare l'autorizzazione a un gruppo di lavoro specifico aggiungendo il relativo ARN.
- `acm:DescribeCertificate`

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

Puoi assegnare il nome di dominio personalizzato eseguendo la procedura seguente.

1. Scegli il cluster nella console Redshift o il gruppo di lavoro nella console Amazon Redshift serverless, quindi seleziona Crea nome dominio personalizzato nel menu Operazioni. Viene visualizzata una finestra di dialogo.
2. Inserisci il nome di dominio personalizzato.
3. Seleziona il modulo ARN AWS Certificate Manager per il certificato ACM. Confermare le modifiche. In base alle indicazioni fornite nei passaggi seguiti per creare il certificato, ti consigliamo di scegliere un certificato convalidato DNS idoneo al rinnovo gestito. AWS Certificate Manager
4. Verifica nelle proprietà del cluster che Nome dominio personalizzato e ARN del certificato del nome dominio personalizzato siano compilati con le tue immissioni. È inoltre elencata la Data di scadenza del certificato del dominio personalizzato.

Dopo la configurazione del dominio personalizzato, l'utilizzo di `sslmode=verify-full` funziona solo per il nuovo dominio personalizzato. Non funziona con l'endpoint predefinito. Ma puoi comunque connetterti all'endpoint predefinito utilizzando altre modalità SSL, ad esempio `sslmode=verify-ca`.

#### Note

Ricordiamo che il [trasferimento del cluster non è un prerequisito per la](#) configurazione di funzionalità di rete aggiuntive di Redshift. Non è necessario attivarlo per abilitare le seguenti attività:

- Connessione da un VPC multiaccount o interregionale a Redshift: puoi connetterti da un cloud privato AWS virtuale (VPC) a un altro che contiene un database Redshift. In tal modo

semplifichi la gestione, ad esempio, dell'accesso dei client da account o VPC diversi, senza dover fornire l'accesso VPC locale alle identità che si connettono al database. Per ulteriori informazioni, consulta [Connessione ad Amazon Redshift serverless da un endpoint VPC Redshift di un altro account o un'altra regione](#).

- Configurazione di un nome di dominio personalizzato: è possibile creare un nome di dominio personalizzato, come descritto in questo argomento, per rendere il nome dell'endpoint più pertinente e semplice.

Ridenominazione di un cluster a cui è assegnato un dominio personalizzato mediante la console

#### Note

Questa serie di passaggi non si applica a un gruppo di lavoro Amazon Redshift serverless. Non è possibile cambiare il nome del gruppo di lavoro.

Per rinominare un cluster con un nome di dominio personalizzato, è richiesta l'autorizzazione IAM `acm:DescribeCertificate`.

1. Vai alla console Amazon Redshift e scegli il cluster di cui desideri modificare il nome. Scegli Modifica per modificare le proprietà del cluster.
2. Modifica l'Identificatore del cluster. Puoi anche modificare altre proprietà del cluster. Selezionare quindi Save changes (Salva modifiche).
3. Dopo aver rinominato il cluster, devi aggiornare il record DNS per modificare la voce CNAME del dominio personalizzato in modo che punti all'endpoint Amazon Redshift aggiornato.

Descrizione delle associazioni di dominio personalizzate utilizzando i comandi della CLI

Usa i comandi descritti in questa sezione per ottenere l'elenco dei nomi di dominio personalizzato associati a uno specifico cluster con provisioning o a uno specifico gruppo di lavoro Amazon Redshift serverless.

Sono necessarie le seguenti autorizzazioni:

- Per un cluster con provisioning: `redshift:DescribeCustomDomainAssociations`
- Per un gruppo di lavoro Amazon Redshift serverless: `redshiftServerless:ListCnameAssociations`

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

Il seguente comando di esempio consente di elencare i nomi di dominio personalizzato per un cluster Amazon Redshift:

```
aws redshift describe-custom-domain-associations --custom-domain-name customdomainname
```

Puoi eseguire questo comando quando hai abilitato un nome di dominio personalizzato per determinare i nomi di dominio personalizzato associati al cluster. Per ulteriori informazioni sul comando CLI per la descrizione delle associazioni di dominio personalizzate, vedere [describe-custom-domain-associations](#)

Analogamente, i seguenti comandi di esempio consentono di elencare i nomi di dominio personalizzato per un determinato gruppo di lavoro Amazon Redshift serverless. Esistono diversi modi per farlo. Puoi fornire solo il nome di dominio personalizzato:

```
aws redshift-serverless list-custom-domain-associations --custom-domain-name customdomainname
```

Puoi anche ottenere le associazioni fornendo solo l'ARN del certificato:

```
aws redshift-serverless list-custom-domain-associations --custom-domain-certificate-arn certificatearn
```

Puoi eseguire questi comandi quando hai abilitato un nome di dominio personalizzato per determinare i nomi di dominio personalizzato associati al gruppo di lavoro. È inoltre possibile eseguire un comando per ottenere le proprietà di un'associazione di dominio personalizzato. A tale scopo, è necessario fornire il nome di dominio personalizzato e il nome del gruppo di lavoro come parametri. Il comando restituisce l'ARN del certificato, il nome del gruppo di lavoro e l'ora di scadenza del certificato del dominio personalizzato:

```
aws redshift-serverless get-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

Per ulteriori informazioni sui comandi di riferimento della CLI disponibili per Amazon Redshift serverless, consulta [redshift-serverless](#).

## Associazione del dominio personalizzato a un certificato diverso

Per modificare l'associazione del certificato per un nome di dominio personalizzato, sono necessarie le seguenti autorizzazioni IAM:

- `redshift:ModifyCustomDomainAssociation`
- `acm:DescribeCertificate`

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

Utilizza il comando seguente per associare il dominio personalizzato a un certificato diverso. Gli argomenti `--custom-domain-name` e `custom-domain-certificate-arn` sono obbligatori. L'ARN del nuovo certificato deve essere diverso dall'ARN esistente.

```
aws redshift modify-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

L'esempio seguente mostra come associare il dominio personalizzato a un certificato diverso per un gruppo di lavoro Amazon Redshift serverless.

```
aws redshift-serverless modify-custom-domain-association --workgroup-name redshiftworkgroup --custom-domain-name customdomainname --custom-domain-certificate-arn certificatearn
```

Si verifica un ritardo massimo di 30 secondi prima di poter eseguire la connessione al cluster. Parte del ritardo si verifica quando il cluster Amazon Redshift aggiorna le sue proprietà e si verifica un ulteriore ritardo con l'aggiornamento del DNS. Per ulteriori informazioni sull'API e su ciascuna impostazione di proprietà, vedere. [ModifyCustomDomainAssociation](#)

## Eliminazione del dominio personalizzato

Per eliminare il nome di dominio personalizzato, l'utente deve disporre delle autorizzazioni per le seguenti operazioni:

- Per un cluster con provisioning: `redshift>DeleteCustomDomainAssociation`
- Per un gruppo di lavoro Amazon Redshift serverless:  
`redshiftServerless>DeleteCustomDomainAssociation`

## Con la console

È possibile eliminare il nome di dominio personalizzato selezionando il pulsante Operazioni e scegliendo Elimina nome di dominio personalizzato. Dopo aver eseguito questa operazione, puoi connetterti al server aggiornando gli strumenti per utilizzare gli endpoint elencati nella console.

## Con un comando della CLI

L'esempio seguente mostra come eliminare il nome di dominio personalizzato. L'operazione di eliminazione ti richiede di fornire il nome di dominio personalizzato esistente per il cluster.

```
aws redshift delete-custom-domain-association --cluster-id redshiftcluster --custom-domain-name customdomainname
```

L'esempio seguente mostra come eliminare il nome di dominio personalizzato per un gruppo di lavoro Amazon Redshift serverless. Il nome di dominio personalizzato è un parametro obbligatorio.

```
aws redshift-serverless delete-custom-domain-association --workgroup-name workgroupname --custom-domain-name customdomainname
```

Per ulteriori informazioni, vedere [DeleteCustomDomainAssociation](#).

## Connessione al cluster o al gruppo di lavoro con un nome di dominio personalizzato utilizzando un client SQL

Per connettersi con un nome di dominio personalizzato, sono necessarie le seguenti autorizzazioni IAM per un cluster con provisioning: `redshift:DescribeCustomDomainAssociations`. Per Amazon Redshift serverless, non è necessario aggiungere autorizzazioni.

Come best practice, consigliamo di collegare le policy di autorizzazioni a un ruolo IAM, che quindi viene assegnato a utenti e gruppi secondo le necessità. Per ulteriori informazioni, consulta [Identity and access management in Amazon Redshift](#).

Dopo aver completato i passaggi per creare il CNAME e averlo assegnato al cluster o al gruppo di lavoro nella console, puoi fornire l'URL personalizzato nelle proprietà della connessione del client SQL. Tieni presente che può verificarsi un ritardo nella propagazione del DNS immediatamente dopo la creazione di un record CNAME.

1. Apertura di un client SQL. Ad esempio, puoi utilizzare SQL/Workbench J. Apri le proprietà di una connessione e aggiungi il nome del dominio personalizzato per la stringa di connessione. Ad

esempio, `jdbc:redshift://mycluster.example.com:5439/dev?sslmode=verify-full`. In questo esempio, `dev` specifica il database predefinito.

2. Aggiungi il Nome utente e la Password per l'utente del database.
3. Esegui il test della connessione. La capacità di eseguire query sulle risorse del database, come tabelle specifiche, può variare in base alle autorizzazioni concesse all'utente del database o ai ruoli assegnati nel database Amazon Redshift.

Tieni presente che potresti dover configurare il cluster o il gruppo di lavoro in modo che sia accessibile pubblicamente per connetterti ad esso quando si trova in un VPC. È possibile modificare questa impostazione nelle proprietà di rete.

#### Note

Le connessioni a un nome di dominio personalizzato sono supportate con i driver JDBC e Python. Le connessioni ODBC non sono supportate.

## Utilizzo degli endpoint VPC gestiti da RedShift

Per impostazione predefinita, un cluster Amazon Redshift o un gruppo di lavoro Serverless Amazon Redshift viene fornito in un cloud privato virtuale (VPC). È possibile accedere al VPC da un altro VPC o sottorete quando si consente l'accesso pubblico o si configura un gateway Internet, un dispositivo NAT o una AWS Direct Connect connessione per indirizzare il traffico verso di esso. Puoi anche accedere a un cluster o a un gruppo di lavoro configurando un endpoint VPC gestito da Redshift (con tecnologia). AWS PrivateLink

Puoi configurare un endpoint VPC gestito da Redshift come connessione privata tra un VPC che contiene un cluster o un gruppo di lavoro e un VPC in cui è in esecuzione uno strumento client. Se il cluster o il gruppo di lavoro si trova in un altro account, il proprietario dell'account (concedente) deve concedere l'accesso all'account connesso (beneficiario). Con questo approccio, è possibile accedere al data warehouse senza utilizzare un indirizzo IP pubblico o instradare il traffico su Internet.

Questi sono i motivi più comuni per consentire l'accesso utilizzando un endpoint VPC gestito da Redshift:

- AWS l'account A desidera consentire a un VPC AWS dell'account B di accedere a un cluster o gruppo di lavoro.

- AWS l'account A desidera consentire a un VPC che si trova anche nell' AWS account A di accedere a un cluster o gruppo di lavoro.
- AWS l'account A desidera consentire a una sottorete diversa nel VPC all' AWS interno dell'account A di accedere a un cluster o gruppo di lavoro.

Il flusso di lavoro per configurare un endpoint VPC gestito da Redshift per accedere a un cluster o gruppo di lavoro in un altro account è il seguente:

1. L'account proprietario concede l'autorizzazione di accesso a un altro account e specifica l'ID dell' AWS account e l'identificatore VPC (o tutti i VPC) del beneficiario.
2. All'account beneficiario viene notificato che dispone dell'autorizzazione per creare un endpoint VPC gestito da RedShift.
3. L'account beneficiario crea un endpoint VPC gestito da RedShift.
4. L'account beneficiario accede al cluster o al gruppo di lavoro dell'account proprietario utilizzando l'endpoint VPC gestito da Redshift.

Puoi farlo utilizzando la console Amazon Redshift AWS CLI, o l'API Amazon Redshift.

## Considerazioni sull'utilizzo degli endpoint VPC gestiti da RedShift

### Note

Per creare o modificare endpoint VPC gestiti da Redshift, è necessaria l'`ec2:CreateVpcEndpoint` autorizzazione `ec2:ModifyVpcEndpoint` o nella policy IAM, oltre alle altre autorizzazioni specificate nella policy gestita. `AWS AmazonRedshiftFullAccess`

Quando si utilizzano gli endpoint VPC gestiti da RedShift, tenere presente quanto riportato di seguito:

- Assicurarsi che il cluster a cui accedere sia un tipo di nodo RA3. Un gruppo di lavoro Serverless Amazon Redshift funziona anche per questo.
- Per i cluster con provisioning, assicurati che il cluster sia abilitato per il trasferimento del cluster o per Multi-AZ. Per informazioni sui requisiti per attivare la rilocazione del cluster, consultare [Trasferimento del cluster](#). Per informazioni sull'attivazione di Multi-AZ, vedere. [Configurazione di implementazioni multi-AZ durante la creazione di un nuovo cluster](#)

- Assicurati che il cluster o il gruppo di lavoro a cui accedere tramite il relativo gruppo di sicurezza sia disponibile negli intervalli di porte validi 5431-5455 e 8191-8215. Il valore predefinito è 5439.
- È possibile modificare i gruppi di sicurezza VPC associati a un endpoint VPC gestito da RedShift esistente. Per modificare altre impostazioni, eliminare l'endpoint VPC gestito da RedShift corrente e crearne uno nuovo.
- Il numero di endpoint VPC gestiti da RedShift che è possibile creare è limitato alla quota di endpoint VPC.
- Gli endpoint VPC gestiti da RedShift non sono accessibili da Internet. Un endpoint VPC gestito da Redshift è accessibile solo all'interno del VPC in cui viene fornito l'endpoint o da qualsiasi VPC collegato al VPC in cui l'endpoint viene fornito come consentito dalle tabelle di routing e dai gruppi di sicurezza.
- Non è possibile utilizzare la console Amazon VPC per gestire endpoint VPC gestiti da RedShift.
- Quando crei un endpoint VPC gestito da Redshift per un cluster con provisioning, il VPC scelto deve avere un gruppo di sottoreti. Per creare un gruppo di sottoreti, consulta [Gestione di gruppi di sottoreti del cluster mediante la console](#)
- Se una zona di disponibilità è inattiva, Amazon Redshift non crea una nuova interfaccia di rete elastica in un'altra zona di disponibilità. In questo caso potrebbe essere necessario creare un nuovo endpoint.

Per informazioni sulle quote e sui vincoli di denominazione, consultare [Quote e limiti in Amazon Redshift](#).

Per informazioni sui prezzi, consultare [Prezzi di AWS PrivateLink](#).

## Gestione degli endpoint VPC gestiti da Redshift tramite la console

È possibile configurare l'uso degli endpoint VPC gestiti da RedShift utilizzando la console Amazon Redshift.

### Concessione dell'accesso per

Se il VPC a cui desideri accedere al tuo cluster o gruppo di lavoro si trova in un altro AWS account, assicurati di autorizzarlo dall'account del proprietario (del concedente).

Per consentire a un VPC di un altro AWS account di accedere al tuo cluster o gruppo di lavoro

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster). Per Amazon Redshift Serverless, scegli la dashboard Serverless.
3. Per un cluster a cui desideri consentire l'accesso, visualizza i dettagli scegliendo il nome del cluster. Scegliere la scheda Proprietà del cluster.

La sezione Account concessi visualizza gli account e i VPC corrispondenti che hanno accesso al cluster. Per un gruppo di lavoro Serverless Amazon Redshift, scegli il gruppo di lavoro. Gli account concessi sono disponibili nella scheda Accesso ai dati.

4. Scegliere Concedi accesso per visualizzare un modulo in cui immettere le informazioni del beneficiario per aggiungere un account.
5. Per ID account AWS , inserire l'ID dell'account a cui si sta concedendo l'accesso. È possibile concedere l'accesso a VPC specifici o a tutti i VPC nell'account specificato.
6. Scegliere Concedi accesso per concedere l'accesso.

## Creazione di un endpoint VPC gestito da RedShift

Se possiedi un cluster o un gruppo di lavoro o ti è stato concesso l'accesso per gestirlo, puoi creare un endpoint VPC gestito da Redshift per esso.

Come creare un endpoint VPC gestito da RedShift

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel menu di navigazione, scegliere Configurations (Configurazioni).

La pagina Configurazioni riporta gli endpoint VPC gestiti da RedShift che sono stati creati. Per visualizzare i dettagli di un endpoint, sceglierne il nome. Per Amazon Redshift Serverless, gli endpoint VPC si trovano nella scheda Accesso ai dati, quando scegli il gruppo di lavoro.

3. Scegliere Crea endpoint per visualizzare un modulo per immettere informazioni sull'endpoint da aggiungere.
4. Inserisci i valori per il nome dell'endpoint, l'ID dell'AWS account a 12 cifre, il cloud privato virtuale (VPC) in cui si trova l'endpoint, la sottorete e il gruppo di sicurezza VPC.

La sottorete in Subnet definisce le sottoreti e gli indirizzi IP in cui Amazon Redshift distribuisce l'endpoint. Amazon Redshift sceglie una sottorete con indirizzi IP disponibili per l'interfaccia di rete associata all'endpoint.

Le regole del gruppo di sicurezza nel gruppo di sicurezza VPC definiscono le porte, i protocolli e le fonti per il traffico in entrata che stai autorizzando per il tuo endpoint. Consenti l'accesso alla porta selezionata tramite il gruppo di sicurezza o l'intervallo CIDR in cui vengono eseguiti i tuoi carichi di lavoro.

5. Per creare l'endpoint VPC, scegliere Crea endpoint.

Dopo aver creato l'endpoint, puoi accedere al cluster o al gruppo di lavoro tramite l'URL mostrato in Endpoint URL nelle impostazioni di configurazione per l'endpoint VPC gestito da Redshift.

## Gestione degli endpoint VPC gestiti da Redshift utilizzando AWS CLI

È possibile utilizzare le seguenti operazioni della CLI di Amazon Redshift per lavorare con gli endpoint VPC gestiti da RedShift. Per ulteriori informazioni, consultare la sezione relativa alle informazioni di riferimento ai comandi della AWS CLI .

- [authorize-endpoint-access](#)
- [revoke-endpoint-access](#)
- [create-endpoint-access](#)
- [modify-endpoint-access](#)
- [delete-endpoint-access](#)
- [describe-endpoint-access](#)
- [describe-endpoint-authorization](#)

## Gestione degli endpoint VPC gestiti da RedShift utilizzando le operazioni API Amazon Redshift

È possibile utilizzare le seguenti operazioni API di Amazon Redshift per lavorare con gli endpoint VPC gestiti da RedShift. Per ulteriori informazioni, consultare la Documentazione di riferimento delle API di Amazon Redshift.

- [AuthorizeEndpointAccess](#)

- [RevokeEndpointAccess](#)
- [CreateEndpointAccess](#)
- [ModifyEndpointAccess](#)
- [DeleteEndpointAccess](#)
- [DescribeEndpointAccess](#)
- [DescribeEndpointAuthorization](#)

## Gestione degli endpoint VPC gestiti da Redshift tramite AWS CloudFormation

Per informazioni sul tipo di AWS CloudFormation risorsa da utilizzare per creare un endpoint VPC gestito da Redshift, [AWS::Redshift::EndpointAccess](#) consulta la Guida per AWS CloudFormation l'utente. AWS CloudFormation

## Routing VPC avanzato in Amazon Redshift

Quando si utilizza il routing VPC avanzato di Amazon Redshift, Amazon Redshift forza il passaggio di tutto il traffico dei comandi [COPY](#) e [UNLOAD](#) tra il cluster e i repository di dati attraverso il Virtual Private Cloud (VPC) basato sul servizio Amazon VPC. Utilizzando il routing VPC avanzato, è possibile utilizzare funzionalità standard del VPC, come [gruppi di sicurezza VPC](#), [liste di controllo accessi \(ACL\) di rete](#), [endpoint VPC](#), [policy di endpoint VPC](#), [gateway Internet](#) e server [Domain Name System \(DNS\)](#), come descritto nella Guida per l'utente di Amazon VPC. Queste funzionalità vengono utilizzate per gestire in modo rigoroso il flusso di dati tra il cluster Amazon Redshift e altre risorse. Quando si utilizza il routing VPC avanzato per instradare il traffico nel VPC, è possibile usare anche i [log di flusso VPC](#) per monitorare il traffico di COPY e UNLOAD.

I cluster Amazon Redshift e i gruppi di lavoro Amazon Redshift serverless supportano il routing VPC avanzato. Non è possibile utilizzare il routing VPC avanzato con Amazon Redshift Spectrum. Per ulteriori informazioni, consulta [Redshift Spectrum e il routing VPC avanzato](#).

Se il routing VPC avanzato non è attivato, Amazon Redshift indirizza il traffico attraverso Internet, incluso il traffico verso altri servizi all'interno della rete. AWS

### Important

Poiché il routing VPC avanzato influisce sul modo in cui Amazon Redshift accede alle altre risorse, se il VPC non viene configurato correttamente i comandi COPY e UNLOAD

potrebbero avere esito negativo. È necessario creare un percorso di rete tra il VPC del cluster e le risorse di dati, come descritto di seguito.

Quando si esegue un comando COPY o UNLOAD in un cluster in cui è attivato il routing VPC avanzato, il VPC instrada il traffico verso la risorsa specificata usando il percorso di rete più restrittivo o più specifico disponibile.

Puoi ad esempio configurare i percorsi seguenti nel VPC:

- **Endpoint VPC:** per il traffico verso un bucket Amazon S3 nella stessa AWS regione del cluster, puoi creare un endpoint VPC per indirizzare il traffico direttamente al bucket. Quando si utilizzano gli endpoint VPC, è possibile collegare una policy dell'endpoint per gestire l'accesso ad Amazon S3. Per ulteriori informazioni sull'uso di endpoint con Amazon Redshift, consultare [Uso di endpoint VPC](#). Se utilizzi Lake Formation, puoi trovare ulteriori informazioni su come stabilire una connessione privata tra il tuo VPC e AWS Lake Formation at [AWS Lake Formation e interfacciare gli endpoint VPC](#) ().AWS PrivateLink

#### Note

Quando utilizzi gli endpoint VPC di Redshift con gli endpoint VPC Gateway di Amazon S3, devi abilitare il routing VPC avanzato in Redshift. Per ulteriori informazioni, consulta [Endpoint gateway per Amazon S3](#).

- **Gateway NAT:** puoi connetterti a un bucket Amazon S3 in AWS un'altra regione e puoi connetterti a un altro servizio all'interno della rete. AWS Puoi anche accedere a un'istanza host all'esterno della rete. AWS A tal fine, configurare un [gateway NAT \(network address translation\)](#), come descritto nella Guida per l'utente di Amazon VPC.
- **Gateway Internet:** per connettersi ai servizi AWS al di fuori del VPC, è possibile collegare un [gateway Internet](#) alla sottorete VPC, come descritto nella Guida per l'utente di Amazon VPC. Per usare un Internet gateway, il cluster deve avere un indirizzo IP pubblico per permettere la comunicazione di altri servizi con il cluster.

Per ulteriori informazioni, consultare [Endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

L'uso del routing VPC avanzato non comporta costi aggiuntivi. Potrebbero essere applicati costi aggiuntivi di trasferimento dei dati per alcune operazioni. Queste includono operazioni come

UNLOAD su Amazon S3 in una AWS regione diversa. COPY da Amazon EMR o Secure Shell (SSH) con indirizzi IP pubblici. Per ulteriori informazioni sui prezzi, consultare [Prezzi di Amazon EC2](#).

## Argomenti

- [Uso di endpoint VPC](#)
- [Routing VPC avanzato](#)
- [Redshift Spectrum e il routing VPC avanzato](#)

## Uso di endpoint VPC

È possibile usare un endpoint VPC per creare una connessione gestita tra il cluster Amazon Redshift in un VPC e Amazon Simple Storage Service (Amazon S3). In tal caso, il traffico dei comandi COPY e UNLOAD tra il database e i dati in Amazon S3 rimane nell'Amazon VPC. Puoi collegare una policy a un endpoint per gestire in modo più rigoroso l'accesso ai dati. Ad esempio è possibile aggiungere una policy all'endpoint VPC che permette di scaricare i dati solo in un bucket Amazon S3 specifico nel proprio account.

Per utilizzare gli endpoint VPC, crea un endpoint VPC per il VPC in cui si trova il data warehouse e attiva il routing VPC avanzato per il cluster. È possibile attivare il routing VPC avanzato al momento della creazione del cluster o del gruppo di lavoro oppure modificare un cluster o un gruppo di lavoro in un VPC per l'uso del routing VPC avanzato.

Un endpoint VPC usa tabelle di instradamento per controllare il routing del traffico tra un cluster o un gruppo di lavoro nel VPC ed Amazon S3. Tutti i cluster e i gruppi di lavoro nelle sottoreti associate alle tabelle di instradamento specificate utilizzano automaticamente tale endpoint per accedere al servizio.

Il VPC utilizza la route più specifica, o più restrittiva, corrispondente al traffico per determinare come instradare il traffico. Ad esempio, si supponga di disporre di una route nella tabella di routing per tutto il traffico Internet (0.0.0.0/0) che fa riferimento a un gateway Internet e un endpoint Amazon S3. In tal caso, la route dell'endpoint ha la precedenza su tutto il traffico destinato ad Amazon S3. Questo perché l'intervallo di indirizzi IP per il servizio Amazon S3 è più specifico di 0.0.0.0/0. In questo esempio, tutto il resto del traffico Internet passa nel gateway Internet, incluso il traffico destinato ai bucket Amazon S3 in altre Regioni AWS.

Per ulteriori informazioni sulla creazione degli endpoint, consulta [Creazione di un Endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

Le policy degli endpoint possono essere utilizzate per controllare l'accesso dal cluster o dal gruppo di lavoro ai bucket Amazon S3 contenenti i file di dati. Per un controllo più specifico, puoi collegare una policy dell'endpoint personalizzata. Per ulteriori informazioni, consulta la sezione [Controllo dell'accesso ai servizi con policy di endpoint](#) nella Guida di AWS PrivateLink .

### Note

AWS Database Migration Service (AWS DMS) è un servizio cloud che consente di migrare database relazionali, data warehouse e altri tipi di archivi dati. Può connettersi a qualsiasi database di AWS origine o di destinazione, incluso un database Amazon Redshift abilitato per VPC, con alcune restrizioni di configurazione. Il supporto degli endpoint Amazon VPC semplifica il mantenimento della sicurezza di end-to-end rete AWS DMS per le attività di replica. Per ulteriori informazioni sull'utilizzo di Redshift con AWS DMS, consulta [Configurazione degli endpoint VPC AWS DMS come endpoint di origine e di destinazione](#) nella Guida per l'utente AWS Database Migration Service

L'uso di endpoint non comporta costi aggiuntivi. Vengono applicati i costi standard per il trasferimento dei dati e l'utilizzo delle risorse. Per ulteriori informazioni sui prezzi, consultare [Prezzi di Amazon EC2](#).

## Routing VPC avanzato

Puoi attivare il routing VPC avanzato quando crei o modifichi un cluster e quando crei o modifichi un gruppo di lavoro Amazon Redshift serverless.

Per l'uso del routing VPC avanzato per un cluster, il cluster deve soddisfare i requisiti e i vincoli seguenti:

- Il cluster deve trovarsi in un VPC.

Se colleghi un endpoint VPC Amazon S3, il cluster utilizza l'endpoint VPC solo per accedere ai bucket Amazon S3 nella stessa regione. AWS Per accedere ai bucket in un'altra AWS regione (senza utilizzare l'endpoint VPC) o per accedere ad AWS altri servizi, rendi il cluster accessibile al pubblico o utilizza [un gateway NAT \(Network Address Translation\)](#). Per ulteriori informazioni, consulta [Creazione di un cluster in un VPC](#).

- È necessario abilitare la risoluzione DNS (Domain Name Service) nel VPC. In alternativa, se si utilizza un server DNS, assicurarsi che le richieste DNS ad Amazon S3 vengano risolte

correttamente negli indirizzi IP gestiti da AWS. Per ulteriori informazioni, consultare [Utilizzo del DNS con i VPC](#) nella Guida per l'utente di Amazon VPC.

- I nomi host DNS devono essere abilitati nel VPC. Gli hostname DNS sono abilitati per impostazione predefinita.
- Le policy dell'endpoint VPC devono consentire l'accesso ai bucket Amazon S3 usati con le chiamate a COPY, UNLOAD o CREATE LIBRARY in Amazon Redshift, incluso l'accesso ai file manifest interessati. Per il comando COPY dagli host remoti, le policy dell'endpoint devono permettere l'accesso a ogni computer host. Per ulteriori informazioni, consultare [Autorizzazioni IAM per COPY, UNLOAD e CREATE LIBRARY](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

Per creare un cluster con routing VPC avanzato

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegli Provisioned clusters dashboard (Pannello di controllo del cluster con provisioning), quindi seleziona Create cluster (Crea cluster) e inserisci le proprietà Cluster details (Dettagli cluster).
3. Per visualizzare la sezione Additional configurations (Configurazioni aggiuntive), scegli di disattivare la voce Use defaults (Utilizza le impostazioni predefinite).
4. Vai alla sezione Network and security (Rete e sicurezza).
5. Per attivare l'opzione Enhanced VPC routing (Routing VPC avanzato) seleziona Turn on (Attiva) per forzare l'instradamento del traffico del cluster attraverso il VPC.
6. Per creare il cluster, scegli Create cluster (Crea cluster). Potrebbero essere necessari diversi minuti prima che il cluster sia pronto per l'utilizzo.

Creazione di un gruppo di lavoro Amazon Redshift serverless con routing VPC avanzato

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Nel menu di navigazione, scegli serverless dashboard (Pannello di controllo serverless), quindi seleziona Create workgroup (Crea gruppo di lavoro) e inserisci le proprietà del gruppo di lavoro.
3. Vai alla sezione Network and security (Rete e sicurezza).

4. Seleziona Turn on enhanced VPC routing (Attiva il routing VPC avanzato) per instradare il traffico di rete attraverso il VPC.
5. Scegli Next (Avanti) e inserisci le proprietà del gruppo di lavoro fino ad arrivare a Create (Crea), la cui selezione consente di creare il gruppo di lavoro.

## Redshift Spectrum e il routing VPC avanzato

Amazon Redshift Spectrum non supporta il routing VPC avanzato con cluster con provisioning. Il routing VPC avanzato di Amazon Redshift instrada il traffico specifico tramite il VPC. Tutto il traffico tra il cluster e i bucket Amazon S3 viene forzato a passare tramite il proprio Amazon VPC. Redshift Spectrum viene eseguito su risorse AWS gestite di proprietà di Amazon Redshift. Poiché tali risorse sono esterne al VPC, Redshift Spectrum non utilizza il routing VPC avanzato.

Il traffico tra Redshift Spectrum e Amazon S3 viene instradato in modo sicuro attraverso AWS la rete privata, all'esterno del tuo VPC. Il traffico in transito viene firmato tramite il protocollo Amazon Signature Version 4 (SIGv4) e crittografato tramite HTTPS. Questo traffico è autorizzato in base al ruolo IAM che è associato al cluster Amazon Redshift. Per gestire ulteriormente il traffico di Redshift Spectrum, è possibile modificare il ruolo IAM del cluster e la policy collegata al bucket Amazon S3. Potrebbe inoltre essere necessario configurare il VPC per consentire l'accesso al cluster o ad AWS Glue Athena, come descritto di seguito.

Si noti che poiché il routing VPC avanzato influisce sul modo in cui Amazon Redshift accede alle altre risorse, se il VPC non viene configurato correttamente, le query potrebbero restituire degli errori. Per ulteriori informazioni, consulta [Routing VPC avanzato in Amazon Redshift](#), che illustra più nel dettaglio la creazione di un endpoint VPC, un gateway NAT e altre risorse di rete per indirizzare il traffico verso i bucket Amazon S3.

### Note

Amazon Redshift serverless supporta il routing VPC avanzato per le query verso tabelle esterne su Amazon S3.

## Considerazioni su quando utilizzare Amazon Redshift Spectrum

Di seguito sono riportate alcune considerazioni da tenere presenti durante l'utilizzo di Redshift Spectrum:

- [Policy di accesso al bucket](#)
- [Ruolo IAM del cluster](#)
- [Registrazione e verifica dell'accesso ad Amazon S3](#)
- [Accesso al nostro AWS Glue Amazon Athena](#)

## Policy di accesso al bucket

È possibile controllare l'accesso ai dati nei bucket Amazon S3 utilizzando una policy di bucket collegata al bucket e un ruolo IAM collegato al cluster.

Redshift Spectrum sui cluster con provisioning non può accedere ai dati archiviati nei bucket Amazon S3 che utilizzano una policy per bucket che limita l'accesso solo a specifici endpoint VPC. Utilizza invece una policy bucket che limiti l'accesso solo a principali specifici, come un account specifico o utenti specifici AWS .

Per il ruolo IAM a cui viene concesso l'accesso al bucket, utilizzare una relazione di trust che consente al ruolo di essere assegnato solo al principale di servizio Amazon Redshift. Se collegato al cluster, il ruolo può essere utilizzato solo nel contesto di Amazon Redshift e non può essere condiviso esternamente al cluster. Per ulteriori informazioni, consultare [Limitazione dell'accesso a ruoli IAM](#). È possibile utilizzare anche una policy di controllo dei servizi (SCP) per limitare ulteriormente il ruolo. Vedi [Impedire agli utenti e ai ruoli IAM di apportare modifiche specifiche, con un'eccezione per un ruolo di amministratore specificato](#) nella Guida per l'utente AWS Organizations .

### Note

Per utilizzare Redshift Spectrum, non è possibile adottare policy IAM che blocchino l'uso degli URL predefiniti di Amazon S3. Gli URL predefiniti generati da Amazon Redshift Spectrum sono validi per 1 ora in modo che Amazon Redshift abbia abbastanza tempo per caricare tutti i file dal bucket Amazon S3. Viene generato un URL predefinito univoco per ogni file scansionato da Redshift Spectrum. Per le policy bucket che includono un'`s3:signatureAgeazione`, assicurati di impostare il valore su almeno 3.600.000 millisecondi.

Il seguente esempio di bucket policy consente l'accesso al bucket specificato solo dal traffico originato da Redshift Spectrum di proprietà dell'account. AWS 123456789012

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Sid": "BucketPolicyForSpectrum",
  "Effect": "Allow",
  "Principal": {
    "AWS": ["arn:aws:iam::123456789012:role/redshift"]
  },
  "Action": ["s3:GetObject", "s3:List*"],
  "Resource": ["arn:aws:s3:::examplebucket/*"],
  "Condition": {
    "StringEquals": {
      "aws:UserAgent": "AWS Redshift/Spectrum"
    }
  }
}]
}

```

## Ruolo IAM del cluster

Il ruolo collegato al cluster deve avere una relazione di trust che gli consenta di essere assunto solo dal servizio Amazon Redshift, come illustrato di seguito.

```

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

```

È possibile aggiungere una policy al ruolo del cluster che impedisce l'accesso COPY e UNLOAD a un bucket specifico. La seguente policy consente il traffico al bucket specifico solo da Redshift Spectrum.

```

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

```

```
    "Effect": "Allow",
    "Action": ["s3:Get*", "s3:List*"],
    "Resource": "arn:aws:s3:::myBucket/*",
    "Condition": {"StringEquals": {"aws:UserAgent": "AWS Redshift/
Spectrum"}}
  }]
```

Per ulteriori informazioni, consulta [Policy IAM per Amazon Redshift Spectrum](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## Registrazione e verifica dell'accesso ad Amazon S3

Un vantaggio dell'utilizzo del routing VPC avanzato di Amazon Redshift consiste nel fatto che tutto il traffico COPY e UNLOAD è registrato nei log di flusso VPC. Il traffico originato da Redshift Spectrum ad Amazon S3 non passa attraverso il VPC, perciò non effettua l'accesso nei log di flusso VPC. Quando Redshift Spectrum accede ai dati in Amazon S3, esegue queste operazioni nel contesto dell' AWS account e dei rispettivi privilegi di ruolo. È possibile registrare e controllare l'accesso ad Amazon S3 utilizzando la registrazione degli accessi al server in AWS CloudTrail e Amazon S3.

Assicurati che gli intervalli IP S3 siano aggiunti all'elenco di indirizzi consentiti. Per ulteriori informazioni sugli intervalli IP S3 richiesti, consulta [Isolamento di rete](#).

## AWS CloudTrail Log

Per tracciare tutti gli accessi agli oggetti in Amazon S3, incluso l'accesso a Redshift Spectrum, abilita la registrazione CloudTrail per gli oggetti Amazon S3.

Puoi utilizzarlo CloudTrail per visualizzare, cercare, scaricare, archiviare, analizzare e rispondere alle attività dell'account nell'intera infrastruttura. AWS Per ulteriori informazioni, consulta [Getting Started with CloudTrail](#).

Per impostazione predefinita, CloudTrail tiene traccia solo delle azioni a livello di bucket. Per tracciare le operazioni a livello di oggetto (come GetObject), abilitare gli eventi di dati e gestione per ciascun bucket registrato.

## Registrazione degli accessi al server Amazon S3

La registrazione degli accessi al server fornisce record dettagliati per le richieste che sono effettuate a un bucket. Il log di accesso può essere utile nei controlli di accesso e di sicurezza. Per ulteriori informazioni, consultare [Come abilitare la registrazione degli accessi al server](#) nella Guida per l'utente di Amazon Simple Storage Service.

Per ulteriori informazioni, consulta il post del blog sulla AWS sicurezza [How to Use Bucket Policies and Apply Defense-in-Depth to Help Protect Your Amazon S3 Data](#).

Accesso al nostro AWS Glue Amazon Athena

Redshift Spectrum accede al tuo catalogo di dati in o AWS Glue Athena. Un'altra opzione consiste nell'utilizzare un Hive Metastore dedicato per il catalogo dati.

Per abilitare l'accesso a AWS Glue o Athena, configura il tuo VPC con un gateway Internet o un gateway NAT. Configura i tuoi gruppi di sicurezza VPC per consentire il traffico in uscita verso gli endpoint pubblici di e Athena. AWS Glue In alternativa, puoi configurare un endpoint VPC di interfaccia per accedere AWS Glue al tuo. AWS Glue Data Catalog Quando utilizzi un endpoint di interfaccia VPC, la comunicazione tra il tuo VPC e il tuo VPC AWS Glue viene condotta all'interno della rete. AWS Per ulteriori informazioni, consultare [Creazione di un endpoint di interfaccia](#).

È possibile configurare i percorsi seguenti nel VPC:

- Gateway Internet: per connetterti a AWS servizi esterni al tuo VPC, puoi collegare [un gateway Internet](#) alla tua sottorete VPC, come descritto nella Amazon VPC User Guide. Per usare un Internet gateway, il cluster deve avere indirizzi IP pubblici per permettere la comunicazione di altri servizi con il cluster.
- Gateway NAT: per connetterti a un bucket Amazon S3 in AWS un'altra regione o a un altro servizio all'interno AWS della rete, configura [un gateway NAT \(Network Address Translation\), come descritto](#) nella Amazon VPC User Guide. Utilizzare questa configurazione anche per effettuare l'accesso a un'istanza host al di fuori dalla rete AWS .

Per ulteriori informazioni, consultare [Routing VPC avanzato in Amazon Redshift](#).

# Monitoraggio delle prestazioni del cluster Amazon Redshift

Amazon Redshift fornisce parametri e dati di prestazioni in modo che sia possibile monitorare l'integrità e le prestazioni di database e cluster. In questa sezione, vengono descritti i tipi di dati che possono essere utilizzati in Amazon Redshift e in particolare nella console Amazon Redshift.

## Argomenti

- [Panoramica](#)
- [Monitoraggio di Amazon Redshift tramite metriche CloudWatch](#)
- [Utilizzo dei dati di prestazioni nella console Amazon Redshift](#)

## Panoramica

I dati relativi alle prestazioni che possono essere utilizzati nella console Amazon Redshift sono suddivisi in due categorie:

- Parametri Amazon CloudWatch : i CloudWatch parametri di Amazon ti aiutano a monitorare gli aspetti fisici del cluster, come l'utilizzo della CPU, la latenza e il throughput. I dati dei parametri sono visualizzati direttamente nella console Amazon Redshift. Puoi anche visualizzarlo nella console. CloudWatch In alternativa, puoi utilizzarlo in qualsiasi altro modo in cui lavori con le metriche, ad esempio con AWS CLI o con uno degli AWS SDK.
- Dati relativi alle prestazioni di query/caricamento: i dati sulle prestazioni consentono di monitorare l'attività e le prestazioni del database. Questi dati vengono aggregati nella console Amazon Redshift per aiutarti a correlare facilmente ciò che vedi CloudWatch nelle metriche con eventi di caricamento e query specifici del database. Puoi inoltre creare query di prestazioni personalizzate ed eseguirle direttamente sul database. I dati relativi a prestazioni di query e caricamento sono visualizzati solo nella console Amazon Redshift. Non vengono pubblicati come metriche. CloudWatch

I dati relativi alle prestazioni sono integrati nella console Amazon Redshift e ciò consente una migliore esperienza per i seguenti motivi:

- I dati di prestazioni associati a un cluster sono visualizzati contestualmente quando visualizzi un cluster, rendendo più agevole la presa di decisioni sulle operazioni inerenti al cluster, ad esempio il ridimensionamento.

- Alcune metriche delle prestazioni vengono visualizzate in unità ridimensionate in modo più appropriato nella console Amazon Redshift rispetto a. CloudWatch Ad esempio `WriteThroughput`, viene visualizzato in GB/s (rispetto ai byte/s in CloudWatch), che è un'unità più rilevante per lo spazio di archiviazione tipico di un nodo.
- Puoi facilmente visualizzare dati di prestazioni per i nodi di un cluster insieme nello stesso grafico. In questo modo, puoi facilmente monitorare le prestazioni di tutti i nodi di un cluster. Puoi inoltre visualizzare i dati di prestazioni per ogni nodo.

Amazon Redshift fornisce dati sulle prestazioni (sia CloudWatch metriche che dati di query e caricamento) senza costi aggiuntivi. I dati di prestazioni sono registrati ogni minuto. È possibile accedere ai valori cronologici dei dati delle prestazioni nella console Amazon Redshift. [Per informazioni dettagliate sull'utilizzo per accedere CloudWatch ai dati sulle prestazioni di Amazon Redshift esposti come CloudWatch metriche, consulta \*What is? CloudWatch\* nella Amazon CloudWatch User Guide.](#)

## Monitoraggio di Amazon Redshift tramite metriche CloudWatch

Utilizzando i CloudWatch parametri per Amazon Redshift, puoi ottenere informazioni sullo stato e le prestazioni del cluster e visualizzare le informazioni a livello di nodo. Quando utilizzi tali parametri, considera che a ogni parametro sono associate una o più dimensioni. Queste dimensioni indicano a cosa si applica il parametro, ovvero l'ambito del parametro. Amazon Redshift ha le seguenti due dimensioni:

- I parametri con la dimensione `NodeID` sono quelli che forniscono dati di prestazioni per i nodi di un cluster. Questo set di parametri include nodi principali e di calcolo. Esempi di questi parametri sono `CPUUtilization`, `ReadIOPS`, `WriteIOPS`.
- I parametri con unicamente la dimensione `ClusterIdentifier` sono quelli che forniscono dati di prestazioni per i cluster. Esempi di questi parametri sono `HealthStatus` e `MaintenanceMode`.

### Note

In alcuni casi, un parametro specifico ai cluster rappresenta un'aggregazione del comportamento dei nodi. In questi casi, presta attenzione all'interpretazione del valore del parametro in quanto il comportamento del nodo principale viene aggregato a quello del nodo di calcolo.

Per informazioni generali su CloudWatch metriche e dimensioni, consulta [CloudWatch i concetti](#) nella Amazon CloudWatch User Guide.

Per un'ulteriore descrizione dei CloudWatch parametri per Amazon Redshift, consulta le seguenti sezioni.

### Argomenti

- [Parametri di Amazon Redshift](#)
- [Dimensioni per i parametri di Amazon Redshift](#)
- [Dati di prestazioni di query e caricamento di Amazon Redshift](#)

## Parametri di Amazon Redshift

Lo spazio dei nomi `AWS/Redshift` include i parametri descritti di seguito. Salvo diversa indicazione, i parametri vengono raccolti a intervalli di 1 minuto.

### Title

Parametro	Descrizione
<code>CommitQueueLength</code>	<p>Il numero di transazioni in attesa di eseguire il commit in un dato momento.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code></p>
<code>ConcurrencyScalingActiveClusters</code>	<p>Il numero di cluster di dimensionamento simultaneo che elaborano attivamente le query in qualsiasi momento.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code></p>
<code>ConcurrencyScalingSeconds</code>	<p>Il numero di secondi impiegati dai cluster di dimensionamento simultaneo con attività di elaborazione di query attiva.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code></p>

Parametro	Descrizione
<code>CPUUtilization</code>	<p>La percentuale di utilizzo della CPU. Per i cluster, questo parametro rappresenta un'aggregazione dei valori di utilizzo della CPU di tutti i nodi (singolo e calcolo).</p> <p>Unità: percentuale</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensioni: <code>ClusterIdentifier</code></p>
<code>DatabaseConnections</code>	<p>Il numero di connessioni di database a un cluster.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code></p>

Parametro	Descrizione
HealthStatus	<p>Indica lo stato del cluster. Il cluster si connette al proprio database ed esegue una semplice query ogni minuto. Se è in grado di eseguire questa operazione correttamente, il cluster è considerato integro. In caso contrario, il cluster non è integro. Uno stato non integro può verificarsi quando il database del cluster è sovraccaricato eccessivamente oppure se si verifica un problema di configurazione con un database sul cluster.</p> <div data-bbox="592 590 1507 1241"><p> <b>Note</b></p><p>In Amazon CloudWatch, questa metrica viene riportata come 1 o 0, mentre nella console Amazon Redshift viene visualizzata con le HEALTHY parole UNHEALTHY o per comodità. Quando questo parametro è visualizzato nella console Amazon Redshift, le medie di campionamento vengono ignorate e viene visualizzato solo HEALTHY o UNHEALTHY . In Amazon CloudWatch, potrebbero verificarsi valori diversi da 1 e 0 a causa di problemi di campionamento. Qualsiasi valore inferiore a 1 per HealthStatus è segnalato come 0 (UNHEALTHY ).</p></div> <p>Unità: conteggio (1/0) (HEALTHY/UNHEALTHY nella console Amazon Redshift)</p> <p>Dimensioni: ClusterIdentifier</p>

Parametro	Descrizione
MaintenanceMode	<p>Indica se il cluster è in modalità di manutenzione.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>In Amazon CloudWatch, questa metrica viene riportata come 1 o 0, mentre nella console Amazon Redshift viene visualizzata con le ON parole OFF o per comodità. Quando questo parametro è visualizzato nella console Amazon Redshift, le medie di campionamento vengono ignorate e viene visualizzato solo ON o OFF. In Amazon CloudWatch, potrebbero verificarsi valori diversi da 1 e 0 a causa di problemi di campionamento. Qualsiasi valore maggiore di 0 per MaintenanceMode è segnalato come 1 (ON).</p> </div> <p>Unità: conteggio (1/0) (ON/OFF nella console Amazon Redshift)</p> <p>Dimensioni: ClusterIdentifier</p>
MaxConfiguredConcurrencyScalingClusters	<p>Numero massimo di cluster di dimensionamento simultaneo configurati dal gruppo di parametri. Per ulteriori informazioni, consultare <a href="#">Gruppi di parametri di Amazon Redshift</a>.</p> <p>Unità: numero</p> <p>Dimensioni: ClusterIdentifier</p>
NetworkReceiveThroughput	<p>La velocità alla quale il nodo o il cluster riceve i dati.</p> <p>Unità: byte/s (MB/s nella console Amazon Redshift)</p> <p>Dimensioni: ClusterIdentifier , NodeID</p> <p>Dimensioni: ClusterIdentifier</p>

Parametro	Descrizione
NetworkTransmitThroughput	<p>La velocità alla quale il nodo o il cluster scrive i dati.</p> <p>Unità: byte/s (MB/s nella console Amazon Redshift)</p> <p>Dimensioni: ClusterIdentifier , NodeID</p> <p>Dimensioni: ClusterIdentifier</p>
PercentageDiskSpaceUsed	<p>La percentuale di spazio su disco utilizzata.</p> <p>Unità: percentuale</p> <p>Dimensioni: ClusterIdentifier</p> <p>Dimensioni: ClusterIdentifier , NodeID</p>
QueriesCompletedPerSecond	<p>Numero medio di query eseguite al secondo. Segnalato in intervalli di 5 minuti. Questa metrica non è supportata nei cluster a nodo singolo.</p> <p>Unità: conteggio/secondo</p> <p>Dimensioni: ClusterIdentifier , latency</p> <p>Dimensioni: ClusterIdentifier , wlmid</p>
QueryDuration	<p>Il tempo medio necessario per il completamento di una query. Segnalato in intervalli di 5 minuti. Questa metrica non è supportata nei cluster a nodo singolo.</p> <p>Unità: microsecondi</p> <p>Dimensioni: ClusterIdentifier , NodeID, latency</p> <p>Dimensioni: ClusterIdentifier , latency</p> <p>Dimensioni: ClusterIdentifier , NodeID, wlmid</p>

Parametro	Descrizione
QueryRuntimeBreakdown	<p>Il tempo totale impiegato dalle query in esecuzione per fase di query. Segnalato in intervalli di 5 minuti.</p> <p>Unità: millisecondi</p> <p>Dimensioni: ClusterIdentifier, NodeID, stage</p> <p>Dimensioni: stage ClusterIdentifier</p>
ReadIOPS	<p>Il numero medio di operazioni di lettura del disco al secondo.</p> <p>Unità: conteggio/secondo</p> <p>Dimensioni: ClusterIdentifier , NodeID</p> <p>Dimensioni: ClusterIdentifier</p>
ReadLatency	<p>La quantità di tempo media che occorre per effettuare operazioni I/O di lettura del disco.</p> <p>Unità: secondi</p> <p>Dimensioni: ClusterIdentifier , NodeID</p> <p>Dimensioni: ClusterIdentifier</p>
ReadThroughput	<p>Il numero medio di byte letti dal disco al secondo.</p> <p>Unità: byte (GB/s nella console Amazon Redshift)</p> <p>Dimensioni: ClusterIdentifier , NodeID</p> <p>Dimensioni: ClusterIdentifier</p>
RedshiftManagedStorageTotalCapacity	<p>Capacità totale di archiviazione gestita.</p> <p>Unità: megabyte</p> <p>Dimensioni: ClusterIdentifier</p>

Parametro	Descrizione
TotalTableCount	<p>Il numero di tabelle utente aperte in un particolare momento. Questo totale non include le tabelle di Amazon Redshift Spectrum.</p> <p>Unità: numero</p> <p>Dimensioni: ClusterIdentifier</p>
WLMQueueLength	<p>Il numero di query in attesa di entrare in una coda Workload Management (WLM).</p> <p>Unità: numero</p> <p>Dimensioni: ClusterIdentifier , service class</p> <p>Dimensioni: ClusterIdentifier , QueueName</p>
WLMQueueWaitTime	<p>Tempo totale trascorso dalle query in attesa nella coda workload management (WLM) Segnalato in intervalli di 5 minuti.</p> <p>Unità: millisecondi</p> <p>Dimensioni: ClusterIdentifier , QueryPriority</p> <p>Dimensioni: ClusterIdentifier , wlmid</p> <p>Dimensioni: ClusterIdentifier , QueueName</p>
WLMQueriesComplete dPerSecond	<p>Numero medio di query eseguite al secondo per una coda Workload Management (WLM). Segnalato in intervalli di 5 minuti. Questa metrica non è supportata nei cluster a nodo singolo.</p> <p>Unità: conteggio/secondo</p> <p>Dimensioni: ClusterIdentifier , wlmid</p> <p>Dimensioni: ClusterIdentifier , QueueName</p>

Parametro	Descrizione
<code>WLMQueryDuration</code>	<p>Durata media temporale per il completamento di una query per una coda Workload Management (WLM). Segnalato in intervalli di 5 minuti. Questa metrica non è supportata nei cluster a nodo singolo.</p> <p>Unità: microsecondi</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>wlmid</code></p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>QueueName</code></p>
<code>WLMRunningQueries</code>	<p>Il numero di query in esecuzione sia dal cluster principale che da quello di dimensionamento simultaneo per coda WLM.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>wlmid</code></p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>QueueName</code></p>
<code>WriteIOPS</code>	<p>Il numero medio di operazioni di scrittura al secondo.</p> <p>Unità: conteggio/secondo</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensioni: <code>ClusterIdentifier</code></p>
<code>WriteLatency</code>	<p>La quantità di tempo media che occorre per effettuare operazioni I/O di scrittura sul disco.</p> <p>Unità: secondi</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensioni: <code>ClusterIdentifier</code></p>

Parametro	Descrizione
<code>WriteThroughput</code>	<p>Il numero medio di byte scritti sul disco al secondo.</p> <p>Unità: byte (GB/s nella console Amazon Redshift)</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>NodeID</code></p> <p>Dimensioni: <code>ClusterIdentifier</code></p>
<code>SchemaQuota</code>	<p>La quota configurata per uno schema.</p> <p>Unità: megabyte</p> <p>Dimensioni: <code>ClusterIdentifier</code> , <code>Database</code>, <code>Schema</code></p> <p>Periodico/Push: <code>Periodic</code></p> <p>Frequenza: 5 minutes</p> <p>Criteri di interruzione: schema eliminato o quota rimossa</p>
<code>NumExceededSchemaQuotas</code>	<p>Il numero di schemi con quote superate.</p> <p>Unità: numero</p> <p>Dimensioni: <code>ClusterIdentifier</code></p> <p>Periodico/Push: <code>Periodic</code></p> <p>Frequenza: 5 minutes</p> <p>Criteri di arresto: N/D</p>

Parametro	Descrizione
StorageUsed	<p>Il disco o lo spazio di archiviazione utilizzato da uno schema.</p> <p>Unità: megabyte</p> <p>Dimensioni: <code>ClusterIdentifier</code> , Database, Schema</p> <p>Periodico/Push: <code>Periodic</code></p> <p>Frequenza: 5 minutes</p> <p>Criteri di interruzione: schema eliminato o quota rimossa</p>
PercentageQuotaUsed	<p>La percentuale di spazio su disco o di archiviazione utilizzato rispetto alla quota dello schema configurata.</p> <p>Unità: percentuale</p> <p>Dimensioni: <code>ClusterIdentifier</code> , Database, Schema</p> <p>Periodico/Push: <code>Periodic</code></p> <p>Frequenza: 5 minutes</p> <p>Criteri di interruzione: schema eliminato o quota rimossa</p>

Parametro	Descrizione
UsageLimitAvailable	<p>A seconda di FeatureType, UsageLimitAvailable restituisce quanto segue:</p> <ul style="list-style-type: none"><li>• Se FeatureType è CONCURRENTLY_SCALING , UsageLimitAvailable restituisce la quantità di tempo totale che può essere utilizzata mediante il ridimensionamento simultaneo in incrementi di 1 minuto.</li><li>• Se FeatureType è CROSS_REGION_DATASHARING , UsageLimitAvailable restituisce la quantità totale di dati che è possibile scansionare con incrementi di 1 TB.</li><li>• In caso FeatureType affermativo SPECTRUM, UsageLimitAvailable restituisce la quantità totale di dati che è possibile scansionare con incrementi di 1 TB.</li></ul> <p>Unità: minuti o TB</p> <p>Dimensioni: ClusterIdentifier , FeatureType , UsageLimitId</p>

Parametro	Descrizione
UsageLimitConsumed	<p>A seconda di FeatureType, UsageLimitConsumed restituisce quanto segue:</p> <ul style="list-style-type: none"> <li>• Se FeatureType è CONCURRENTY_SCALING , UsageLimitAvailable restituisce la quantità totale di tempo utilizzata dal ridimensionamento simultaneo in incrementi di 1 minuto.</li> <li>• Se FeatureType è CROSS_REGION_DATASHARING , UsageLimitAvailable restituisce la quantità totale di dati scansionati con incrementi di 1 TB.</li> <li>• Se FeatureType è SPECTRUM, UsageLimitAvailable restituisce la quantità totale di dati scansionati con incrementi di 1 TB.</li> </ul> <p>Unità: minuti o TB</p> <p>Dimensioni: ClusterIdentifier , FeatureType , UsageLimitId</p>

## Dimensioni per i parametri di Amazon Redshift

I dati Amazon Redshift possono essere filtrati insieme alle dimensioni nella seguente tabella.

Dimensione	Descrizione
latency	<p>I valori possibili sono i seguenti:</p> <ul style="list-style-type: none"> <li>• breve: meno di 10 secondi</li> <li>• media: tra 10 secondi e 10 minuti</li> <li>• lunga: più di 10 minuti</li> </ul>
NodeID	<p>Filtra i dati richiesti che sono specifici dei nodi di un cluster. NodeID è "Leader", "Shared" o "Compute-N", dove N è 0, 1, ... per il numero di nodi nel cluster. "Shared" significa che il cluster ha solo un nodo, ovvero che il nodo principale e il nodo di calcolo sono combinati.</p>

Dimensione	Descrizione
	I parametri di <code>CPUUtilization</code> , <code>NetworkTransmitThroughput</code> e <code>ReadIOPS</code> vengono indicati solo per il nodo principale e i nodi di calcolo. Altri parametri che utilizzano la dimensione <code>NodeId</code> vengono indicati solo per i nodi di calcolo.
<code>ClusterIdentifier</code>	Filtra i dati richiesti che sono specifici del cluster. I parametri specifici dei cluster includono <code>HealthStatus</code> , <code>MaintenanceMode</code> e <code>DatabaseConnections</code> . I parametri generali per questa dimensione (ad esempio <code>ReadIOPS</code> ) che sono anche parametri dei nodi rappresentano un'aggregazione dei dati dei parametri dei nodi. Presta attenzione nell'interpretare questi parametri in quanto aggregano il comportamento di nodi principali e nodi di calcolo.
<code>service class</code>	L'identificatore per una classe di servizio WLM.

Dimensione	Descrizione
stage	<p>Le fasi dell'esecuzione per una query. I valori possibili sono i seguenti:</p> <ul style="list-style-type: none"> <li>• QueryPlanning: Tempo impiegato per l'analisi e l'ottimizzazione delle istruzioni SQL.</li> <li>• QueryWaiting: Tempo di attesa nella coda WLM.</li> <li>• QueryExecutingRead: Tempo impiegato per l'esecuzione di interrogazioni di lettura.</li> <li>• QueryExecutingInsert: Tempo impiegato per l'esecuzione delle interrogazioni di inserimento.</li> <li>• QueryExecutingDelete: tempo impiegato per l'esecuzione delle interrogazioni di eliminazione.</li> <li>• QueryExecutingUpdate: tempo impiegato per l'esecuzione delle interrogazioni di aggiornamento.</li> <li>• QueryExecutingCtas: tempo impiegato per l'esecuzione della creazione della tabella come query.</li> <li>• QueryExecutingUnload: tempo impiegato per l'esecuzione delle interrogazioni di scaricamento.</li> <li>• QueryExecutingCopy: tempo impiegato per l'esecuzione di interrogazioni di copia.</li> <li>• QueryCommit: tempo impiegato a impegnarsi.</li> </ul>
wlmid	Identificatore per una coda di gestione dei carichi di lavoro.
QueryPriority	La priorità della query. I valori possibili sono CRITICAL, HIGHEST, HIGH, NORMAL, LOW e LOWEST.
QueueName	Nome della coda di gestione del carico di lavoro.
FeatureType	La funzionalità è vincolata da un limite di utilizzo. I valori possibili sono CONCURRENTLY_SCALING , CROSS_REGION_DATAS HARING e SPECTRUM.
UsageLimitId	L'identificatore di un limite di utilizzo.

## Dati di prestazioni di query e caricamento di Amazon Redshift

Oltre alle CloudWatch metriche, Amazon Redshift fornisce dati sulle prestazioni di query e caricamento. Questi dati ti consentono di comprendere la relazione tra le prestazioni dei database e i parametri dei cluster. Ad esempio, se si verifica un picco nella CPU di un cluster, questo è indicato sul grafico della CPU del cluster e puoi quindi determinare le query che erano in esecuzione in quel momento. Al contrario, se esamini una specifica query, i dati dei parametri (come la CPU) sono visualizzati in contesto di modo che sia possibile comprendere l'impatto della query sui parametri del cluster.

I dati sulle prestazioni di query e carico non vengono pubblicati come CloudWatch metriche e possono essere visualizzati solo nella console Amazon Redshift. I dati relativi alle prestazioni di query e caricamenti sono generati a partire dalle query sulle tabelle di sistema del database (per ulteriori informazioni, consultare [Riferimento delle tabelle di sistema](#) nella Guida per gli sviluppatori di Amazon Redshift). Puoi anche generare query di prestazioni di database personalizzate, ma ti consigliamo di cominciare con i dati di prestazioni di query e di caricamento presentati nella console. Per ulteriori informazioni sulla misurazione e il monitoraggio delle prestazioni dei database, consultare [Gestione delle prestazioni](#) nella Guida per gli sviluppatori di Amazon Redshift.

La tabella seguente descrive i diversi aspetti dei dati di query e di caricamento accessibili nella console Amazon Redshift.

Dati di query/caricamento	Descrizione
Riepilogo delle query	Un elenco di query in un determinato periodo di tempo. L'elenco può essere ordinato in base a valori come ID, tempo di esecuzione e stato della query. Visualizzare questi dati nella scheda Monitoraggio della query della pagina dei dettagli del cluster.
Dettagli della query	Fornisce dettagli su una determinata query, tra cui: <ul style="list-style-type: none"><li>• Proprietà della query come ID, tipo, cluster su cui la query è stata eseguita e tempo di esecuzione.</li><li>• Dettagli come lo stato della query e il numero di errori.</li><li>• L'istruzione SQL che è stata eseguita.</li><li>• Un piano explain, se disponibile.</li></ul>

Dati di query/caricamento	Descrizione
	<ul style="list-style-type: none"> <li>• Dati sulle prestazioni del cluster durante l'esecuzione della query (per ulteriori informazioni, consultare <a href="#">Visualizzazione dei dati della cronologia delle query</a>).</li> </ul>
Riepilogo del caricamento	<p>Elenca tutti i caricamenti in un determinato periodo di tempo. L'elenco può essere ordinato in base a valori come ID, tempo di esecuzione e stato della query. Visualizzare questi dati nella scheda Monitoraggio della query della pagina dei dettagli del cluster.</p>
Dettagli del caricamento	<p>Fornisce dettagli su una determinata operazione di caricamento, tra cui:</p> <ul style="list-style-type: none"> <li>• Proprietà del caricamento come ID, tipo, cluster su cui la query è stata eseguita e tempo di esecuzione.</li> <li>• Dettagli come lo stato del caricamento e il numero di errori.</li> <li>• L'istruzione SQL che è stata eseguita.</li> <li>• Un elenco di file caricati.</li> <li>• Dati sulle prestazioni del cluster durante l'operazione di caricamento (per ulteriori informazioni, consultare <a href="#">Visualizzazione dei dati della cronologia delle query</a>).</li> </ul>

## Utilizzo dei dati di prestazioni nella console Amazon Redshift

In questa sezione viene descritto come visualizzare i dati relativi alle prestazioni nella console Amazon Redshift, tra cui le informazioni sulle prestazioni di cluster e query. Inoltre, è possibile creare allarmi sui parametri del cluster direttamente dalla console Amazon Redshift.

Quando vengono visualizzati i dati relativi alle prestazioni nella console Amazon Redshift, questi sono visualizzati per cluster. I grafici dei dati di prestazioni di un cluster sono concepiti per consentirti di accedere ai dati e per rispondere alle domande più comuni relative alle prestazioni. Per alcuni dati sulle prestazioni (vedi [Monitoraggio di Amazon Redshift tramite metriche CloudWatch](#)), puoi anche utilizzarli CloudWatch per personalizzare ulteriormente i grafici delle metriche. Ad esempio, puoi scegliere tempi più lunghi o combinare parametri tra cluster. Per ulteriori informazioni sull'utilizzo della CloudWatch console, consulta [Utilizzo delle metriche delle prestazioni nella console CloudWatch](#)

Per scoprire come monitorare, isolare e ottimizzare le query utilizzando le funzionalità di monitoraggio delle query sulla console Amazon Redshift, guardare il video [Monitoraggio delle query con Amazon Redshift](#).

## Argomenti

- [Visualizzazione di dati di prestazioni dei cluster](#)
- [Visualizzazione dei dati della cronologia delle query](#)
- [Visualizzazione dei dati delle prestazioni dei database](#)
- [Visualizzazione dei dati relativi alla simultaneità del carico di lavoro e al dimensionamento simultaneo](#)
- [Visualizzazione di query e caricamenti](#)
- [Visualizzazione dei parametri del cluster durante le operazioni di caricamento](#)
- [Analisi delle prestazioni del carico di lavoro](#)
- [Gestione degli allarmi](#)
- [Utilizzo delle metriche delle prestazioni nella console CloudWatch](#)

## Visualizzazione di dati di prestazioni dei cluster

I parametri dei cluster in Amazon Redshift consentono di completare le seguenti attività comuni relative alle prestazioni:

- Determinare se i parametri dei cluster sono anormali nel corso di un intervallo di tempo specificato e se è il caso, identificare le query responsabili del peggioramento delle prestazioni.
- Verificare se le query storiche o correnti hanno un impatto sulle prestazioni dei cluster. Se identifichi una query problematica, puoi visualizzarne i dettagli, incluse le prestazioni del cluster, durante l'esecuzione della query. Puoi utilizzare queste informazioni per diagnosticare il motivo per cui la query era lenta e le soluzioni per migliorarne le prestazioni.

Per visualizzare i dati relativi alle prestazioni

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono

includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.

3. Scegli la scheda Cluster performance (Prestazioni del cluster) per visualizzare le informazioni relative alle prestazioni tra cui:

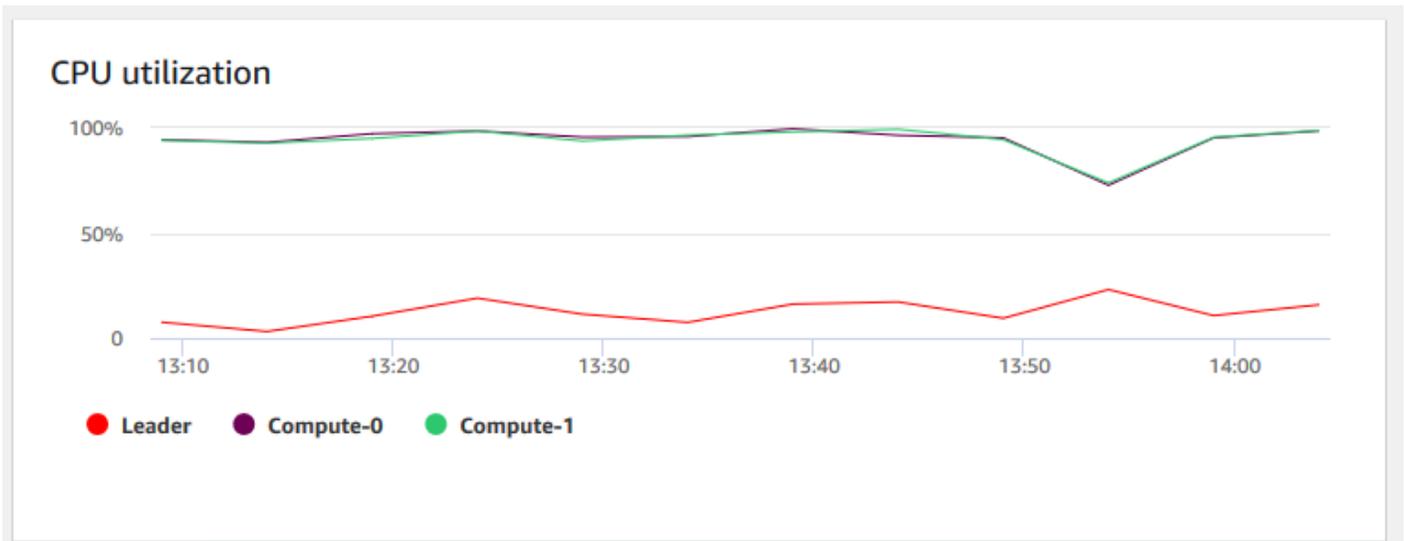
- Utilizzo CPU
- Percentuale di spazio su disco utilizzata
- Connessioni database
- Health status (Stato di integrità)
- Durata query
- Volume di elaborazione query
- Attività di dimensionamento della concorrenza

Sono disponibili molti altri parametri. Per visualizzare i parametri disponibili e scegliere quelli da visualizzare, scegli l'icona Preferences (Preferenze).

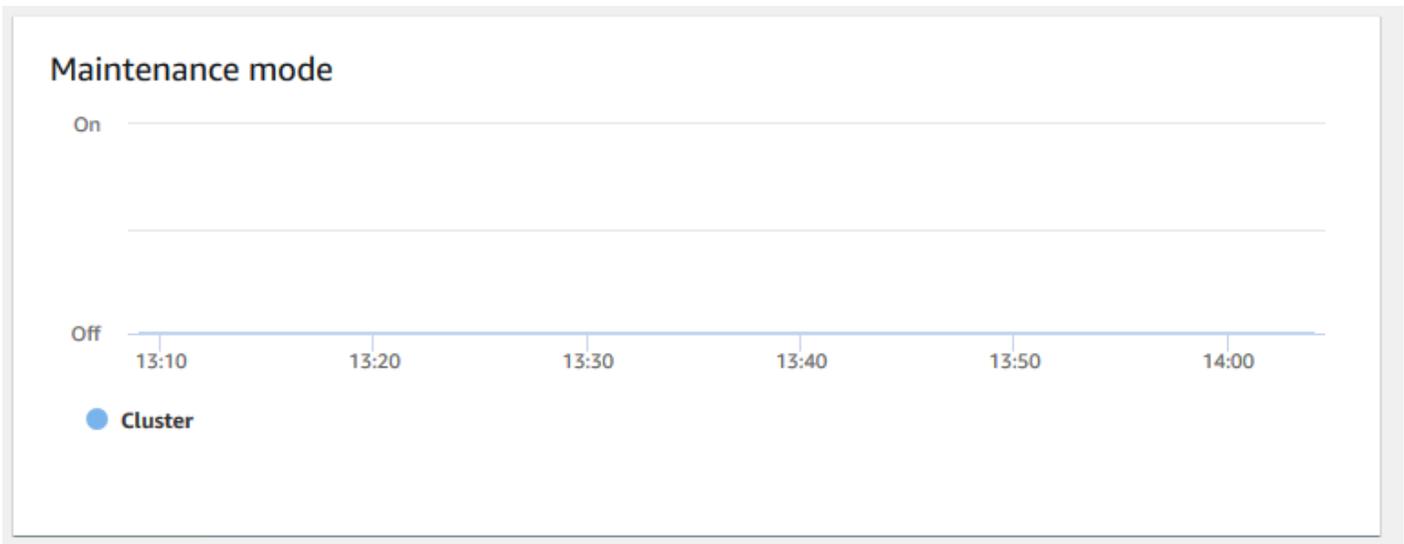
## Grafici delle prestazioni del cluster

Negli esempi seguenti vengono illustrati alcuni dei grafici che vengono visualizzati nella nuova console Amazon Redshift.

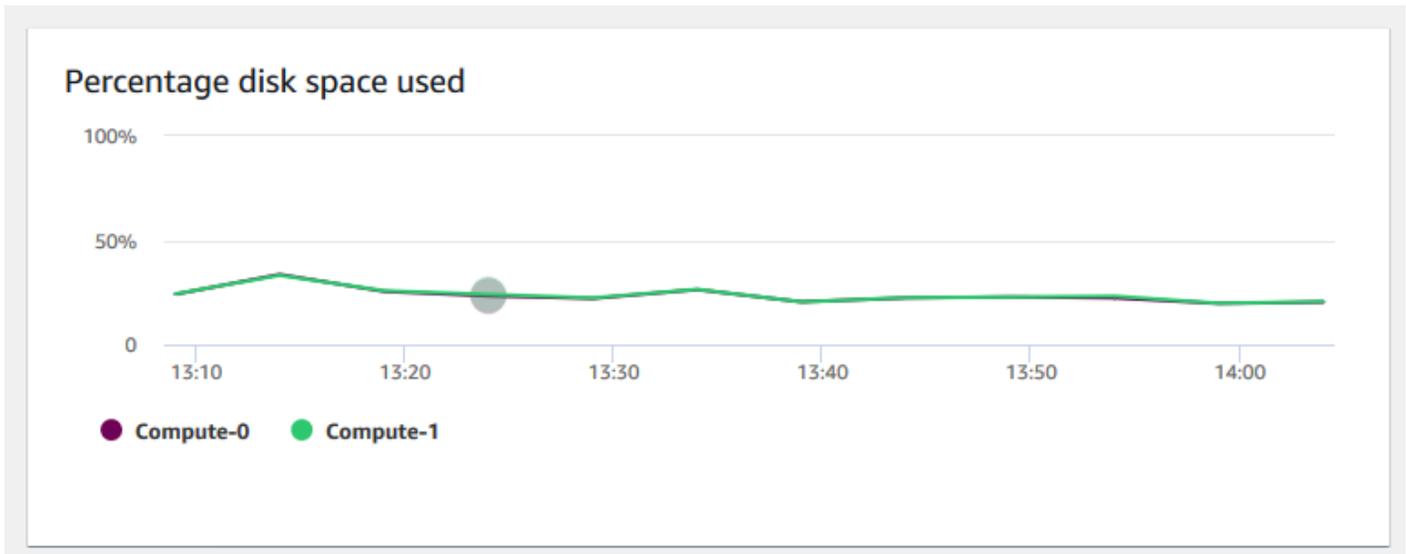
- Utilizzo della CPU: mostra la percentuale di utilizzo della CPU per tutti i nodi (principale e di calcolo). Per individuare il momento in cui l'utilizzo del cluster è minimo prima di pianificare la migrazione del cluster o altre operazioni che richiedono risorse, monitora questo grafico per visualizzare l'utilizzo della CPU per singolo nodo o per tutti i nodi.



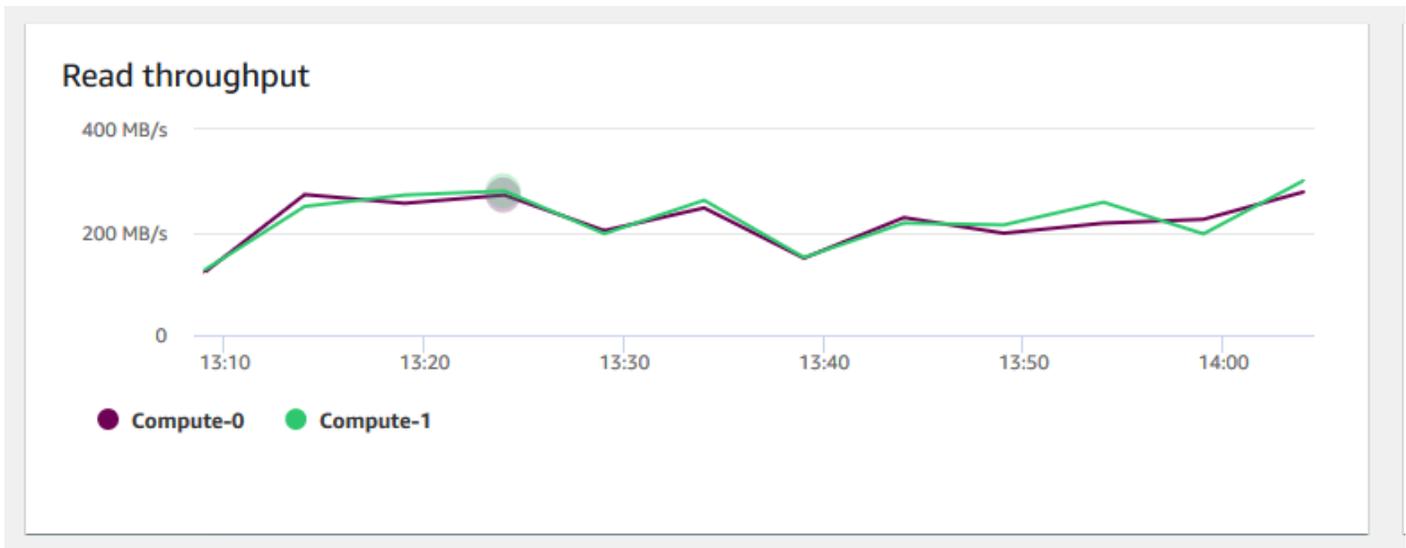
- Modalità di manutenzione: indica se il cluster è in modalità di manutenzione all'ora specificata utilizzando gli indicatori On e Off. È possibile visualizzare l'ora in cui il cluster è in fase di manutenzione. È quindi possibile correlare questa volta alle operazioni eseguite al cluster per stimarne i tempi di inattività futuri per eventi ricorrenti.



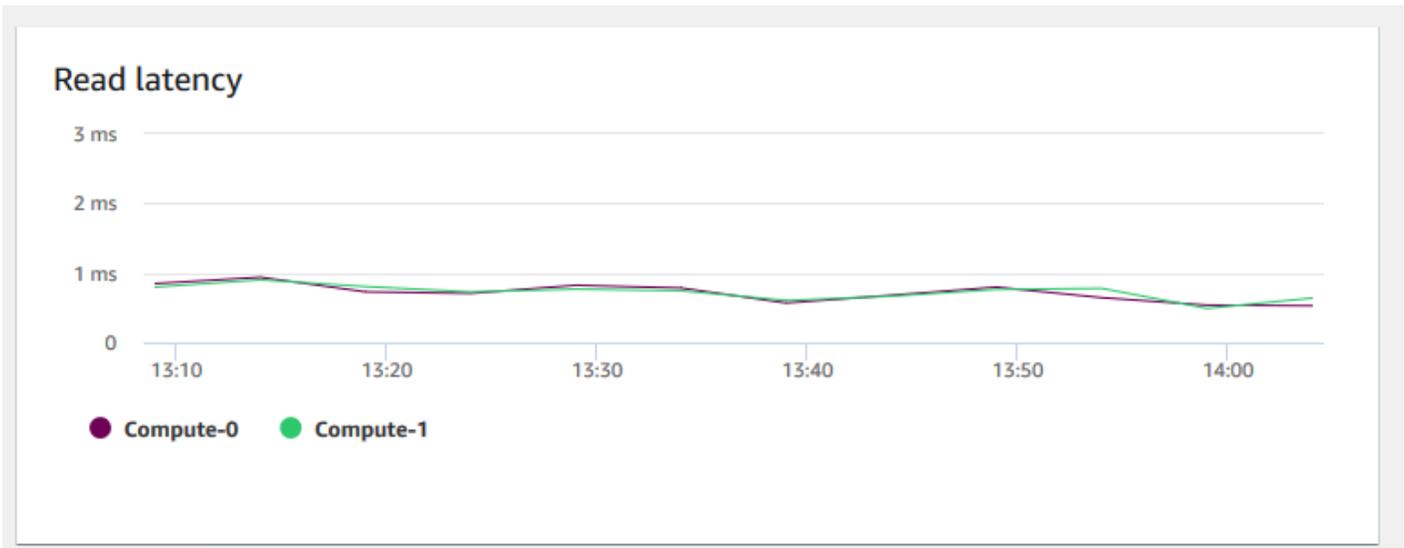
- Percentuale di spazio su disco utilizzato: indica la percentuale di utilizzo dello spazio su disco per ciascun nodo di calcolo e non per il cluster nel suo complesso. Puoi esaminare questo grafico per monitorare l'utilizzo del disco. Le operazioni di manutenzione come VACUUM e COPY utilizzano spazio di storage temporaneo intermedio per le operazioni di ordinamento, quindi è previsto un picco nell'utilizzo del disco.



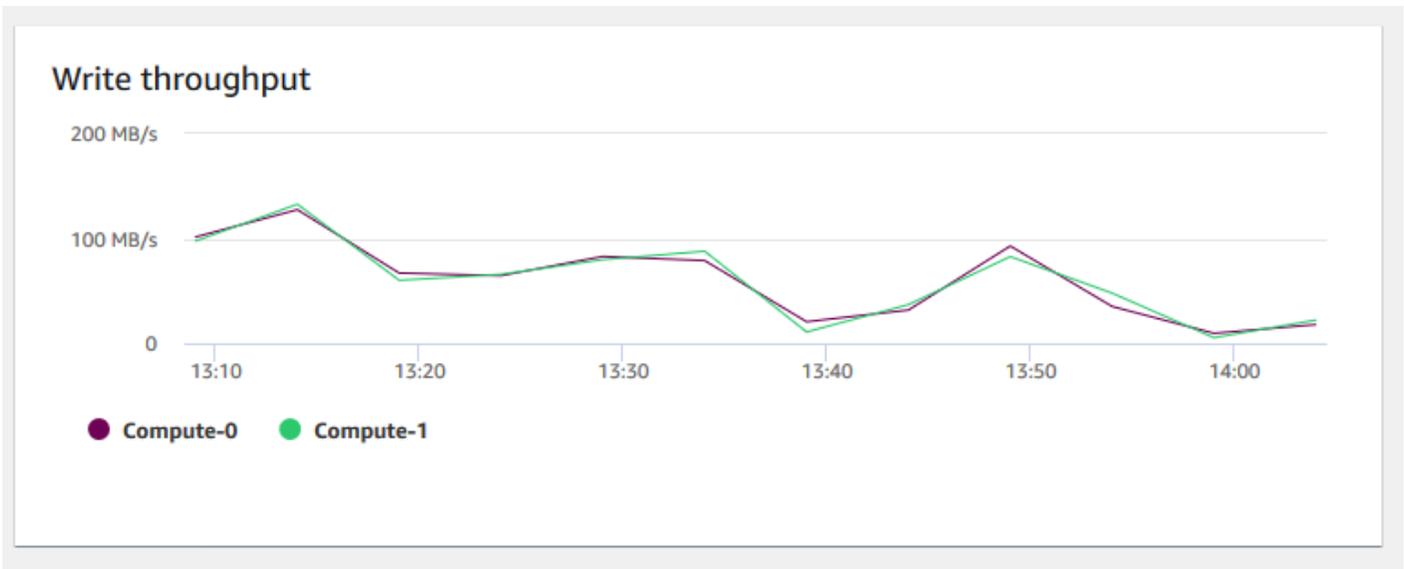
- **Throughput di lettura:** mostra il numero medio di megabyte letti dal disco al secondo. Puoi esaminare questo grafico per monitorare l'aspetto fisico corrispondente del cluster. Questo throughput non include il traffico di rete tra le istanze nel cluster e il volume.



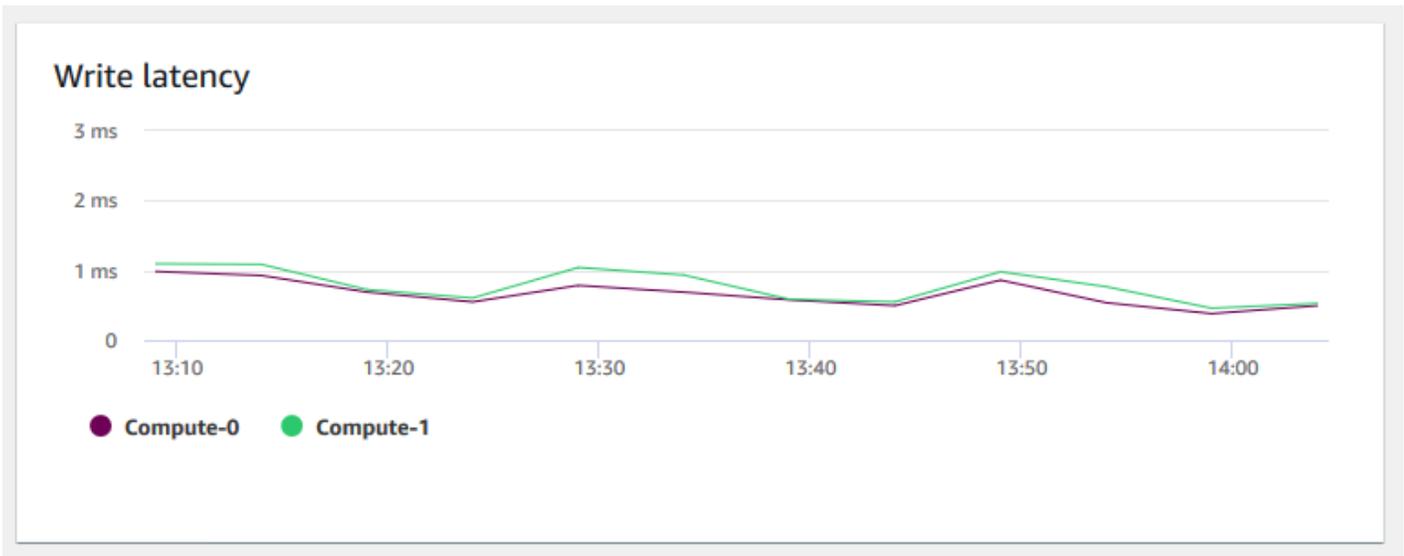
- **Latenza di lettura:** mostra il tempo medio impiegato per le operazioni di I/O di lettura su disco al millisecondo. Puoi visualizzare i tempi di risposta per la restituzione dei dati. Quando la latenza è elevata significa che il sender trascorre più tempo in inattività (non inviando nuovi pacchetti), riducendo così la velocità di crescita del throughput.



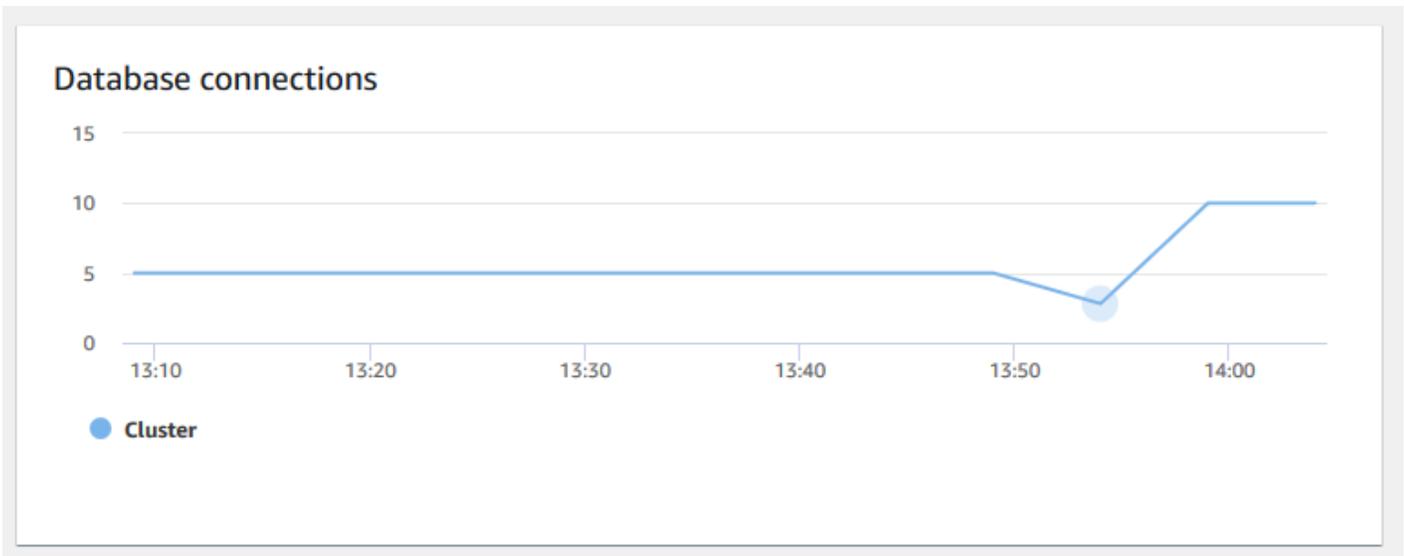
- **Throughput di scrittura:** mostra il numero medio di megabyte scritti sul disco al secondo. Puoi esaminare questo parametro per monitorare l'aspetto fisico corrispondente del cluster. Questo throughput non include il traffico di rete tra le istanze nel cluster e il volume.



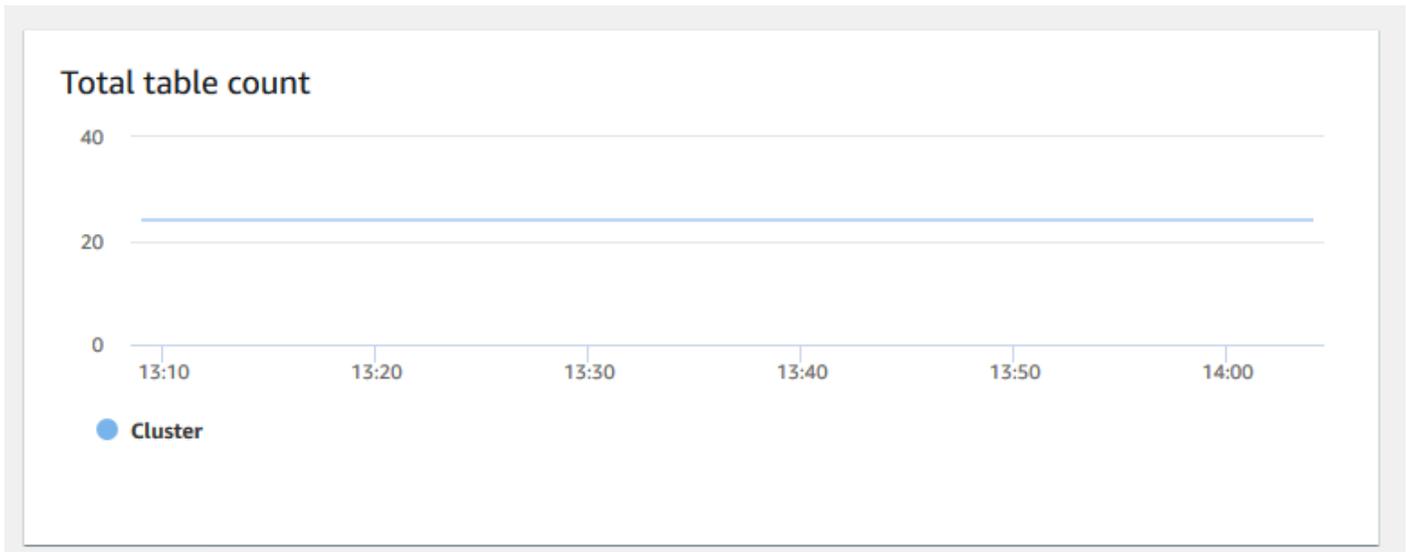
- **Latenza di scrittura:** mostra il tempo medio impiegato per le operazioni di I/O di scrittura su disco al millisecondo. Puoi valutare il tempo di restituzione della conferma di scrittura. Quando la latenza è elevata significa che il sender trascorre più tempo in inattività (non inviando nuovi pacchetti), riducendo così la velocità di crescita del throughput.



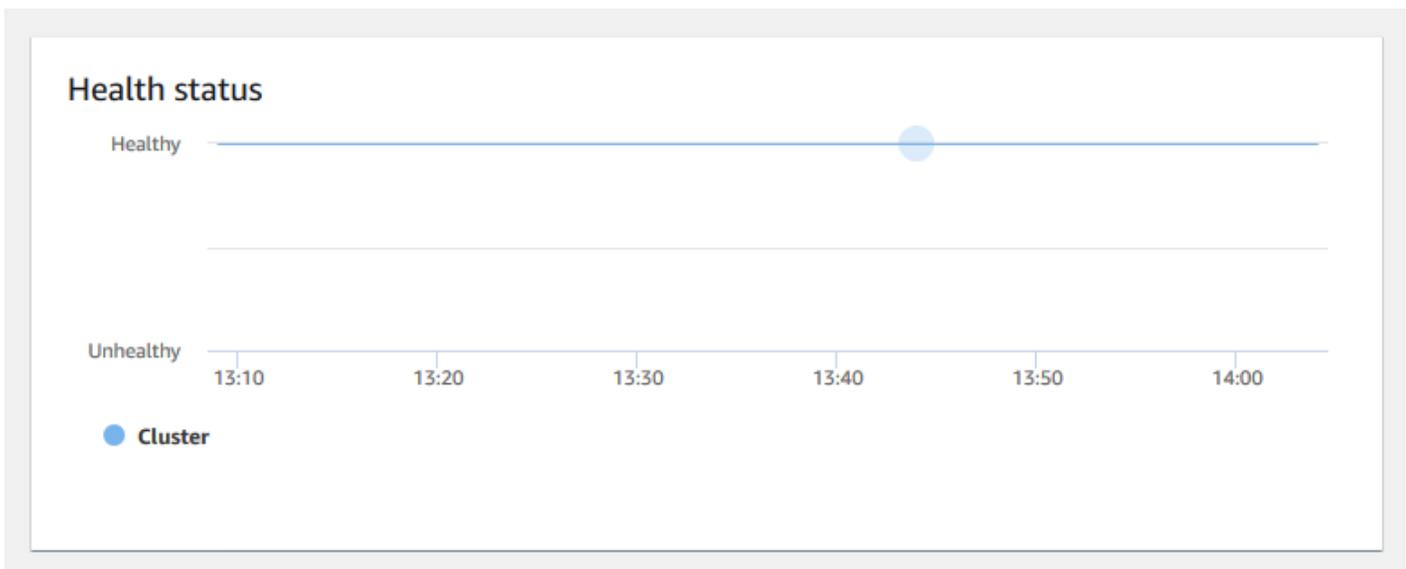
- **Connessioni al database:** mostra il numero di connessioni al database per un cluster. È possibile utilizzare questo grafico per vedere il numero di connessioni stabilite al database e individuare l'ora in cui l'utilizzo del cluster è più basso.



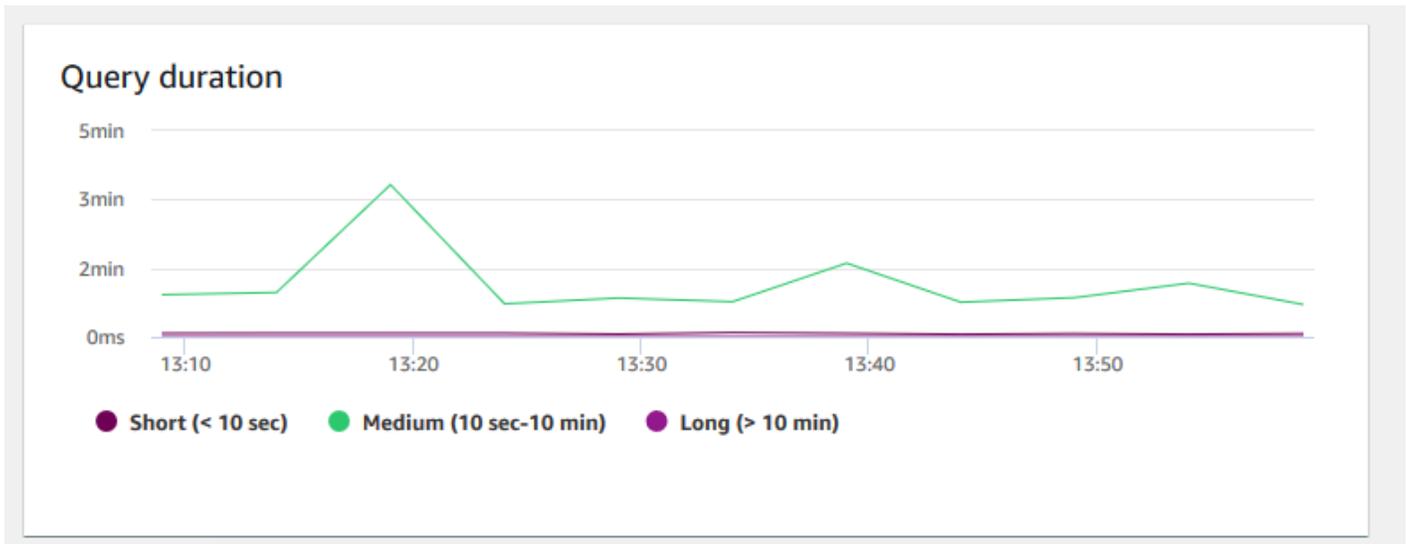
- **Numero totale di tabelle:** mostra il numero di tabelle utente aperte in un determinato momento all'interno di un cluster. Puoi monitorare le prestazioni del cluster quando il numero di tabelle aperte è elevato.



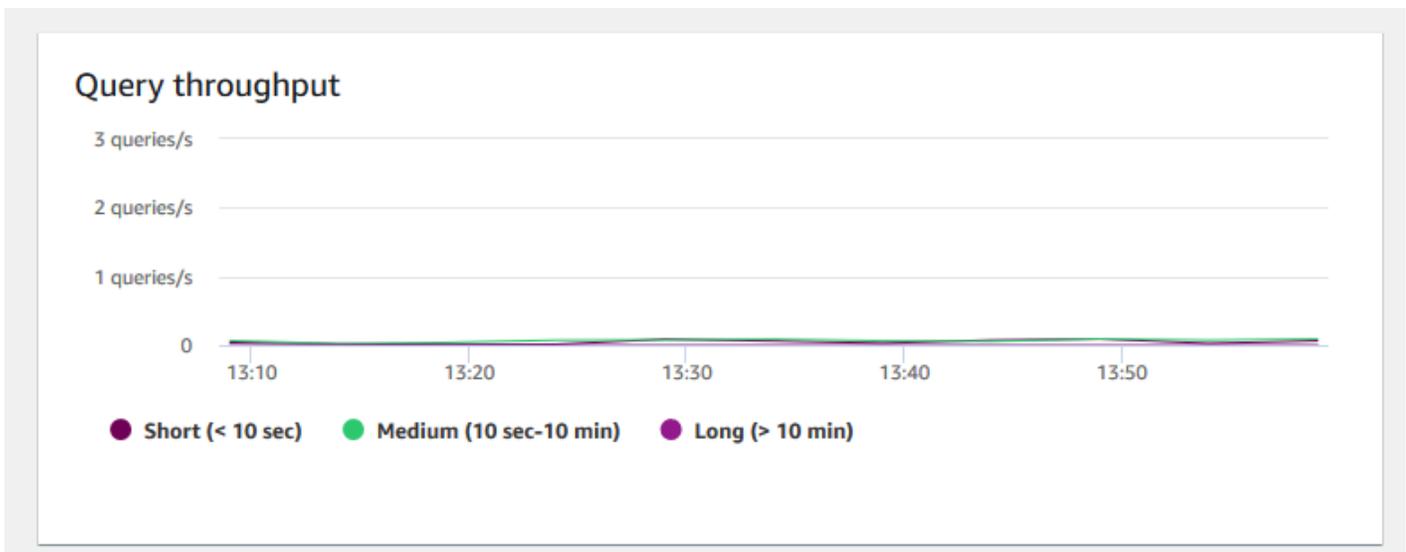
- **Stato di integrità:** indica lo stato di integrità del cluster come `Healthy` o `Unhealthy`. Se il cluster è in grado di connettersi al database ed esegue correttamente una query semplice, il cluster viene considerato integro. In caso contrario, il cluster non è integro. Uno stato non integro può verificarsi quando il database del cluster è sovraccaricato eccessivamente oppure se si verifica un problema di configurazione con un database sul cluster.



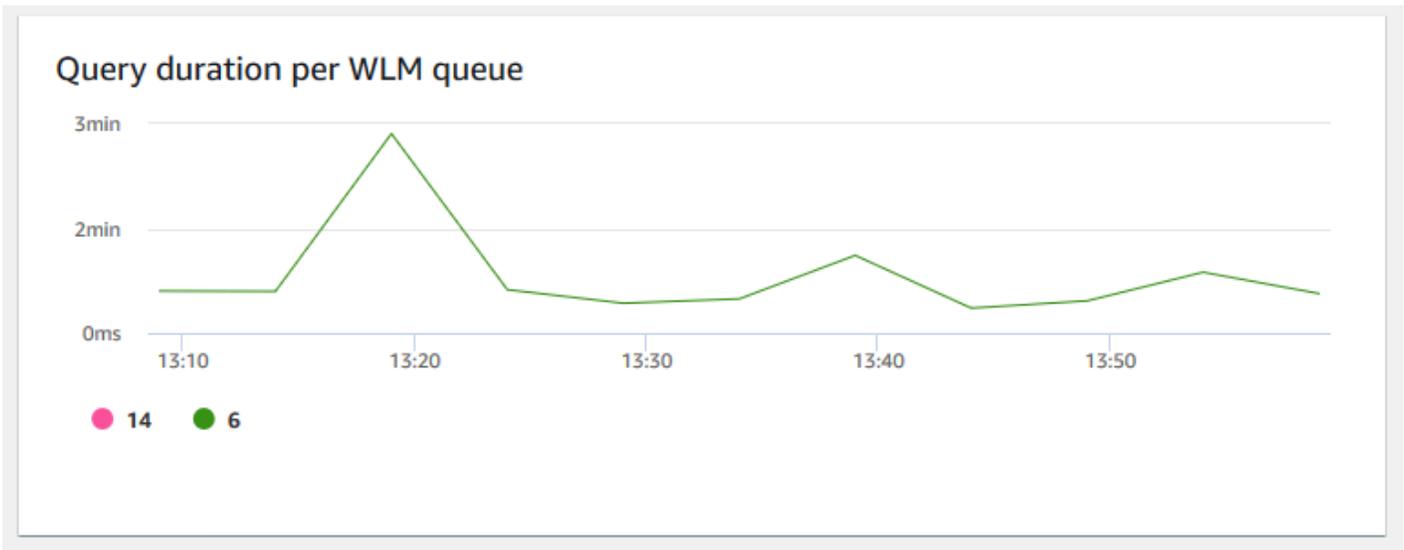
- **Durata della query:** mostra il tempo medio impiegato per completare una query in microsecondi. Puoi eseguire il benchmark dei dati in questo grafico per misurare le prestazioni di I/O all'interno del cluster e ottimizzarne le query più dispendiose in termini di tempo, se necessario.



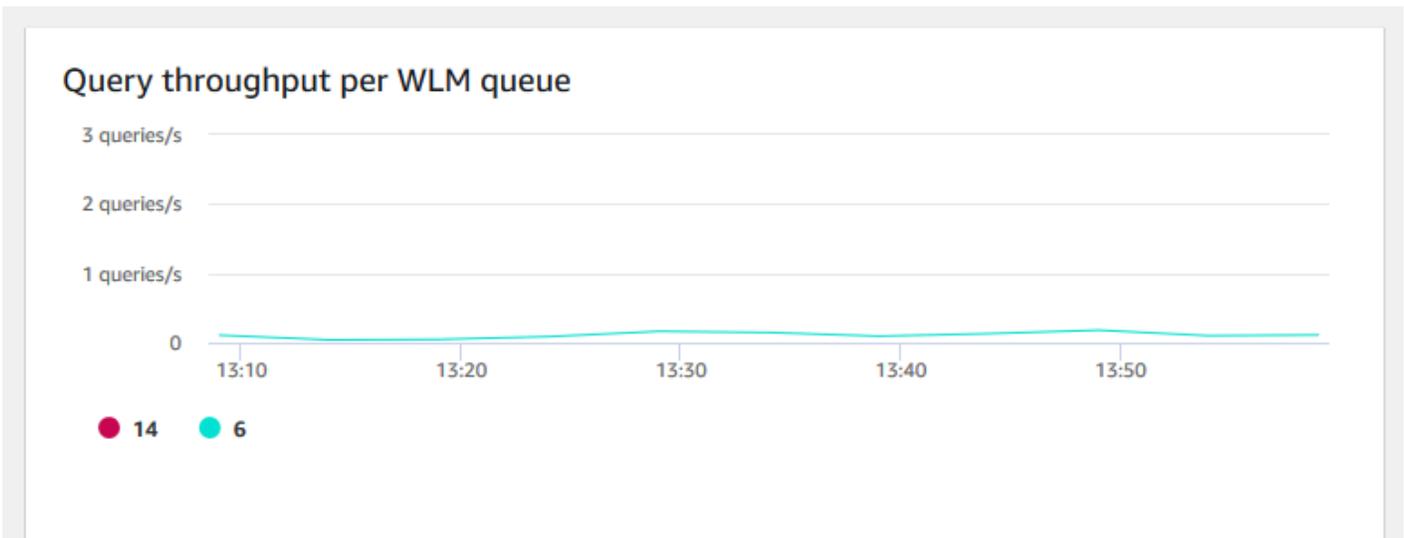
- Throughput della query: mostra il numero medio di query completate al secondo. Puoi analizzare i dati in questo grafico per misurare le prestazioni del database e caratterizzare la capacità del sistema di supportare un carico di lavoro multiutente in modo equilibrato.



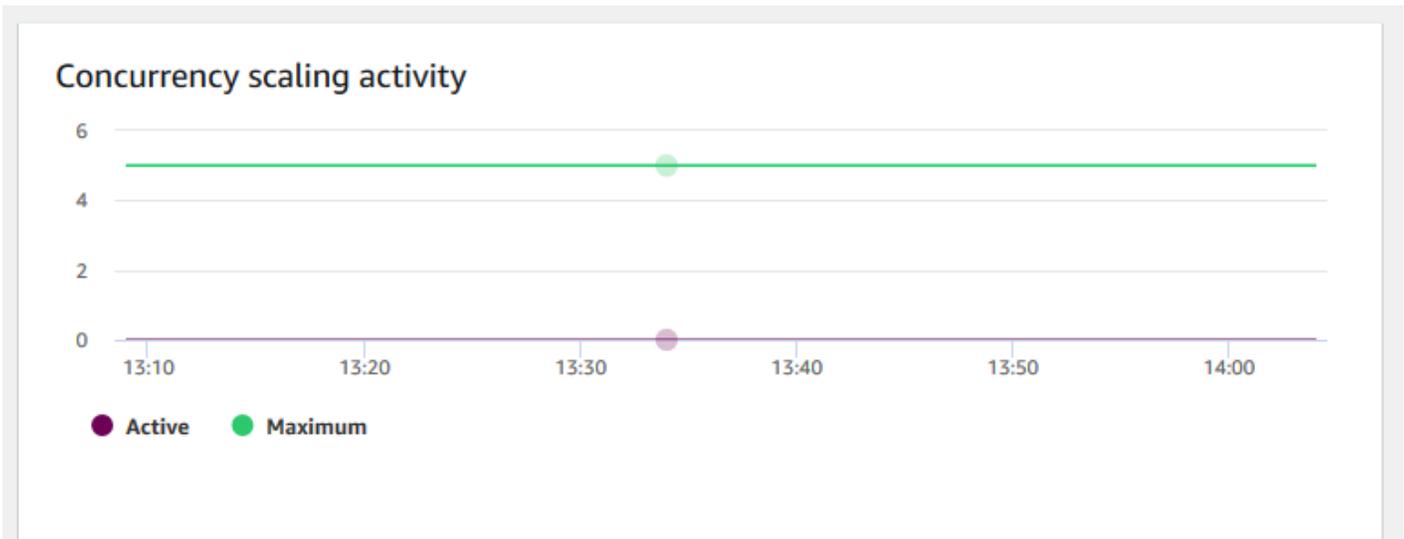
- Durata delle query per coda WLM: mostra il tempo medio per completare una query in microsecondi. Puoi eseguire il benchmark dei dati in questo grafico per misurare le prestazioni di I/O per coda WLM e ottimizzare le query che richiedono più tempo, se necessario.



- Throughput delle query per coda WLM: indica il numero medio di query completate al secondo. Puoi analizzare i dati in questo grafico per misurare le prestazioni del database per coda WLM.



- Attività di dimensionamento simultaneo: mostra il numero di cluster di dimensionamento simultaneo attivi nell'intervallo di tempo selezionato. Quando il dimensionamento simultaneo è abilitato, Amazon Redshift aggiunge automaticamente ulteriore capacità del cluster quando necessario per elaborare un aumento delle query di lettura simultanee.



## Visualizzazione dei dati della cronologia delle query

È possibile utilizzare i parametri della cronologia delle query in Amazon Redshift per completare le seguenti operazioni:

- Isolare e diagnosticare i problemi di prestazioni delle query.
- Confrontare i parametri di runtime delle query e i parametri delle prestazioni del cluster nella stessa sequenza temporale per vedere come potrebbero essere correlati i due parametri. Ciò consente di identificare le query con prestazioni scadenti, cercare colli di bottiglia e determinare se è necessario ridimensionare il cluster per il carico di lavoro.
- Espandere i dettagli di una query specifica selezionandola nella sequenza temporale. Quando l'ID query e altre proprietà vengono visualizzati in una riga sotto il grafico, è possibile scegliere la query per visualizzare i dettagli della query. I dettagli includono, ad esempio, l'istruzione SQL della query, i dettagli di esecuzione e il piano di query. Per ulteriori informazioni, consultare [Visualizzazione dei dettagli delle query](#).
- Determinare se i processi di caricamento vengono completati correttamente e soddisfare i contratti sul livello di servizio (SLA, service level agreement).

Per visualizzare i dati della cronologia delle query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Scegli la scheda Query monitoring (Monitoraggio delle query) per visualizzare i parametri relativi alle query.
4. Nella sezione Monitoraggio della query scegliere la scheda Cronologia di query.

Utilizzando i controlli nella finestra, è possibile attivare/disattivare l'elenco delle query e i parametri del cluster.

Quando si sceglie l'elenco delle query, la scheda include i seguenti grafici:

- Runtime query: l'attività della query in una sequenza temporale. Utilizzare questo grafico per vedere quali query sono in esecuzione nello stesso intervallo di tempo. Scegliere una query per visualizzare ulteriori dettagli di esecuzione delle query. L'asse x mostra il periodo selezionato. È possibile filtrare le query grafiche per in esecuzione, completate, caricamenti e così via. Ogni barra rappresenta una query e la lunghezza della barra rappresenta il suo runtime dall'inizio della barra alla fine. Le query possono includere istruzioni di manipolazione dei dati SQL (ad esempio SELECT, INSERT, DELETE) e caricamenti (ad esempio COPY). Per impostazione predefinita, vengono visualizzate le prime 100 query con esecuzione più lunga per il periodo di tempo selezionato.
- Query e caricamenti: un elenco di query e caricamenti eseguiti nel cluster. La finestra include l'opzione Interrompi query se una query è attualmente in esecuzione.

Quando si sceglie Parametri cluster, la scheda include i seguenti grafici:

- Runtime query: l'attività della query in una sequenza temporale. Utilizzare questo grafico per vedere quali query sono in esecuzione nello stesso intervallo di tempo. Scegliere una query per visualizzare ulteriori dettagli di esecuzione delle query.
- Utilizzo CPU: l'utilizzo della CPU del cluster in base al nodo principale e alla media dei nodi di calcolo.
- Capacità di archiviazione utilizzata: la percentuale della capacità di archiviazione utilizzata.
- Connessioni al database attive: il numero di connessioni al database attive per il cluster.

Quando utilizzi i grafici della cronologia delle query, considera quanto segue:

- Scegli una barra che rappresenti una query specifica nel grafico Query runtime (Runtime query) per visualizzare i dettagli relativi alla query. Inoltre puoi scegliere un ID query nell'elenco Query e caricamenti per visualizzarne i dettagli.
- Puoi scorrere rapidamente per selezionare una sezione del grafico Query runtime (Runtime query) per ingrandire e visualizzare un periodo di tempo specifico.
- Nel grafico Query runtime (Runtime query) per tenere conto di tutti i dati in base al filtro scelto, inoltra tutte le pagine elencate nell'elenco Query e caricamenti.
- Puoi modificare le colonne e il numero di righe visualizzate nell'elenco Query e caricamenti utilizzando la finestra delle preferenze visualizzata dall'icona a forma di ingranaggio delle impostazioni.
- L'elenco Query e caricamenti può essere visualizzato anche dall'icona Query del navigatore a sinistra, Query e caricamenti. Per ulteriori informazioni, consultare [Visualizzazione di query e caricamenti](#).

## Grafici della cronologia delle query

Negli esempi seguenti sono riportati i grafici visualizzati nella nuova console Amazon Redshift.

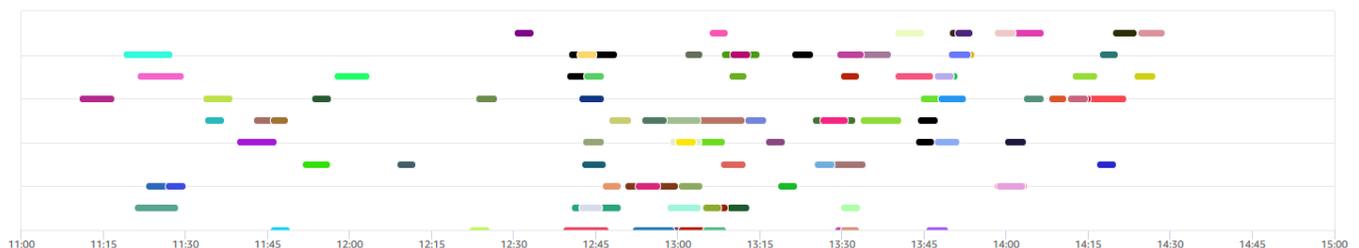
### Note

I grafici della console Amazon Redshift contengono i dati per le 100.000 query più recenti.

### • Query runtime (Runtime query)

#### Query runtime

The query activity on a timeline. Use this graph to see which queries are running in the same timeframe. Choose a query to view more query execution details.



### • Query e caricamenti

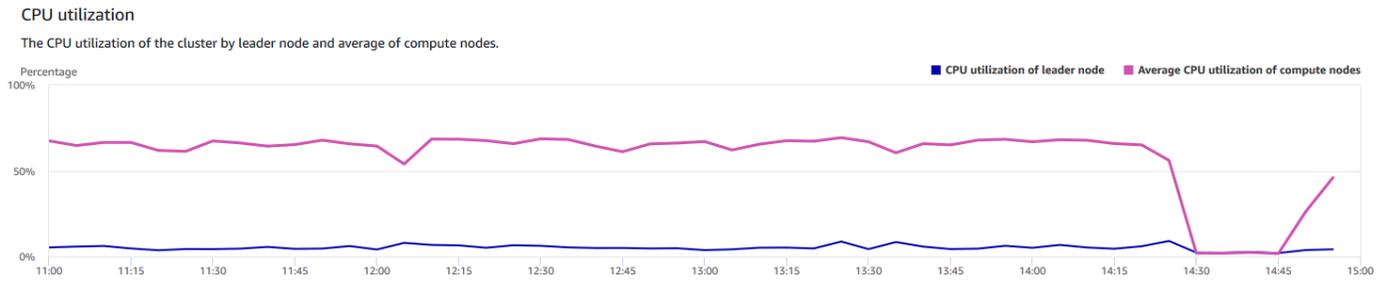
**Queries and loads(100)**

Filter queries

Terminate query

Start time	Query	Status	Duration	SQL	Copy SQL	User	Transaction ID
Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105501
Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105414
Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105283
Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	105128
Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	106659
Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_05cu_run01_nocache.stream-quer ...	Copy	rsperf	101092
Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tp.L0 ICF:IR-09c6a4cc-6ec8-11e a-8047-06872b3fecc8.stream_10cu_run01_nocache.stream-quer ...	Copy	rsperf	104789

• Utilizzo CPU



• Capacità di storage utilizzata



• Active database connections (Connessioni al database attive)



## Visualizzazione dei dati delle prestazioni dei database

È possibile utilizzare i parametri delle prestazioni dei database in Amazon Redshift per completare le seguenti operazioni:

- Analizzare il tempo impiegato dalle query in base alle fasi di elaborazione. Puoi cercare tendenze insolite nella quantità di tempo trascorso in una fase.
- Analizzare il numero di query, la durata e il throughput delle query per intervalli di durata (breve, medio, lungo).
- Cercare le tendenze relative al tempo di attesa della query in base alla priorità della query (Minimo, Basso, Normale, Alto, Massimo, Critico).
- Cercare le tendenze della durata della query, del throughput o del tempo di attesa per coda WLM.

Per visualizzare i dati delle prestazioni dei database

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, incluse le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Scegli la scheda Query monitoring (Monitoraggio delle query) per visualizzare i parametri relativi alle query.
4. Nella sezione Monitoraggio della query scegliere la scheda Database performance (Prestazioni database).

Utilizzando i controlli nella finestra, è possibile attivare/disattivare i parametri del cluster e i parametri della coda WLM.

Quando si sceglie Parametri cluster, la scheda include i seguenti grafici:

- Suddivisione dell'esecuzione del carico di lavoro: il tempo utilizzato nelle fasi di elaborazione delle query.
- Query per intervallo di durata: il numero di query brevi, medie e lunghe.
- Throughput della query: il numero medio di query completate al secondo.
- Durata della query: il tempo medio per il completamento di una query.

- Tempo medio di attesa in coda per priorità: il tempo totale delle query in attesa nella coda WLM per priorità di query.

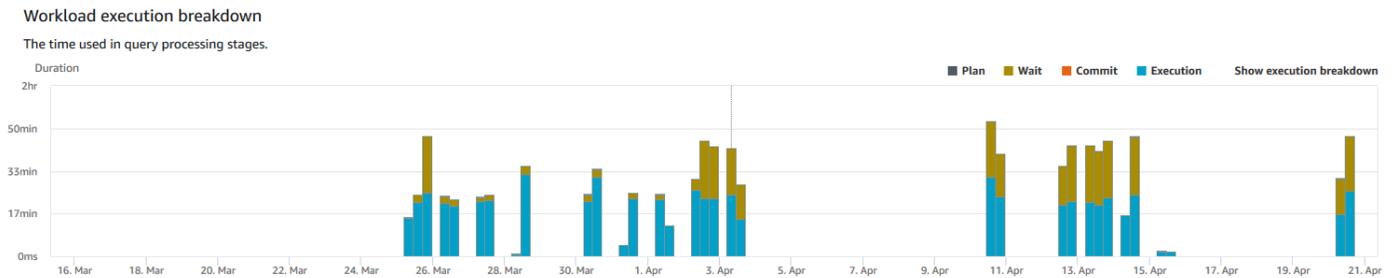
Quando si scelgono i parametri della coda WLM, la scheda include i grafici seguenti:

- Durata query per coda: la durata media della query per coda WLM.
- Throughput query per coda: il numero medio di query completate al secondo per coda WLM.
- Tempo di attesa query per coda: la durata media delle query in attesa per coda WLM.

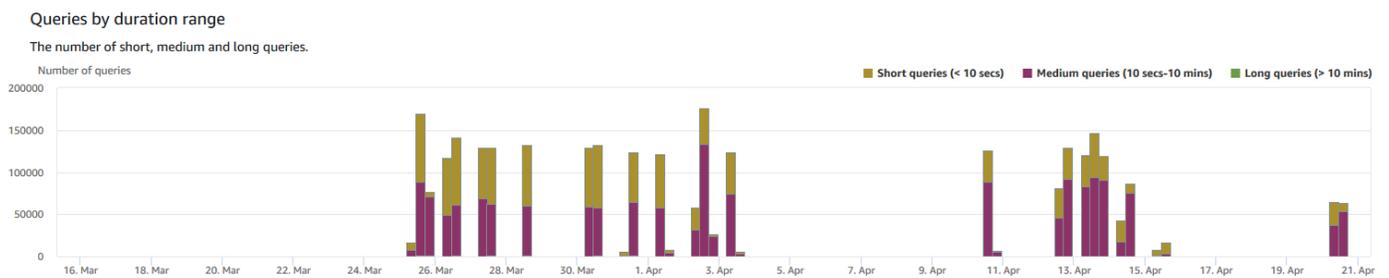
## Grafici delle prestazioni del database

Negli esempi seguenti sono riportati i grafici visualizzati nella nuova console Amazon Redshift.

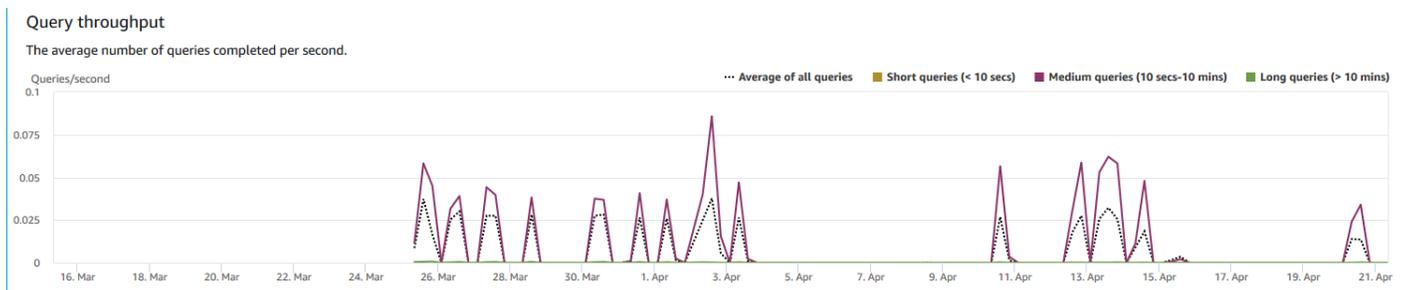
- Suddivisione dell'esecuzione del carico di lavoro



- Queries by duration range (Query per intervallo di durata)



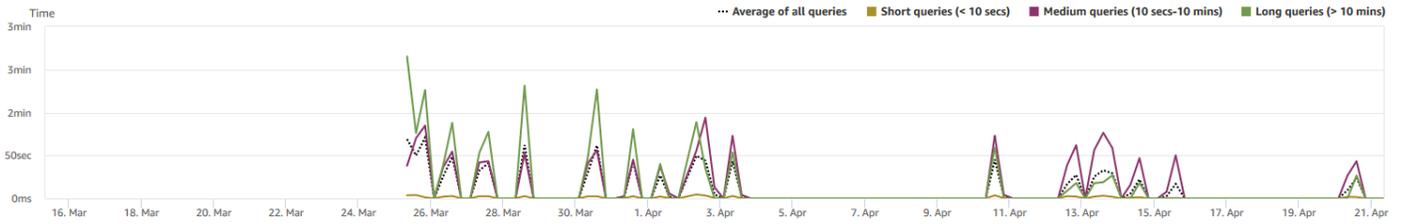
- Volume di elaborazione query



- Durata query

Query Duration

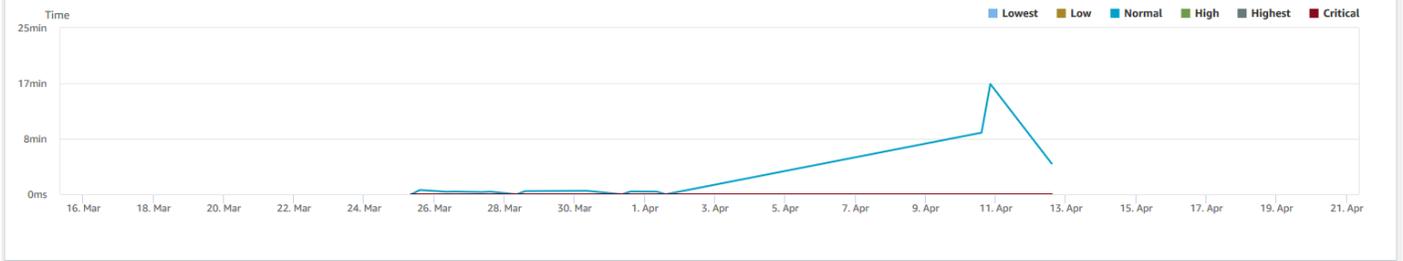
The average amount of time to complete a query.



- Average queue wait time by priority Tempo medio di attesa in coda per priorità

Average queue wait time by priority

The total time queries spent waiting in the WLM queue by query priority.



- Query duration by queue (Durata query per coda)

Query Duration by queue

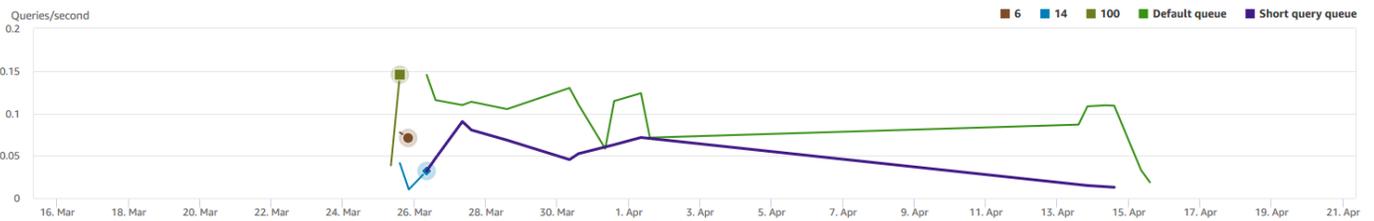
The average query duration by WLM queue.



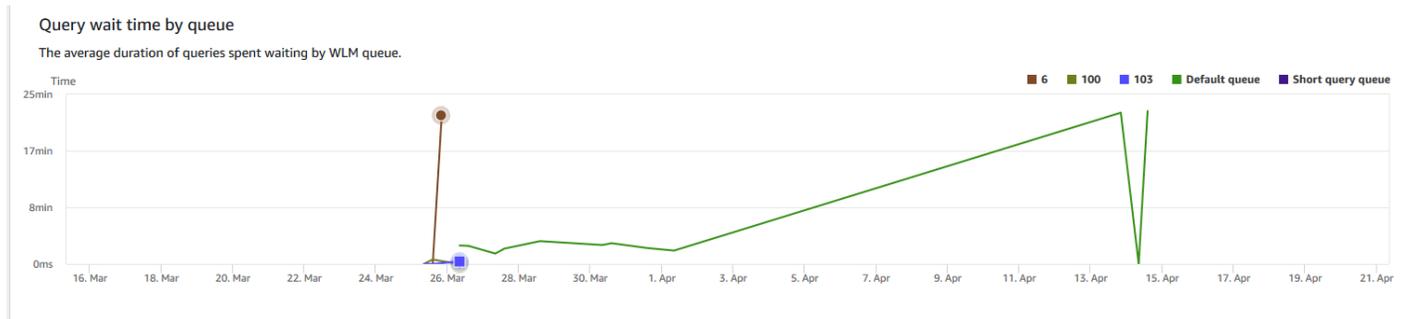
- Query throughput by queue (Throughput query per coda)

Query throughput by queue

The average number of queries completed per second by WLM queue.



- Query wait time by queue (Tempo di attesa query per coda)



## Visualizzazione dei dati relativi alla simultaneità del carico di lavoro e al dimensionamento simultaneo

Utilizzando i parametri di dimensionamento simultaneo in Amazon Redshift, è possibile completare le seguenti operazioni:

- Analizzare se è possibile ridurre il numero di query in coda abilitando il dimensionamento simultaneo. È possibile eseguire il confronto per coda WLM o per tutte le code WLM.
- Visualizzare l'attività di dimensionamento simultaneo nei cluster di dimensionamento simultaneo. Può indicare se il dimensionamento simultaneo è limitato da `max_concurrency_scaling_clusters`. In tal caso, puoi scegliere di aumentare `max_concurrency_scaling_clusters` nel parametro database.
- Visualizzare l'utilizzo totale del dimensionamento simultaneo in tutti i cluster di dimensionamento simultaneo.

Come visualizzare i dati di dimensionamento simultaneo

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Scegli la scheda Query monitoring (Monitoraggio delle query) per visualizzare i parametri relativi alle query.
4. Nella sezione Monitoraggio della query scegliere la scheda Simultaneità del carico di lavoro.

La scheda include i seguenti grafici:

- Query in coda rispetto a query in esecuzione nel cluster: il numero di query in esecuzione (dal cluster principale e dal cluster di dimensionamento simultaneo) rispetto al numero di query in attesa in tutte le code WLM del cluster.
- Query in coda rispetto a query in esecuzione per coda: il numero di query in esecuzione (dal cluster principale e dal cluster di dimensionamento simultaneo) rispetto al numero delle query in attesa in ogni coda WLM.
- Attività di dimensionamento simultaneo: il numero di cluster di dimensionamento simultaneo che elaborano attivamente le query.
- Utilizzo di dimensionamento simultaneo: l'uso dei cluster di dimensionamento simultaneo con attività di elaborazione delle query attive.

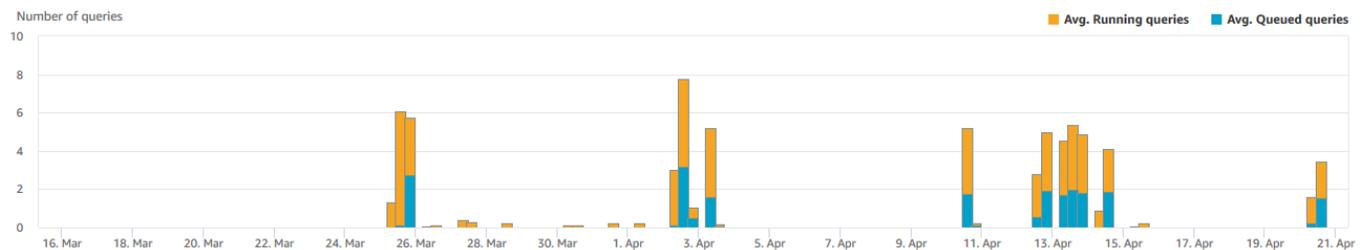
## Grafici di simultaneità del carico di lavoro

Negli esempi seguenti sono riportati i grafici visualizzati nella nuova console Amazon Redshift. Per creare grafici simili in Amazon CloudWatch, puoi utilizzare la scalabilità simultanea e le metriche WLM. CloudWatch Per ulteriori informazioni sui CloudWatch parametri per Amazon Redshift, consulta. [Monitoraggio di Amazon Redshift tramite metriche CloudWatch](#)

- Query in coda rispetto a query in esecuzione nel cluster

Queued vs. Running queries on the cluster

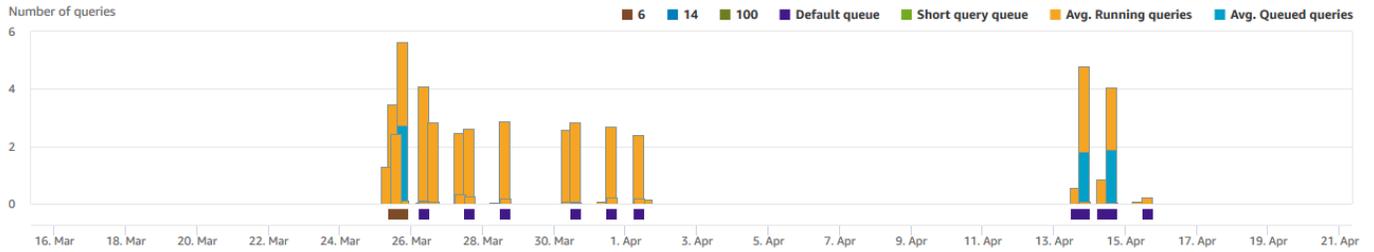
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in all WLM queues in the cluster.



- Query in coda rispetto a query in esecuzione per coda

### Queued vs. Running queries per queue

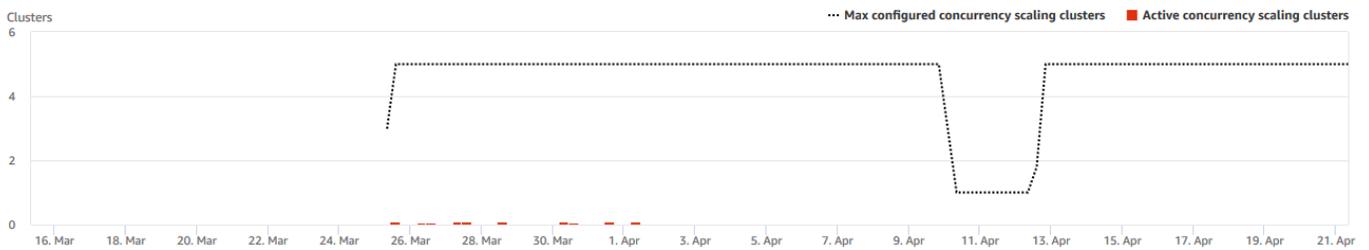
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in each WLM queue.



- Attività di dimensionamento della concorrenza

### Concurrency scaling activity

The number of concurrency scaling clusters that are actively processing queries.



- Modalità dimensionamento della concorrenza

### Concurrency scaling usage

The usage of concurrency scaling clusters that have active query processing activity.



## Visualizzazione di query e caricamenti

La console Amazon Redshift fornisce informazioni su query e caricamenti che vengono eseguiti nel database. Puoi utilizzare queste informazioni per identificare e risolvere i problemi delle query la cui elaborazione richiede molto tempo e che creano colli di bottiglia impedendo un'elaborazione efficace delle altre query. È possibile utilizzare le informazioni sulle query nella console Amazon Redshift per monitorare l'elaborazione delle query.

Per visualizzare i dati relativi alle prestazioni delle query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Queries and loads (Query e carichi) per visualizzare l'elenco delle query dell'account.

Per impostazione predefinita, l'elenco visualizza le query di tutti i cluster delle ultime 24 ore. Puoi modificare l'ambito della data visualizzata nella console.

#### Important

La scheda Query and loads (Query e carichi) mostra le query la cui esecuzione sul sistema è durata più a lungo, fino a un massimo di 100 query.

## Terminazione di una query in esecuzione

Puoi utilizzare la pagina Queries (Query) anche per terminare una query in esecuzione.

#### Note

Per terminare query e carichi nella console Amazon Redshift, è necessario disporre di un'autorizzazione specifica. Se desideri che gli utenti siano in grado di terminare query e carichi, assicurati di aggiungere `redshift:CancelQuerySession` alla tua policy AWS Identity and Access Management (IAM). Questo requisito si applica sia che si selezioni la policy AWS gestita di Amazon Redshift Read Only sia che si crei una policy personalizzata in IAM. Gli utenti che hanno già la policy Amazon Redshift accesso completo dispongono dell'autorizzazione necessaria per terminare query e carichi. Per ulteriori informazioni sulle operazioni nelle policy IAM per Amazon Redshift, consultare [Gestione dell'accesso alle risorse](#).

Per terminare una query in esecuzione

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

2. Dal menu di navigazione, scegliere Queries and loads (Query e carichi) per visualizzare l'elenco delle query dell'account.
3. Scegli la query in esecuzione che desideri terminare nell'elenco e quindi scegli Terminate query (Termina query).

## Visualizzazione dei dettagli delle query

È possibile analizzare i dettagli delle query sulla console Amazon Redshift. Con un identificatore di query è possibile visualizzare i dettagli di una query. I dettagli possono includere, ad esempio, lo stato di completamento della query, la durata, l'istruzione SQL e se si tratta di una query utente o di una query riscritta da Amazon Redshift. A query utente è una query inviata ad Amazon Redshift da un client SQL o generata da uno strumento di business intelligence. Amazon Redshift potrebbe riscrivere la query per ottimizzarla e questo può comportare la riscrittura di diverse query. Sebbene il processo sia eseguito da Amazon Redshift, le query riscritte vengono visualizzate nella pagina dei dettagli della query insieme alla query dell'utente.

Per visualizzare una query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Queries and loads (Query e carichi) per visualizzare l'elenco delle query dell'account. Per individuare la tua query potrebbe essere necessario modificare le impostazioni di questa pagina.
3. Scegli l'identificatore della Query nell'elenco per visualizzare i Query details (Dettagli della query).

La pagina Query details (Dettagli della query) include le schede Query details (Dettagli della query) e Query plan (Piano di esecuzione della query) contenenti i parametri relativi alla query.

Le metriche includono dettagli su una query, ad esempio ora di inizio, ID query, stato e durata. Altri dettagli includono se una query viene eseguita su un cluster principale o su un cluster con dimensionamento simultaneo e se si tratta di una query parent o riscritta.

## Analisi dell'esecuzione delle query

### Per analizzare una query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Queries and loads (Query e carichi) per visualizzare l'elenco delle query dell'account. Per individuare la tua query potrebbe essere necessario modificare le impostazioni di questa pagina.
3. Scegli l'identificatore della Query nell'elenco per visualizzare i Query details (Dettagli della query).

La pagina Query details (Dettagli della query) include le schede Query details (Dettagli della query) e Query plan (Piano di esecuzione della query) contenenti i parametri relativi alla query.

#### Note

È inoltre possibile passare alla pagina Dettagli della query da una pagina Dettagli del cluster, nella scheda Cronologia di query durante la navigazione di una query in un grafico Runtime query.

La pagina Dettagli della query contiene le sezioni riportate di seguito:

- Un elenco di query riscritte, come mostrato nello screenshot seguente.

Rewritten queries <sup>(5)</sup>						
This query was rewritten by Amazon Redshift for optimization						
	Start time	Query	Status	Duration	Executed on	Query type
<input type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927,122928,122929...	✔ Completed	5 min		Parent query
<input checked="" type="radio"/>	Apr 15th, 2020 01:44:44 PM 6 days ago	122927	✔ Completed	4 sec	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122928	✔ Completed	22 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122929	✔ Completed	19 ms	Main	Rewritten query
<input type="radio"/>	Apr 15th, 2020 01:44:48 PM 6 days ago	122931	✔ Completed	5 min	Main	Rewritten query

- Una sezione Dettagli della query come mostrato nello screenshot seguente.

Query details				
Query ID 122927	Cluster dnd-sudhare-qa	User [redacted]	Type Rewritten query	Status Completed
From April 15, 2020 at 01:44:44 PM To April 15, 2020 at 01:44:48 PM				Total runtime 4sec

- Una scheda Dettagli della query contenente l'SQL eseguito e i dettagli relativi all'esecuzione.
- Una scheda Piano di query contenente le fasi del piano di query e altre informazioni. Questa tabella contiene inoltre grafici sul cluster durante l'esecuzione della query.
- Cluster health status (Stato integrità del cluster)

Cluster health status

Cluster health during the workload.



Utilizzo CPU

CPU utilization

The CPU utilization of the cluster by leader node and average of compute nodes.



Capacità di storage utilizzata

Storage capacity used

The percent of the storage capacity used.



Active database connections (Connessioni al database attive)

Active database connections

The number of active database connections to the cluster.



## Visualizzazione delle prestazioni del cluster durante l'esecuzione delle query

Come visualizzare le prestazioni del cluster durante l'esecuzione delle query

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Per ulteriori dettagli scegli la scheda Query monitoring (Monitoraggio delle query).

Per ulteriori informazioni, consulta [Visualizzazione dei dati della cronologia delle query](#).

## Visualizzazione dei parametri del cluster durante le operazioni di caricamento

Quando visualizzi le prestazioni del cluster durante le operazioni di caricamento, puoi identificare le query che consumano risorse e adottare le soluzioni appropriate per attenuarne l'effetto. Puoi terminare un caricamento se non vuoi che venga completato.

### Note

Per terminare query e caricamenti nella console Amazon Redshift, è necessario disporre di un'autorizzazione specifica. Se desideri che gli utenti siano in grado di terminare query e caricamenti, assicurati di aggiungere l'`redshift:CancelQuerySessionazione` alla tua policy AWS Identity and Access Management (IAM). Questo requisito si applica sia che si selezioni la policy AWS gestita da Amazon Redshift Read Only sia che si crei una policy personalizzata in IAM. Gli utenti che hanno già la policy Amazon Redshift accesso completo dispongono dell'autorizzazione necessaria per terminare query e caricamenti. Per ulteriori informazioni sulle operazioni nelle policy IAM per Amazon Redshift, consultare [Gestione dell'accesso alle risorse](#).

Per visualizzare le prestazioni del cluster durante l'esecuzione dei caricamenti

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Per ulteriori dettagli scegli la scheda Query monitoring (Monitoraggio delle query).
4. Nella sezione Queries and loads (Query e caricamenti), scegli Loads (Caricamenti) per visualizzare le operazioni di caricamento di un cluster. Se un caricamento è in esecuzione, puoi terminarlo scegliendo Terminate query (Termina query).

## Analisi delle prestazioni del carico di lavoro

Puoi ottenere una visualizzazione dettagliata delle prestazioni del carico di lavoro osservando la tabella di suddivisione dell'esecuzione del carico di lavoro nella console. Creiamo il grafico con i dati forniti dalla QueryRuntimeBreakdown metrica. Con questo grafico, puoi vedere quanto tempo impiegano le query nelle varie fasi di elaborazione, come attesa e pianificazione.

### Note

Il grafico di suddivisione dell'esecuzione del carico di lavoro non viene mostrato per i cluster a nodo singolo.

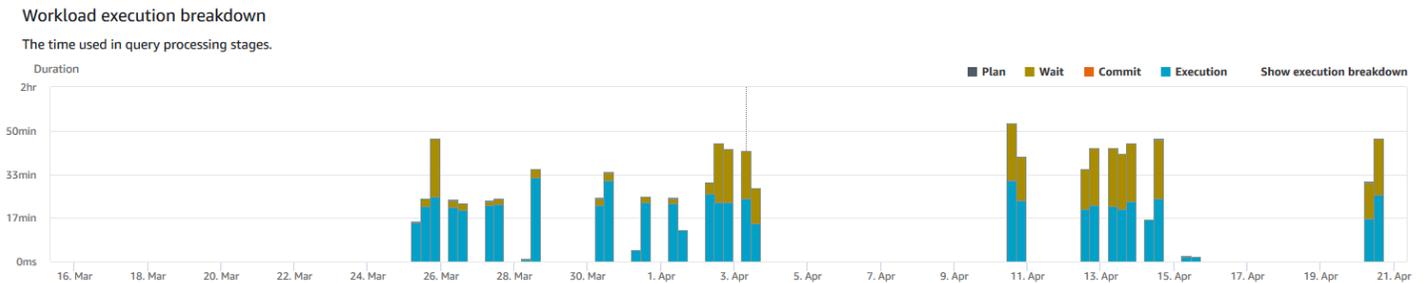
Il seguente elenco di parametri descrive le varie fasi di elaborazione:

- QueryPlanning: tempo trascorso per l'analisi e l'ottimizzazione delle dichiarazioni SQL.
- QueryWaiting: tempo trascorso in attesa nella coda Workload Management (WLM).
- QueryExecutingRead: tempo trascorso per l'esecuzione delle query di lettura.
- QueryExecutingInsert: tempo trascorso per l'esecuzione delle query di inserimento.
- QueryExecutingDelete: tempo trascorso per l'esecuzione delle query di eliminazione.
- QueryExecutingUpdate: tempo trascorso per l'esecuzione delle query di aggiornamento.
- QueryExecutingCtas: tempo trascorso per l'esecuzione di query CREATE TABLE AS (CREA TABELLA COME).

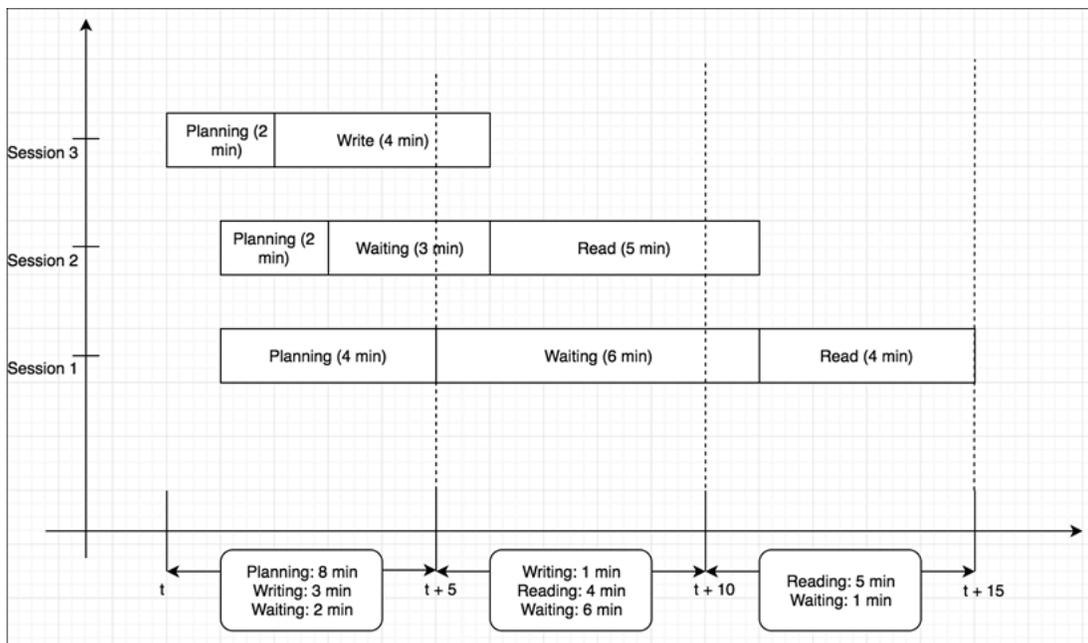
- QueryExecutingUnload: tempo trascorso per l'esecuzione delle query di scaricamento.
- QueryExecutingCopy: tempo trascorso per l'esecuzione delle query di copia.

Ad esempio, il grafico seguente nella console Amazon Redshift mostra il tempo che le query hanno trascorso nelle fasi di pianificazione, attesa, lettura e scrittura. Puoi combinare i risultati di questo grafico con altri parametri per ulteriori analisi. In alcuni casi, il grafico può mostrare che le query di breve durata (come misurato dal parametro QueryDuration) passano molto tempo nella fase di attesa. In questi casi, puoi aumentare il tasso di simultaneità WLM per una determinata coda per aumentare il throughput.

Di seguito, è riportato un esempio del grafico di ripartizione esecuzione del carico di lavoro. Nel grafico, il valore dell'asse y è la durata media di ogni stadio nel tempo specificato mostrato come grafico a barre in pila.



Il diagramma seguente illustra il modo in cui Amazon Redshift aggrega l'elaborazione delle query per le sessioni simultanee.



Per visualizzare il grafico di scomposizione dell'esecuzione del carico di lavoro del cluster

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione scegliere Clusters (Cluster), quindi scegliere dall'elenco il nome del cluster per visualizzarne i dettagli. Vengono visualizzati i dettagli del cluster, che possono includere le schede Prestazioni del cluster, Monitoraggio della query, Database, Condivisioni di dati, Pianificazioni, Manutenzione e Proprietà.
3. Scegli la scheda Query monitoring (Monitoraggio delle query) per visualizzare i parametri relativi alle query.
4. Nella sezione Monitoraggio della query scegliere la scheda Database performance (Prestazioni database) e selezionare Parametri cluster.

I seguenti parametri sono rappresentati sul grafico a barre impilate per l'intervallo di tempo selezionato:

- Tempo di Plan (Pianificazione)
- Tempo di Wait (Attesa)
- Ora di commit
- Ora di esecuzione

## Gestione degli allarmi

Gli allarmi che crei nella console CloudWatch Amazon Redshift sono allarmi. Sono utili in quanto ti consentono di prendere decisioni proattive sul cluster o sull'istanza serverless. Puoi impostare uno o più allarmi per qualsiasi parametro elencato in [Monitoraggio di Amazon Redshift tramite metriche CloudWatch](#). Ad esempio, l'impostazione di un allarme per un valore elevato di `CPUUtilization` su un nodo di cluster consente di determinare quando un nodo è sovrautilizzato. Un allarme per `DataStorage` elevato monitorerebbe lo spazio di archiviazione utilizzato dallo spazio dei nomi serverless per i dati.

Da Operazioni, è possibile modificare o eliminare gli allarmi. Puoi anche creare un avviso chime o slack da CloudWatch cui inviare un avviso a Slack o Amazon Chime specificando l'URL di un webhook per Slack o Amazon Chime.

In questa sezione, viene descritto come creare un allarme utilizzando la console Amazon Redshift. Puoi creare un allarme utilizzando la CloudWatch console o in qualsiasi altro modo in cui lavori con le metriche, ad esempio con o un SDK. AWS CLI AWS

Per creare un CloudWatch allarme con la console Amazon Redshift

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)

Se utilizzi Amazon Redshift serverless, scegli Go to serverless (Vai a serverless) in alto a destra del pannello di controllo.

2. Dal menu di navigazione, scegliere Alarms (Allarmi), quindi scegliere Create alarm (Crea allarme).
3. Nella pagina Crea allarme, inserisci le proprietà per creare un CloudWatch allarme.
4. Scegli Crea allarme.

## Utilizzo delle metriche delle prestazioni nella console CloudWatch

Quando lavori con i parametri di Amazon Redshift nella CloudWatch console, tieni a mente un paio di cose:

- I dati relativi alle prestazioni di query e caricamenti sono disponibili solo nella console Amazon Redshift.
- Alcune metriche CloudWatch hanno unità diverse da quelle utilizzate nella console Amazon Redshift. Ad esempio, `WriteThroughput` viene visualizzato in GB/s (rispetto ai byte/s in CloudWatch), che è un'unità più rilevante per lo spazio di archiviazione tipico di un nodo.

Quando lavori con i parametri di Amazon Redshift nella CloudWatch console, negli strumenti a riga di comando o in un Amazon SDK, tieni a mente questi concetti:

1. Prima di tutto, specifica la dimensione dei parametri da utilizzare. Una dimensione è una coppia nome-valore che consente di identificare un parametro in modo univoco. Le dimensioni per Amazon Redshift sono `ClusterIdentifier` e `NodeID`. Nella CloudWatch console, vengono fornite le Redshift Node viste Redshift Cluster e le viste per selezionare facilmente dimensioni specifiche del cluster e del nodo. Per ulteriori informazioni sulle dimensioni, consulta [Dimensioni](#) nella CloudWatch Developer Guide.
2. Quindi, specifica il nome del parametro, per esempio `ReadIOPS`.

La tabella seguente contiene un riepilogo dei tipi di parametri di Amazon Redshift disponibili. A seconda del parametro, i dati sono disponibili gratuitamente a intervalli di 1 minuto o 5 minuti. Per ulteriori informazioni, consulta [Parametri di Amazon Redshift](#).

CloudWatch namespace	Dimensione	Descrizione
AWS/Redshift	NodeID	Filtra i dati richiesti che sono specifici dei nodi di un cluster. NodeID è "Leader", "Shared" o "Compute-N", dove N è 0, 1, ... per il numero di nodi nel cluster. "Shared" significa che il cluster ha solo un nodo, ovvero che il nodo principale e il nodo di calcolo sono combinati.
	ClusterIdentifier	Filtra i dati richiesti che sono specifici del cluster. I parametri specifici dei cluster includono HealthStatus, MaintenanceMode e DatabaseConnections. I parametri generali per questa dimensione (ad esempio ReadIOPS) che sono anche parametri dei nodi rappresentano un'aggregazione dei dati dei parametri dei nodi. Presta attenzione nell'interpretare questi parametri in quanto aggregano il comportamento di nodi principali e nodi di calcolo.

L'utilizzo di parametri di gateway e volume è simile all'utilizzo di altri parametri di servizio. Molte delle attività più comuni sono descritte nella CloudWatch documentazione, tra cui:

- [Visualizzazione di parametri disponibili](#)
- [Ottenere le statistiche di un parametro](#)
- [Creazione di allarmi CloudWatch](#)

# Eventi di Amazon Redshift

## Argomenti

- [Panoramica degli eventi del cluster](#)
- [Utilizzo di Amazon Simple Notification Service](#)
- [Sottoscrizione alle notifiche degli eventi del cluster di Amazon Redshift](#)
- [Visualizzazione degli eventi del cluster mediante la console](#)
- [Visualizzazione degli eventi del cluster utilizzando AWS CLI l'API Amazon Redshift](#)
- [Gestione delle notifiche degli eventi del cluster](#)
- [Notifiche di eventi Amazon Redshift](#)
- [Notifiche di eventi Serverless di Amazon Redshift con Amazon EventBridge](#)
- [Notifiche di eventi di integrazione zero-ETL con Amazon EventBridge](#)

## Panoramica degli eventi del cluster

Amazon Redshift tiene traccia degli eventi del cluster e conserva le informazioni su di essi per un periodo di diverse settimane nel tuo account. AWS Per ogni evento, Amazon Redshift fornisce informazioni come la data in cui si è verificato, una descrizione, l'origine (ad esempio un cluster, un gruppo di parametri o uno snapshot) e l'ID di origine.

Amazon Redshift fornisce notifiche preventive per alcuni eventi. Questi eventi hanno una categoria di evento `pending`. Ad esempio, inviamo una notifica preventiva se è necessario un aggiornamento dell'hardware per uno dei nodi nel cluster. È possibile effettuare la sottoscrizione agli eventi in sospeso come per gli altri eventi Amazon Redshift. Per ulteriori informazioni, consulta [Sottoscrizione alle notifiche degli eventi del cluster di Amazon Redshift](#).

Puoi utilizzare la console di gestione Amazon Redshift, l'API Amazon Redshift o gli SDK per ottenere informazioni AWS sugli eventi. Puoi ottenere un elenco di tutti gli eventi oppure applicare filtri, come la durata o la data di inizio e di fine dell'evento, per acquisire informazioni su eventi verificatisi in un determinato periodo.

Puoi inoltre ottenere eventi generati da una specifico tipo di origine, ad esempio eventi di cluster o di gruppi di parametri. La colonna Origine mostra il nome della risorsa e il tipo di risorsa che attiva una determinata azione.

È possibile creare abbonamenti a notifiche di eventi di Amazon Redshift che specificano un set di filtri di evento. Quando si verifica un evento che corrisponde alle opzioni di filtro, Amazon Redshift utilizza Amazon Simple Notification Service per informare attivamente del verificarsi dell'evento.

Per un elenco di eventi di Amazon Redshift ordinati per categoria e tipo di origine, consultare [the section called “Categorie di eventi Amazon Redshift e messaggi di evento”](#).

## Utilizzo di Amazon Simple Notification Service

Amazon Redshift utilizza Amazon Simple Notification Service (Amazon SNS) per comunicare le notifiche degli eventi Amazon Redshift. Le notifiche vengono abilitate in seguito alla creazione di una sottoscrizione agli eventi di Amazon Redshift. Nella sottoscrizione ad Amazon Redshift si specifica un set di filtri per gli eventi Amazon Redshift e un argomento Amazon SNS. Ogni volta che si verifica un evento che corrisponde ai criteri di filtro, Amazon Redshift pubblica un messaggio di notifica sull'argomento di Amazon SNS. Amazon SNS trasmette quindi il messaggio a tutti i consumer Amazon SNS che hanno una sottoscrizione Amazon SNS per l'argomento. I messaggi inviati ai consumatori di Amazon SNS possono essere in qualsiasi forma supportata da Amazon SNS per AWS una regione, ad esempio un'e-mail, un messaggio di testo o una chiamata a un endpoint HTTP. Ad esempio, tutte le regioni supportano le notifiche tramite e-mail, ma le notifiche via SMS possono essere create solo nella regione Stati Uniti orientali (Virginia settentrionale).

### Note

Al momento, puoi creare una sottoscrizione di eventi solo per un argomento standard di Amazon SNS (non un argomento FIFO di Amazon SNS). Per ulteriori informazioni, consulta [Origini eventi Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Quando si crea una sottoscrizione alle notifiche di eventi, vengono specificati uno o più filtri di evento. Amazon Redshift invia le notifiche tramite la sottoscrizione ogni volta che si verifica un evento che corrisponde a tutti i criteri di filtro. I criteri di filtro includono il tipo di origine (come cluster o snapshot), l'ID di origine (come il nome di un cluster o uno snapshot), la categoria dell'evento (come Monitoring o Security) e la gravità dell'evento (come INFO o ERROR).

Puoi disattivare facilmente la notifica senza eliminare un abbonamento impostando il pulsante di opzione Enabled su No in AWS Management Console o impostando il Enabled parametro per false utilizzare la CLI o l'API di Amazon Redshift.

La fatturazione per la notifica degli eventi Amazon Redshift avviene tramite Amazon Simple Notification Service (Amazon SNS). L'uso della notifica degli eventi è soggetta alle tariffe di Amazon SNS. Per ulteriori informazioni sulla fatturazione di Amazon SNS, consultare [Prezzi di Amazon Simple Notification Service](#).

È possibile visualizzare gli eventi Amazon Redshift che si sono verificati tramite la console di gestione. Per ulteriori informazioni, consulta [Eventi di Amazon Redshift](#).

## Sottoscrizione alle notifiche degli eventi del cluster di Amazon Redshift

È possibile creare una sottoscrizione alle notifiche di eventi Amazon Redshift per ricevere una notifica quando si verifica un evento relativo a un determinato cluster, snapshot, gruppo di sicurezza o gruppo di parametri. Il modo più semplice per creare una sottoscrizione è utilizzare la console Amazon SNS. Per informazioni sulla creazione di un argomento Amazon SNS e sulla relativa sottoscrizione, consultare [Nozioni di base su Amazon SNS](#).

È possibile creare una sottoscrizione alle notifiche di eventi Amazon Redshift per ricevere una notifica quando si verifica un evento relativo a un determinato cluster, snapshot, gruppo di sicurezza o gruppo di parametri. Il modo più semplice di creare un abbonamento è utilizzare la AWS Management Console. Se si sceglie di creare sottoscrizioni delle notifiche degli eventi tramite la CLI o l'API, è necessario creare un argomento Amazon Simple Notification Service e sottoscrivere l'argomento con la console Amazon SNS o l'API di Amazon SNS. Dovrai inoltre annotare l'Amazon Resource Name (ARN) dell'argomento, in quanto viene utilizzato quando si inviano comandi CLI o operazioni API. Per informazioni sulla creazione di un argomento Amazon SNS e sulla relativa sottoscrizione, consultare [Nozioni di base su Amazon SNS](#).

In una sottoscrizione agli eventi di Amazon Redshift è possibile specificare i seguenti criteri di evento:

- Tipo di origine: i valori sono cluster, snapshot, parameter-groups e security-groups.
- L'ID di origine di una risorsa, ad esempio `my-cluster-1` o `my-snapshot-20130823`. L'ID deve riferirsi a una risorsa nella stessa AWS regione dell'abbonamento all'evento.
- Categoria dell'evento: i valori sono Configuration, Management, Monitoring, e Pending
- Gravità dell'evento: i valori sono INFO o ERROR.

I criteri di evento possono essere specificati indipendentemente, ma per un'ID di origine è dapprima necessario specificare un tipo di origine nella console. Ad esempio, puoi specificare una categoria di

evento senza dover specificare un tipo di origine, un ID di origine o la gravità. Sebbene sia possibile specificare gli ID di origine delle risorse che non sono del tipo specificato nel tipo di origine, nessuna notifica sarà inviata per gli eventi relativi a queste risorse. Ad esempio, se specifichi un tipo di origine per il cluster e l'ID di un gruppo di sicurezza, nessuno degli eventi generati da quel gruppo di sicurezza corrisponde ai criteri di filtro del tipo di origine e di conseguenza nessuna notifica sarà inviata per tali eventi

Amazon Redshift invia una notifica per qualsiasi evento che corrisponde a tutti i criteri specificati in una sottoscrizione. Di seguito sono riportati alcuni esempi di set di eventi restituiti:

- L'abbonamento specifica cluster come tipo di origine, my-cluster-1 come ID di origine, Monitoring come categoria ed ERROR come gravità. L'abbonamento invierà notifiche soltanto per gli eventi di monitoraggio con gravità ERROR di my-cluster-1.
- L'abbonamento specifica cluster come tipo di origine, Configuration come categoria e INFO come gravità. L'abbonamento invierà notifiche per gli eventi di configurazione con una gravità di INFO da qualsiasi cluster Amazon Redshift dell' AWS account.
- L'abbonamento specifica Configuration come categoria e INFO come gravità. L'abbonamento invierà notifiche per gli eventi di configurazione con una gravità di INFO da qualsiasi risorsa Amazon Redshift nell' AWS account.
- L'abbonamento specifica ERROR come gravità. L'abbonamento invierà notifiche per tutti gli eventi con una gravità di ERRORE da qualsiasi risorsa Amazon Redshift nell' AWS account.

Se elimini o rinomini un oggetto il cui nome è un ID di origine in un abbonamento esistente, l'abbonamento rimarrà attivo, ma non verranno inoltrati eventi in relazione a quell'oggetto. Se successivamente crei un nuovo oggetto con lo stesso nome dell'ID di origine nell'abbonamento, l'abbonamento inizierà a inviare le notifiche per gli eventi relativi a quel nuovo oggetto.

Amazon Redshift pubblica notifiche di eventi su un argomento Amazon SNS identificato dal relativo Amazon Resource Name (ARN). Quando si crea una sottoscrizione agli eventi con la console Amazon Redshift, è possibile specificare un argomento Amazon SNS esistente o richiedere alla console di creare l'argomento durante la creazione della sottoscrizione. Tutte le notifiche di eventi Amazon Redshift inviate all'argomento Amazon SNS sono a loro volta trasmesse a tutti i consumer Amazon SNS che hanno effettuato la sottoscrizione a quell'argomento. Utilizzare la console Amazon SNS per apportare modifiche all'argomento Amazon SNS, ad esempio per aggiungere o rimuovere le sottoscrizioni dei consumer all'argomento. Per ulteriori informazioni sulla creazione e la sottoscrizione di argomenti Amazon SNS, consultare [Nozioni di base di Amazon Simple Notification Service](#).

Nelle sezioni seguenti sono elencate tutte le categorie e gli eventi che possono essere notificati. Vengono inoltre fornite informazioni su come sottoscrivere e utilizzare le sottoscrizioni a eventi Amazon Redshift.

## Visualizzazione degli eventi del cluster mediante la console

Per visualizzare gli eventi

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Events (Eventi).

## Visualizzazione degli eventi del cluster utilizzando AWS CLI l'API Amazon Redshift

Per visualizzare gli eventi, è possibile utilizzare la seguente operazione della CLI di Amazon Redshift.

- [describe-events](#)

Amazon Redshift fornisce l'API seguente per visualizzare gli eventi.

- [DescribeEvents](#)

## Gestione delle notifiche degli eventi del cluster

È possibile creare una sottoscrizione alle notifiche di eventi Amazon Simple Notification Service (Amazon SNS) per inviare notifiche quando si verifica un evento relativo a un determinato cluster, snapshot, gruppo di sicurezza o gruppo di parametri di Amazon Redshift. Queste notifiche sono inviate a un argomento SNS, che a sua volta trasmette messaggi a tutti i consumer SNS abbonati all'argomento. I messaggi SNS ai consumatori possono essere in qualsiasi modulo di notifica supportato da Amazon SNS per AWS una regione, ad esempio un'e-mail, un messaggio di testo o una chiamata a un endpoint HTTP. Ad esempio, tutte le regioni supportano le notifiche tramite e-mail, ma le notifiche via SMS possono essere create solo nella regione Stati Uniti orientali (Virginia settentrionale). Per ulteriori informazioni, consulta [Notifiche di eventi Amazon Redshift](#).

# Gestione delle notifiche degli eventi del cluster mediante la console Amazon Redshift

## Creazione di un abbonamento alle notifiche di eventi

Per creare una sottoscrizione a un evento

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/](https://console.aws.amazon.com/redshiftv2/).
2. Dal menu di navigazione, scegliere Events (Eventi).
3. Scegli la scheda Event subscriptions (Sottoscrizioni di eventi), quindi scegli Create event subscription (Crea sottoscrizione di eventi).
4. Inserisci le proprietà della tua sottoscrizione all'evento come nome, tipo di sorgente, categoria e gravità. Per ricevere le notifiche degli eventi è possibile anche abilitare gli argomenti Amazon SNS.
5. Scegli Create Event Subscription (Crea sottoscrizione a eventi) per creare la sottoscrizione.

## Gestione delle notifiche degli eventi del cluster utilizzando AWS CLI l'API Amazon Redshift

È possibile utilizzare le operazioni della CLI di Amazon Redshift seguenti per gestire le notifiche degli eventi del cluster.

- [create-event-subscription](#)
- [delete-event-subscription](#)
- [describe-event-categories](#)
- [describe-event-subscriptions](#)
- [describe-events](#)
- [modify-event-subscription](#)

È possibile utilizzare le operazioni API di Amazon Redshift seguenti per gestire le notifiche di eventi.

- [CreateEventSubscription](#)
- [DeleteEventSubscription](#)

- [DescribeEventCategories](#)
- [DescribeEventSubscriptions](#)
- [DescribeEvents](#)
- [ModifyEventSubscription](#)

Per ulteriori informazioni sulle notifiche di eventi Amazon Redshift, consultare [Notifiche di eventi Amazon Redshift](#).

## Notifiche di eventi Amazon Redshift

### Categorie di eventi Amazon Redshift e messaggi di evento

In questa sezione sono descritte le categorie e gli ID di evento per ogni tipo di origine di Amazon Redshift.

La tabella seguente mostra la categoria di evento e un elenco di eventi quando il tipo di origine è un cluster.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Configurazione	REDSHIFT-EVENT-1000	INFO	Il gruppo di parametri [nome del gruppo di parametri] è stato aggiornato alle [ora]. Se hai modificato solo i parametri dinamici, i cluster associati vengono modificati ora. Se hai modificato i parametri statici, tutti gli aggiornamenti, inclusi i parametri dinamici, verranno applicati quando vengono riavviati i cluster associati.
Configurazione	REDSHIFT-EVENT-1001	INFO	Il cluster Amazon Redshift [nome cluster] è stato modificato per utilizzare il gruppo di parametri [nome gruppo di parametri] alle [ora].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Configurazione	REDSHIFT-EVENT-1500	ERRORE	L'Amazon VPC [nome VPC] non esiste. Le modifiche alla configurazione per il cluster [nome del cluster] non sono state applicate. Accedi alla AWS Management Console per correggere il problema.
Configurazione	REDSHIFT-EVENT-1501	ERRORE	Le sottoreti del cliente [nome sottoreti] specificate per l'Amazon VPC [nome VPC] non esistono o non sono valide. Le modifiche alla configurazione per il cluster [nome del cluster] non sono state applicate. Accedi alla AWS Management Console per correggere il problema.
Configurazione	REDSHIFT-EVENT-1502	ERRORE	Le sottoreti nel gruppo di sottoreti del cluster [nome gruppo sottoreti] non hanno indirizzi IP disponibili. Impossibile creare il cluster [nome cluster].
Configurazione	REDSHIFT-EVENT-1503	ERRORE	All'Amazon VPC [nome VPC] non sono collegati gateway Internet. Le modifiche alla configurazione per il cluster [nome del cluster] non sono state applicate. Visita il sito AWS Management Console per correggere il problema.
Configurazione	REDSHIFT-EVENT-1504	ERRORE	L'HSM per il cluster [nome del cluster] non è accessibile.
Configurazione	REDSHIFT-EVENT-1505	ERRORE	L'HSM per il cluster [nome del cluster] non può essere registrato. Prova un'altra configurazione.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Configurazione	REDSHIFT-EVENT-1506	ERRORE	<p>Amazon Redshift ha superato il limite di interfacce di rete elastiche del tuo account. Elimina fino al [numero massimo di interfacce di rete elastiche] interfacce di rete elastiche o richiedi un aumento limite del numero di interfacce di rete per AWS regione con EC2.</p>
Configurazione	REDSHIFT-EVENT-1509	ERRORE	<p>Il cluster Amazon Redshift [nome cluster] non può essere creato perché è stato raggiunto il limite degli endpoint VPC del tuo account. Eliminare gli endpoint VPC inutilizzati o richiedere un aumento del limite degli endpoint VPC.</p> <p>Per ulteriori informazioni, consultare <a href="#">Endpoint VPC</a> nella Guida per l'utente di Amazon VPC.</p>
Configurazione	REDSHIFT-EVENT-1510	ERRORE	<p>Abbiamo rilevato che il tentativo di caricamento dei dati campione sul cluster Amazon Redshift [nome del cluster] non è riuscito. Per caricare i dati di esempio, è necessario prima configurare il VPC in modo che abbia accesso ai bucket Amazon S3 e poi creare un nuovo cluster e caricare i dati di esempio.</p> <p>Per ulteriori informazioni, consulta <a href="#">Abilitazione del routing VPC avanzato</a> nella Guida alla gestione di Amazon Redshift.</p>

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Configurazione	REDSHIFT-EVENT-1511	ERRORE	Il cluster Amazon Redshift [nome cluster] non può essere creato perché è stato superato il limite degli indirizzi IP elastici del tuo account. Elimina gli indirizzi IP elastici non utilizzati o richiedi un aumento del limite con Amazon EC2.
Gestione	REDSHIFT-EVENT-2000	INFO	Il cluster Amazon Redshift [nome cluster] è stato creato ed è pronto per l'uso.
Gestione	REDSHIFT-EVENT-2001	INFO	Il cluster Amazon Redshift [nome del cluster] è stato eliminato alle [ora]. Uno snapshot finale [è stato/non è stato] salvato.
Gestione	REDSHIFT-EVENT-2002	INFO	Gruppi di sicurezza VPC per il cluster [nome cluster] aggiornati a [ora in UTC].
Gestione	REDSHIFT-EVENT-2003	INFO	La manutenzione è stata avviata sul cluster [nome del cluster] alle [ora in UTC].
Gestione	REDSHIFT-EVENT-2004	INFO	La manutenzione è stata completata sul cluster [nome del cluster] alle [ora in UTC].
Gestione	REDSHIFT-EVENT-2006	INFO	Un ridimensionamento del cluster [nome cluster] è stato avviato alle [ora in UTC]. Il cluster è in modalità di sola lettura.
Gestione	REDSHIFT-EVENT-2007	INFO	È stata confermata una richiesta di ridimensionamento per il cluster [nome del cluster].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-2008	INFO	L'operazione di ripristino per creare un nuovo snapshot [nome snapshot] del cluster Amazon Redshift [nome cluster] è stato avviato alle [ora]. Per monitorare l'avanzamento del ripristino, accedi alla AWS Management Console.
Gestione	REDSHIFT-EVENT-2013	INFO	Il cluster Amazon Redshift [cluster name] è stato rinominato alle [ora].
Gestione	REDSHIFT-EVENT-2014	INFO	È stata ricevuta una richiesta di ripristino di tabella per il cluster Amazon Redshift [nome cluster].
Gestione	REDSHIFT-EVENT-2015	INFO	Il ripristino della tabella è stato annullato per il cluster Amazon Redshift [nome del cluster] alle [ora].
Gestione	REDSHIFT-EVENT-2016	INFO	La sostituzione del cluster Amazon Redshift [nome cluster] è stata avviata alle [ora].
Gestione	REDSHIFT-EVENT-2017	INFO	La manutenzione iniziata dal cliente è stata avviata sul cluster Amazon Redshift [nome del cluster] alle [ora]. È possibile che il cluster non sia disponibile durante la manutenzione.
Gestione	REDSHIFT-EVENT-2018	INFO	La manutenzione iniziata dal cliente è stata completata sul cluster Amazon Redshift [nome del cluster] alle [ora].
Gestione	REDSHIFT-EVENT-2019	ERRORE	Si è verificato un errore durante la manutenzione iniziata dal cliente sul cluster Amazon Redshift [nome del cluster] alle [ora]. Viene ripristinato lo stato originale del cluster.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-2020	INFO	La traccia del cluster Amazon Redshift [nome del cluster] è stata modificata da [traccia iniziale] a [traccia corrente].
Gestione	REDSHIFT-EVENT-2021	ERRORE	L'[operazione] del cluster Amazon Redshift [nome cluster] non è riuscita durante l'acquisizione di capacità dal pool di capacità. Stiamo lavorando per acquisire capacità, ma per ora abbiamo annullato la tua richiesta. Elimina il cluster e riprova in un secondo momento.
Gestione	REDSHIFT-EVENT-2022	ERRORE	L'[operazione] del cluster Amazon Redshift [nome cluster] non è riuscita durante l'acquisizione di capacità dal pool di capacità. Stiamo lavorando per acquisire capacità, ma per ora abbiamo annullato la tua richiesta. La capacità è disponibile in [zone di disponibilità alternative]. Elimina il cluster e riprova in una zona di disponibilità alternativa.
Gestione	REDSHIFT-EVENT-2023	ERRORE	Abbiamo rilevato un errore dell'hardware nel cluster Amazon Redshift a nodo singolo [nome cluster], che potrebbe aver causato query non riuscite o disponibilità intermittente del cluster. La sostituzione del cluster non è riuscita durante l'acquisizione di capacità dal pool di capacità. Dovrai ripristinare un nuovo cluster da una snapshot. Elimina il cluster, seleziona l'ultima snapshot disponibile e ripristina un nuovo cluster dalla snapshot. Verrà eseguito assegnato automaticamente hardware integro.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-2024	ERRORE	Abbiamo rilevato un errore dell'hardware nel cluster Amazon Redshift a nodo singolo [nome cluster], che potrebbe aver causato query non riuscite o disponibilità intermittente del cluster. La sostituzione del cluster non è riuscita durante l'acquisizione di capacità dal pool di capacità. La capacità è disponibile in zona di disponibilità: [zone di disponibilità alternative]. Elimina il cluster, seleziona l'ultima snapshot disponibile e ripristina un nuovo cluster dalla snapshot. Verrà eseguito assegnato automaticamente hardware integro.
Gestione	REDSHIFT-EVENT-3011	INFO	Un ridimensionamento elastico del cluster Amazon Redshift "[nome cluster]" è stato avviato alle [ora]. Le connessioni del database verranno mantenute durante il ridimensionamento. Durante l'operazione potrebbe verificarsi la chiusura o il timeout di alcune query e connessioni.
Gestione	REDSHIFT-EVENT-3012	INFO	Abbiamo ricevuti una richiesta di ridimensionamento elastico per il cluster "[nome cluster]" avviata alle [ora]. All'avvio del ridimensionamento, verrà fornita una notifica di evento.
In attesa	REDSHIFT-EVENT-2025	INFO	Il database per il cluster <nome cluster> sarà aggiornato tra le <ora di inizio> e le <ora di fine>. Il cluster non sarà accessibile. Pianifica le attività di conseguenza.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
In attesa	REDSHIFT-EVENT-2026	INFO	Il cluster <nome cluster> sarà aggiornato tra le <ora di inizio> e le <ora di fine>. Il cluster non sarà accessibile. Pianifica le attività di conseguenza.
Monitoraggio	REDSHIFT-EVENT-2050	INFO	È stato rilevato un problema hardware sul cluster Amazon Redshift [nome del cluster]. Una richiesta di sostituzione è stata avviata alle [ora].
Monitoraggio	REDSHIFT-EVENT-3000	INFO	Il cluster Amazon Redshift [cluster name] è stato riavviato alle [time].
Monitoraggio	REDSHIFT-EVENT-3001	INFO	Un nodo sul cluster Amazon Redshift [nome cluster] è stato automaticamente sostituito alle [ora] e il cluster funziona normalmente.
Monitoraggio	REDSHIFT-EVENT-3002	INFO	Il ridimensionamento del cluster Amazon Redshift [nome cluster] è stato completato e il cluster è disponibile per operazioni di lettura e scrittura. Il ridimensionamento è stato avviato alle [ore] ed è stato completato in [ore] ore.
Monitoraggio	REDSHIFT-EVENT-3003	INFO	Il cluster Amazon Redshift [cluster name] è stato creato correttamente dallo snapshot [nome snapshot] ed è disponibile per l'uso.
Monitoraggio	REDSHIFT-EVENT-3007	INFO	Lo snapshot di Amazon Redshift [nome snapshot] è stato copiato correttamente da [regione di origine] a [AWS regione di destinazione] in [ora AWS].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3008	INFO	Il ripristino della tabella è stato avviato per il cluster Amazon Redshift [nome cluster] alle [ora].
Monitoraggio	REDSHIFT-EVENT-3009	INFO	Il ripristino della tabella è stato completato correttamente per il cluster Amazon Redshift [nome cluster] alle [ora].
Monitoraggio	REDSHIFT-EVENT-3010	ERRORE	Il ripristino della tabella per il cluster Amazon Redshift [nome cluster] non è riuscito alle [ora].
Monitoraggio	REDSHIFT-EVENT-3013	ERRORE	L'operazione di ridimensionamento elastico richiesta per il cluster Amazon Redshift [nome cluster] non è riuscita alle [ora] a causa di [motivo].
Monitoraggio	REDSHIFT-EVENT-3014	INFO	Il cluster [cluster name] è stato riavviato da Amazon Redshift alle [time].
Monitoraggio	REDSHIFT-EVENT-3500	ERRORE	Si è verificato un errore durante il ridimensionamento del cluster Amazon Redshift [nome del cluster]. Un nuovo tentativo di ridimensionamento verrà eseguito tra qualche minuto.
Monitoraggio	REDSHIFT-EVENT-3501	ERRORE	Si è verificato un errore alle [ora] durante l'operazione di ripristino per creare un cluster Amazon Redshift [nome del cluster] a partire dallo snapshot [nome dello snapshot]. Esegui di nuovo l'operazione.
Monitoraggio	REDSHIFT-EVENT-3504	ERRORE	Il bucket Amazon S3 [nome bucket] non è valido per la registrazione del cluster [nome cluster].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3505	ERRORE	Il bucket Amazon S3 [nome bucket] non dispone delle policy IAM corrette per il cluster [nome del cluster].
Monitoraggio	REDSHIFT-EVENT-3506	ERRORE	Il bucket Amazon S3 [nome del bucket] non esiste. La registrazione non può continuare per il cluster [nome del cluster].
Monitoraggio	REDSHIFT-EVENT-3507	ERRORE	Il cluster Amazon Redshift [nome del cluster] non può essere creato mediante l'EIP (indirizzo IP). Questo EIP è già in uso.
Monitoraggio	REDSHIFT-EVENT-3508	ERRORE	Il cluster Amazon Redshift [nome del cluster] non può essere creato mediante l'EIP (indirizzo IP). Non è possibile trovare l'EIP.
Monitoraggio	REDSHIFT-EVENT-3509	ERRORE	La copia dello snapshot tra regioni non è abilitata per il cluster [cluster name].
Monitoraggio	REDSHIFT-EVENT-3510	ERRORE	Il ripristino della tabella per il cluster Amazon Redshift [nome cluster] non è stato avviato alle [ora]. Motivo: [motivo].
Monitoraggio	REDSHIFT-EVENT-3511	ERRORE	Il ripristino della tabella per il cluster Amazon Redshift [nome cluster] non è riuscito alle [ora].
Monitoraggio	REDSHIFT-EVENT-3512	ERRORE	Si è verificato un errore nel cluster Amazon Redshift [nome del cluster] a causa di un problema hardware. È in corso il ripristino automatico del cluster a partire dall'ultimo snapshot [nome dello snapshot] creato alle [ore].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3513	ERRORE	Si è verificato un errore nel cluster Amazon Redshift [nome del cluster] a causa di un problema hardware. È in corso il ripristino automatico del cluster a partire dall'ultimo snapshot [nome dello snapshot] creato alle [ore]. Tutte le modifiche al database apportate dopo quest'ora dovranno essere ripetute.
Monitoraggio	REDSHIFT-EVENT-3514	ERRORE	Si è verificato un errore nel cluster Amazon Redshift [nome del cluster] a causa di un problema hardware. Il cluster viene posto in stato di errore hardware. Elimina il cluster ed esegui il ripristino a partire dall'ultimo snapshot [nome dello snapshot] creato alle [ore].
Monitoraggio	REDSHIFT-EVENT-3515	ERRORE	Si è verificato un errore nel cluster Amazon Redshift [nome del cluster] a causa di un problema hardware. Il cluster viene posto in stato di errore hardware. Elimina il cluster ed esegui il ripristino a partire dall'ultimo snapshot [nome dello snapshot] creato alle [ore]. Tutte le modifiche al database apportate dopo quest'ora dovranno essere ripetute.
Monitoraggio	REDSHIFT-EVENT-3516	ERRORE	Si è verificato un errore nel cluster Amazon Redshift [nome cluster] a causa di un problema hardware e non sono disponibili backup per il cluster. Il cluster viene posto in stato di errore hardware e può essere eliminato

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3519	INFO	Il riavvio del cluster [nome del cluster] è iniziato alle [ora].
Monitoraggio	REDSHIFT-EVENT-3520	INFO	Il riavvio del cluster [nome del cluster] è stato completato alle [ora].
Monitoraggio	REDSHIFT-EVENT-3521	INFO	È stato rilevato un problema di connettività sul cluster "[nome del cluster]". Un controllo di diagnostica automatico è stato avviato alle [ora].
Monitoraggio	REDSHIFT-EVENT-3522	INFO	Si è verificato un errore durante l'operazione di recupero sul cluster "[nome del cluster]" alle [ore]. Il team Amazon Redshift sta lavorando su una soluzione.
Monitoraggio	REDSHIFT-EVENT-3533	ERRORE	Il ridimensionamento del cluster "[nome cluster]" è stato annullato alle [ora]. L'operazione è stata annullata perché [motivo]. [operazione richiesta].
Monitoraggio	REDSHIFT-EVENT-3534	INFO	Il ridimensionamento elastico del cluster Amazon Redshift "[nome cluster]" è stato completato alle [ora]. Il cluster è ora disponibile per le operazioni di lettura e scrittura mentre vengono trasferiti i dati. Alcune query possono richiedere più tempo per il completamento del trasferimento dei dati.
Monitoraggio	REDSHIFT-EVENT-3537	INFO	Il trasferimento dei dati del cluster '[nome cluster]' è stato completato alle [ora in UTC].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3600	INFO	L'operazione di ridimensionamento per il cluster Amazon Redshift "[nome cluster]" è stata annullata in passato. Il rollback è stato completato alle [ora].
In attesa	REDSHIFT-EVENT-3601	INFO	Un nodo nel cluster <nome cluster> sarà sostituito tra le <ora di inizio> e le <ora di fine>. Non puoi rinviare questa operazione e di manutenzione. Pianifica le attività di conseguenza.
In attesa	REDSHIFT-EVENT-3602	INFO	La sostituzione di un nodo nel cluster <nome cluster> è pianificata tra le <ora di inizio> e le <ora di fine>. Il cluster non sarà accessibile. Pianifica le attività di conseguenza.
Gestione	REDSHIFT-EVENT-3603	INFO	L'operazione di ripristino per creare un cluster [nome del cluster] a partire dallo snapshot [nome dello snapshot] non è riuscita a causa di un errore interno. Il cluster viene posto in stato di ripristino non compatibile e può essere eliminato. Prova a ripristinare lo snapshot in un cluster con una configurazione differente.
Gestione	REDSHIFT-EVENT-3614	INFO	L'azione pianificata [nome azione pianificata] è stata creata in [ora in UTC]. La prima chiamata è programmata alle [ora in UTC].
Gestione	REDSHIFT-EVENT-3615	INFO	L'azione pianificata [nome azione pianificata] è pianificata alle [ora in UTC].
Monitoraggio	REDSHIFT-EVENT-3616	INFO	L'azione pianificata [nome azione pianificata] alle [ora in UTC] è terminata con lo stato "SUCCEEDED".

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3617	ERRORE	L'azione pianificata [nome azione pianificata] è stata ignorata alle [ora in UTC] a causa di un ritardo.
Monitoraggio	REDSHIFT-EVENT-3618	INFO	L'operazione di sospensione del cluster [nome cluster] è stata avviata alle [ora UTC]. Sospensione iniziata
Monitoraggio	REDSHIFT-EVENT-3619	INFO	Il cluster Amazon Redshift [nome del cluster] è stato messo in pausa alle [ora UTC].
Gestione	REDSHIFT-EVENT-3626	INFO	L'azione pianificata [nome azione pianificata] è stata modificata alle [ora in UTC]. La prima chiamata è programmata alle [ora in UTC].
Gestione	REDSHIFT-EVENT-3627	INFO	L'azione pianificata [nome azione pianificata] è stata eliminata alle [ora in UTC].
Monitoraggio	REDSHIFT-EVENT-3628	ERRORE	L'azione pianificata [nome azione pianificata] alle [ora in UTC] è terminata con lo stato "FAILED".
Gestione	REDSHIFT-EVENT-3629	INFO	Amazon Redshift [nome del cluster] ha ricevuto la tua richiesta di rilocalizzazione. Al termine della rilocalizzazione della zona di disponibilità, Amazon Redshift invia una notifica di evento.
Gestione	REDSHIFT-EVENT-3630	INFO	Il cluster Amazon Redshift [nome del cluster] è stato correttamente rilocato da [zona di disponibilità] a [zona di disponibilità]. È possibile utilizzare il cluster ora.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-3631	INFO	Amazon Redshift ha correttamente rilocato il cluster Amazon Redshift [nome cluster] da [zona di disponibilità] a [zona di disponibilità] per il recupero.
Gestione	REDSHIFT-EVENT-3632	INFO	Amazon Redshift ha temporaneamente disabilitato la rilocazione del cluster per il cluster Amazon Redshift [nome cluster] a causa di modifiche alla configurazione. Riprovare la rilocazione del cluster in un secondo momento.
Monitoraggio	REDSHIFT-EVENT-3658	ERRORE	Migrazione da EC2 Classic a EC2 VPC non riuscita per il cluster Redshift [ID cluster].
Monitoraggio	REDSHIFT-EVENT-3659	INFO	Migrazione da EC2 Classic a EC2 VPC non riuscita per il cluster Redshift [ID cluster].
Monitoraggio	REDSHIFT-EVENT-3660	INFO	Il cluster viene posto in stato di errore hardware. Elimina il cluster EC2 Classic ed esegui il ripristino del cluster EC2 VPC a partire dall'ultimo snapshot [nome dello snapshot] creato alle [ore in formato UTC].
Gestione	REDSHIFT-EVENT-3666	INFO	Il cluster Amazon Redshift Multi-AZ [nome del cluster] ha rilevato un errore in [ora in UTC] e ha attivato un ripristino automatico.
Gestione	REDSHIFT-EVENT-3667	INFO	Il cluster Amazon Redshift Multi-AZ [nome cluster] è stato ripristinato con successo a [ora in UTC] ed è disponibile per l'uso in [prima zona di disponibilità]. L'elaborazione secondari a in un'altra zona sarà disponibile a breve.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3668	ERRORE	Il cluster Amazon Redshift Multi-AZ [nome cluster] non è stato ripristinato in [ora in UTC].
Gestione	REDSHIFT-EVENT-3669	INFO	Il cluster Amazon Redshift Multi-AZ [nome cluster] è stato ripristinato con successo a [ora in UTC] ed è disponibile per l'uso con risorse di calcolo sia dalla [prima zona di disponibilità] che dalla [seconda zona di disponibilità].
Gestione	REDSHIFT-EVENT-3670	INFO	La manutenzione sul cluster Amazon Redshift [nome del cluster] è stata completata in [ora in UTC] ed è disponibile per l'uso con risorse di calcolo nella [prima zona di disponibilità]. L'elaborazione secondaria in un'altra zona sarà disponibile a breve.
Gestione	REDSHIFT-EVENT-3671	INFO	Il ridimensionamento sul cluster Amazon Redshift [nome del cluster] è stato completato al [ora in UTC] ed è disponibile per l'uso in [prima zona di disponibilità]. L'elaborazione secondaria in un'altra zona sarà disponibile a breve.
Gestione	REDSHIFT-EVENT-3672	INFO	Il cluster Amazon Redshift Multi-AZ [nome del cluster] ha rilevato un errore nella [seconda zona di disponibilità] a [ora in UTC] e ha attivato un ripristino automatico.
Gestione	REDSHIFT-EVENT-3673	INFO	L'operazione per abilitare Multi-AZ per il cluster Amazon Redshift [nome cluster] è iniziata al [ora in UTC].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-3674	INFO	L'operazione per abilitare Multi-AZ per il cluster Amazon Redshift [nome cluster] è stata completata con successo in [ora in UTC].
Monitoraggio	REDSHIFT-EVENT-3675	ERRORE	L'operazione per abilitare Multi-AZ per il cluster Amazon Redshift [nome cluster] non è riuscita in [ora in UTC].
Gestione	REDSHIFT-EVENT-3676	INFO	L'operazione per disabilitare Multi-AZ per il tuo cluster Amazon Redshift Multi-AZ [nome cluster] è iniziata il [ora in UTC].
Gestione	REDSHIFT-EVENT-3677	INFO	L'operazione per disabilitare Multi-AZ per il tuo cluster Amazon Redshift [nome cluster] è stata completata con successo in [ora in UTC].
Monitoraggio	REDSHIFT-EVENT-3678	ERRORE	L'operazione per disabilitare Multi-AZ per il tuo cluster Amazon Redshift [nome cluster] non è riuscita in [ora in UTC].
Configurazione	REDSHIFT-EVENT-3679	INFO	La porta del cluster Amazon Redshift [nome cluster] è stata modificata correttamente.
Configurazione	REDSHIFT-EVENT-3680	ERRORE	Amazon Redshift non è riuscito a creare il cluster [nome cluster] perché il ruolo collegato al servizio (SLR, Service Linked Role) necessario per questa operazione non è accessibile. Riprova la creazione dalla console di Amazon Redshift. Amazon Redshift creerà automaticamente il ruolo collegato al servizio (SRL).

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Monitoraggio	REDSHIFT-EVENT-3684	ERRORE	Il tuo bucket Amazon S3 [nome del bucket] è stato crittografato con una chiave sconosciuta o inaccessibile. AWS KMS Modifica la crittografia del bucket Amazon S3.
Gestione	REDSHIFT-EVENT-3685	ERRORE	L'operazione di ripristino sul cluster [nome del cluster] non è riuscita perché lo spazio su disco disponibile non è sufficiente. È in corso il rollback dell'operazione. Prova a eseguire il ripristino in un cluster con una configurazione diversa.
Gestione	REDSHIFT-EVENT-3686	ERRORE	L'operazione di ridimensionamento sul cluster [nome del cluster] non è riuscita perché lo spazio su disco disponibile non è sufficiente. È in corso il rollback dell'operazione. Prova a ridimensionare in un cluster con una configurazione diversa.
Sicurezza	REDSHIFT-EVENT-4000	INFO	Le credenziali amministratore del cluster Amazon Redshift [nome cluster] sono state aggiornate alle [ora].
Sicurezza	REDSHIFT-EVENT-4001	INFO	Il gruppo di sicurezza [nome del gruppo di sicurezza] è stato modificato alle [ora]. Le modifiche saranno applicate automaticamente a tutti i cluster associati.
Sicurezza	REDSHIFT-EVENT-4500	ERRORE	Il gruppo di sicurezza [nome del gruppo di sicurezza] fornito non è valido. Le modifiche alla configurazione per il cluster [nome del cluster] non sono state applicate. Visita il sito AWS Management Console per correggere il problema.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Sicurezza	REDSHIFT-EVENT-4501	ERRORE	Non è possibile trovare il gruppo di sicurezza [nome del gruppo di sicurezza] specificato nel gruppo di sicurezza del cluster [nome del gruppo di sicurezza del cluster]. L'autorizzazione non può essere completata.
Sicurezza	REDSHIFT-EVENT-4502	ERRORE	Le credenziali amministratore per il cluster Amazon Redshift [nome cluster] non sono state aggiornate alle [ora] a causa di attività simultanea. Consentire al carico di lavoro corrente di completare o ridurre il carico di lavoro attivo, quindi ritentare l'operazione.
Sicurezza	REDSHIFT-EVENT-4503	ERRORE	Amazon Redshift non è in grado di accedere al segreto del cluster [nome del cluster].
Sicurezza	REDSHIFT-EVENT-4504	ERRORE	Amazon Redshift non è in grado di accedere alla chiave KMS [chiave KMS] utilizzata per crittografare il segreto delle credenziali dell'amministratore per il cluster [nome del cluster].
Sicurezza	REDSHIFT-EVENT-4505	ERRORE	Amazon Redshift non è in grado di modificare il segreto del cluster [nome del cluster] perché sul cluster è in corso un'operazione.
Sicurezza	REDSHIFT-EVENT-4506	ERRORE	Il cluster [nome del cluster] Amazon Redshift è sospeso. Amazon Redshift non è in grado di ruotare i segreti dei cluster sospesi.

Nella tabella seguente sono indicati la categoria di evento e un elenco di eventi quando il tipo di origine è un gruppo di parametri.

Categorie ed eventi per il tipo di origine gruppo di parametri

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Configurazione	REDSHIFT-EVENT-1002	INFO	Il parametro [nome del parametro] è stato aggiornato da [valore] a [valore] alle [time].
Configurazione	REDSHIFT-EVENT-1003	INFO	Il gruppo di parametri del cluster [nome del gruppo] è stato creato.
Configurazione	REDSHIFT-EVENT-1004	INFO	Il gruppo di parametri del cluster [nome del gruppo] è stato eliminato.
Configurazione	REDSHIFT-EVENT-1005	INFO	Il gruppo di parametri del cluster [nome del gruppo] è stato aggiornato alle [time]. Se hai modificato solo i parametri dinamici, i cluster associati vengono modificati ora. Se hai modificato i parametri statici, tutti gli aggiornamenti, inclusi i parametri dinamici, verranno applicati quando vengono riavviati i cluster associati.

Le tabelle seguenti indicano la categoria di evento e un elenco di eventi quando il tipo di origine è un gruppo di sicurezza.

#### Categorie ed eventi per il tipo di origine gruppi di sicurezza

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Sicurezza	REDSHIFT-EVENT-4002	INFO	Il gruppo di sicurezza del cluster [nome del gruppo] è stato creato.

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Sicurezza	REDSHIFT-EVENT-4003	INFO	Il gruppo di sicurezza del cluster [nome del gruppo] è stato eliminato.
Sicurezza	REDSHIFT-EVENT-4004	INFO	Il gruppo di sicurezza del cluster [nome del gruppo] è stato modificato alle [time]. Le modifiche saranno applicate automaticamente a tutti i cluster associati.

Le tabelle seguenti indicano la categoria di evento e un elenco di eventi quando il tipo di origine è uno snapshot.

Categorie ed eventi per il tipo di origine snapshot

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-2009	INFO	Uno snapshot utente [nome snapshot] per il cluster Amazon Redshift [nome cluster] è stato avviato alle [ora]. Per monitorare l'avanzamento dello snapshot, accedi alla AWS Management Console.
Gestione	REDSHIFT-EVENT-2010	INFO	Lo snapshot utente [nome snapshot] per il cluster Amazon Redshift [nome cluster] è stato annullato alle [ora].
Gestione	REDSHIFT-EVENT-2011	INFO	Lo snapshot utente [nome dello snapshot] per il cluster Amazon Redshift [nome cluster] è stato eliminato alle [ora].

Categoria di Amazon Redshift	ID evento	Gravità dell'evento	Descrizione
Gestione	REDSHIFT-EVENT-2012	INFO	Lo snapshot finale [nome dello snapshot] per il cluster Amazon Redshift [nome del cluster] è stato avviato alle [ora].
Monitoraggio	REDSHIFT-EVENT-3004	INFO	Lo snapshot utente [nome snapshot] per il cluster Amazon Redshift [nome cluster] è stato completato correttamente alle [ora].
Monitoraggio	REDSHIFT-EVENT-3005	INFO	Lo snapshot finale [nome] per il cluster Amazon Redshift [nome] è stato completato o senza errori alle [ora].
Monitoraggio	REDSHIFT-EVENT-3006	INFO	Lo snapshot finale [nome dello snapshot] per il cluster Amazon Redshift [nome del cluster] è stato annullato alle [ora].
Monitoraggio	REDSHIFT-EVENT-3502	ERRORE	Si è verificato un errore durante lo snapshot finale [nome snapshot] per il cluster Amazon Redshift [nome cluster] alle [ora]. Il team sta lavorando a una soluzione. Visita il sito AWS Management Console per riprovare l'operazione.
Monitoraggio	REDSHIFT-EVENT-3503	ERRORE	Si è verificato un errore durante lo snapshot utente [nome snapshot] per il cluster Amazon Redshift [nome cluster] alle [ora]. Il team sta lavorando a una soluzione. Visita il sito AWS Management Console per riprovare l'operazione.

# Notifiche di eventi Serverless di Amazon Redshift con Amazon EventBridge

Amazon Redshift Serverless utilizza Amazon EventBridge per gestire le notifiche degli eventi per tenerti aggiornato up-to-date sulle modifiche nel tuo data warehouse. Amazon EventBridge è un servizio di bus eventi senza server che puoi utilizzare per connettere le tue applicazioni con dati provenienti da una varietà di fonti. In questo caso, l'origine dell'evento è Amazon Redshift. Gli eventi, che sono modifiche monitorate in un ambiente, vengono inviati EventBridge automaticamente dal tuo data warehouse Amazon Redshift. Gli eventi vengono recapitati quasi in tempo reale.

Le funzionalità EventBridge includono la fornitura di un ambiente in cui scrivere regole di eventi, in grado di specificare le azioni da intraprendere per eventi specifici. È inoltre possibile impostare obiettivi, ovvero risorse a cui EventBridge inviare un evento. Una destinazione può includere una destinazione API, un gruppo di CloudWatch log Amazon e altri. Per ulteriori informazioni sulle regole, consulta le [EventBridge regole di Amazon](#). Per ulteriori informazioni sugli obiettivi, consulta [Amazon EventBridge targets](#).

Gli eventi possono essere classificati in gravità e categorie. I filtri disponibili sono:

- Resource filtering (Filtro delle risorse): ricevi i messaggi in base alla risorsa a cui sono associati gli eventi. Le risorse includono un gruppo di lavoro, uno snapshot e così via.
- Time window filtering (Filtraggio finestra temporale): esamina gli eventi in un determinato periodo di tempo.
- Filtro delle categorie: ricevi notifiche di eventi per tutti gli eventi nelle categorie specificate.

La tabella seguente include gli eventi Amazon Redshift Serverless, con metadati aggiuntivi:

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
RateChange	REDSHIFT-SERVERLESS-EVENT-1001	INFO	Modifica RPU di base del gruppo di lavoro completata correttamente alle <ora in UTC>.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
RateChange	REDSHIFT-SERVERLESS-EVENT-1002	ERRORE	Modifica RPU di base del gruppo di lavoro non completata alle <ora in UTC>.
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1003	INFO	Il software è stato aggiornato sul tuo data warehouse Amazon Redshift <nome endpoint> alle <ora in UTC>.
Configurazione	REDSHIFT-SERVERLESS-EVENT-1011	ERRORE	Amazon Redshift Serverless non è riuscito a creare un gruppo di lavoro [nome del gruppo di lavoro] perché il ruolo legato al servizio (SLR, Service Linked Role) necessario per questa operazione non è accessibile. Riprova la creazione dalla console di Amazon Redshift. Amazon Redshift creerà automaticamente il ruolo collegato al servizio (SRL).

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1029	ERRORE	La modifica della RPU di base del gruppo di lavoro non è stata completata in [ora in UTC] perché lo spazio su disco disponibile non è sufficiente. Riprova con una configurazione diversa.
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1500	ERRORE	Impossibile creare o aggiornare il gruppo di lavoro <nome gruppo di lavoro> in quanto hai superato il limite di indirizzi IP elastici per il tuo account. Elimina gli indirizzi IP elastici inutilizzati o richiedi un aumento del limite con Amazon EC2.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1501	ERRORE	La sottorete <ID sottorete> non ha indirizzi IP disponibili. Ciò impedirà l'esecuzione corretta dei seguenti tipi di query sul gruppo di lavoro <nome gruppo di lavoro>: EMR, query federate, COPY/UNLOAD da Amazon EC2. Per risolvere il problema, libera gli IP nella tua sottorete eliminando le ENI.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1502	ERRORE	La sottorete <ID sottorete> non ha indirizzi IP disponibili. Ciò impedirà la corretta esecuzione dei tipi di query Amazon EMR, query federate Redshift, Redshift COPY/ UNLOAD e Redshift ML nel gruppo di lavoro <nome gruppo di lavoro>. Per risolvere il problema, libera gli IP nella tua sottorete eliminando le interfacce di rete elastiche (ENI) non utilizzate.
Gestione	REDSHIFT-SERVERLESS-EVENT-1008	INFO	Il gruppo di lavoro Amazon Redshift <nome gruppo di lavoro> è stato creato ed è pronto per l'uso.
Gestione	REDSHIFT-SERVERLESS-EVENT-1009	INFO	Il tuo gruppo di lavoro Amazon Redshift <nome gruppo di lavoro> è stato eliminato alle <ora in UTC>.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-SERVERLESS-EVENT-1000	INFO	Snapshot <nome snapshot> completato correttamente alle <ora in UTC>.
Gestione	REDSHIFT-SERVERLESS-EVENT-1004	INFO	Ripristino dallo snapshot sullo spazio dei nomi <nome spazio dei nomi> completato correttamente alle <ora in UTC>.
Gestione	REDSHIFT-SERVERLESS-EVENT-1005	ERRORE	Ripristino dallo snapshot sullo spazio dei nomi <nome spazio dei nomi> non riuscito alle <ora in UTC>.
Gestione	REDSHIFT-SERVERLESS-EVENT-1006	INFO	Ripristino dal punto di ripristino sullo spazio dei nomi <nome spazio dei nomi> completato correttamente alle <ora in UTC>.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Gestione	REDSHIFT-SERVERLESS-EVENT-1007	INFO	Ripristino dal punto di ripristino sullo spazio dei nomi <nome spazio dei nomi> non riuscito alle <ora in UTC>.
Sicurezza	REDSHIFT-SERVERLESS-EVENT-1012	ERRORE	Amazon Redshift non è in grado di accedere al segreto dello spazio dei nomi <nome dello spazio dei nomi>.
Sicurezza	REDSHIFT-SERVERLESS-EVENT-1013	ERRORE	Amazon Redshift non è in grado di accedere alla chiave KMS utilizzata per crittografare il segreto delle credenziali di amministratore per lo spazio dei nomi <nome dello spazio dei nomi>.
Sicurezza	REDSHIFT-SERVERLESS-EVENT-1014	ERRORE	Amazon Redshift non è in grado di ruotare il segreto dello spazio dei nomi <nome dello spazio dei nomi> perché nel gruppo di lavoro è in corso un'operazione.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Sicurezza	REDSHIFT-SERVERLESS-EVENT-1015	ERRORE	Allo spazio dei nomi <nome dello spazio dei nomi> non è associato un gruppo di lavoro. Amazon Redshift può ruotare i segreti solo per gli spazi dei nomi a cui sono associati gruppi di lavoro.
Sicurezza	REDSHIFT-SERVERLESS-EVENT-1016	INFO	Credenziali di amministratore aggiornate per lo spazio dei nomi <nome dello spazio dei nomi> alle <ora UTC>.

## Notifiche di eventi di integrazione zero-ETL con Amazon EventBridge

L'integrazione Zero-ETL utilizza Amazon EventBridge per gestire le notifiche degli eventi per tenerti aggiornato up-to-date sulle modifiche nelle tue integrazioni. Amazon EventBridge è un servizio di bus eventi senza server che puoi utilizzare per connettere le tue applicazioni con dati provenienti da una varietà di fonti. In questo caso, l'origine dell'evento è Amazon Redshift. Gli eventi, che sono modifiche monitorate in un ambiente, vengono inviati EventBridge automaticamente dal tuo data warehouse Amazon Redshift. Gli eventi vengono distribuiti pressoché in tempo reale.

EventBridge fornisce un ambiente in cui scrivere regole relative agli eventi, che possono specificare le azioni da intraprendere per eventi specifici. È inoltre possibile impostare obiettivi, ovvero risorse a cui EventBridge inviare un evento. Una destinazione può includere una destinazione API, un gruppo

di CloudWatch log Amazon e altri. Per ulteriori informazioni sulle regole, consulta le [EventBridge regole di Amazon](#). Per ulteriori informazioni sugli obiettivi, consulta [Amazon EventBridge targets](#).

Gli eventi possono essere classificati in gravità e categorie. I filtri disponibili sono:

- Filtro delle risorse: ricevi i messaggi in base alla risorsa a cui sono associati gli eventi. Le risorse sono un gruppo di lavoro o uno snapshot.
- Time window filtering (Filtraggio finestra temporale): esamina gli eventi in un determinato periodo di tempo.
- Filtro delle categorie: ricevi notifiche di eventi per tutti gli eventi nelle categorie specificate.

La tabella seguente illustra gli eventi di integrazione Zero-ETL con metadati aggiuntivi:

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0000	INFO	L'integrazione Zero-ETL <nome integrazione> è stata creata ed è attiva.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0001	INFO	L'integrazione Zero-ETL <nome integrazione> è stata eliminata alle <ora UTC>.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0002	INFO	L'eliminazione dell'integrazione zero-ETL <nome integrazione> è stata avviata alle <ora UTC>.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0003	INFO	L'integrazione Zero-ETL <nome integrazione> sta

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
			sincronizzando i dati transazionali nel data warehouse di destinazione.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0004	WARNING	Una o più tabelle non dispongono di una chiave primaria e non possono essere sincronizzate. Esegui un backup su Amazon RDS, rilascia queste tabelle e ricrea seguendo le best practice di Amazon Redshift per la progettazione delle tabelle.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0005	WARNING	Una o più tabelle non possono essere sincronizzate perché contengono tipi o lunghezze di dati non supportati. Correggi le tabelle e riprova. Per ulteriori informazioni sui tipi di dati, consulta <a href="#">Unsupport ed data types</a> .

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0006	ERRORE	Impossibile creare l'integrazione. Elimina e ricrea l'integrazione.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0007	ERRORE	Impossibile caricare i dati a causa di un errore interno. Elimina e ricrea l'integrazione.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0008	ERRORE	Autorizzazione non riuscita perché le autorizzazioni sono state revocate dal cluster DB del cluster DB Aurora DB di origine. Elimina e ricrea l'integrazione.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0009	ERRORE	Impossibile inviare dati ad Amazon Redshift perché il numero di tabelle e schemi supera il limite di Amazon Redshift. Elimina e ricrea l'integrazione.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0012	ERRORE	È stato richiamato un ripristino dal punto di ripristino sullo spazio dei nomi serverless di destinazione. Elimina e ricrea l'integrazione.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0013	INFO	L'integrazione Zero-ETL <nome integrazione> è attiva.
Monitoraggio	REDSHIFT-INTEGRATION-EVENT-0014	ERRORE	L'integrazione <nome integrazione> non è riuscita perché non è stato possibile modificarla a causa di un errore interno. Elimina e ricrea l'integrazione. Se l'errore persiste, contatta l'AWS assistenza.
Operazione	REDSHIFT-INTEGRATION-EVENT-0015	INFO	Alla tabella <schema.name> è stata applicata la modifica DDL <modifica DDL>.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Operazione	REDSHIFT-INTEGRATION-EVENT-0016	INFO	L'integrazione Zero-ETL <nome integrazione> sta elaborando una richiesta di modifica con i seguenti argomenti: <copia degli argomenti della richiesta>.
Operazione	REDSHIFT-INTEGRATION-EVENT-0017	INFO	La modifica all'integrazione Zero-ETL <nome integrazione> è stata applicata.
Operazione	REDSHIFT-INTEGRATION-EVENT-0018	WARNING	Il cluster Amazon Redshift di destinazione è in fase di sospensione. Attendi che il completamento della sospensione, quindi riprendi il cluster per continuare lo streaming di dati.
Operazione	REDSHIFT-INTEGRATION-EVENT-0019	WARNING	Il cluster Amazon Redshift di destinazione è in fase di sospensione. Riprendi il cluster per continuare lo streaming di dati.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Operazione	REDSHIFT-INTEGRATION-EVENT-0020	WARNING	Il cluster Amazon Redshift di destinazione è in fase di recupero. Attendi che il cluster sia attivo per continuare lo streaming di dati.
Configurazione	REDSHIFT-INTEGRATION-EVENT-1000	ERRORE	Uno o più parametri sul cluster DB del cluster Aurora DB di origine non sono configurati correttamente. Correggi il gruppo di parametri e riavvia il cluster per applicare le modifiche, quindi ricrea l'integrazione.
Configurazione	REDSHIFT-INTEGRATION-EVENT-1001	ERRORE	L'integrazione non è riuscita perché il valore del parametro <code>enable_case_sensitive_identifier</code> non è corretto. Imposta il valore su <code>true</code> per il cluster DB del cluster DB Aurora DB di origine, quindi elimina e ricrea l'integrazione.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Configurazione	REDSHIFT-INTEGRATION-EVENT-1002	ERRORE	L'integrazione non è riuscita perché il valore del parametro <code>cdc_insert_enabled</code> non è corretto. Imposta il valore su <code>true</code> per il cluster DB del cluster DB Aurora DB di origine, quindi elimina e ricrea l'integrazione.
Configurazione	REDSHIFT-INTEGRATION-EVENT-1003	ERRORE	Il parametro <code>binlog_format</code> nel gruppo di parametri del cluster di database di origine deve essere impostato su <code>ROW</code> . Correggi il gruppo di parametri e riavvia il cluster per applicare la modifica, quindi ricrea l'integrazione.

Categoria di Amazon Redshift	ID evento esterno	Gravità dell'evento	Descrizione messaggio
Configurazione	REDSHIFT-INTEGRATION-EVENT-1004	ERRORE	Impossibile caricare i dati perché il parametro del cluster <code>binlog_transaction_compression</code> è abilitato. Imposta il valore del parametro su OFF e riavvia l'istanza di scrittura per applicare la modifica, quindi ricrea l'integrazione.
Configurazione	REDSHIFT-INTEGRATION-EVENT-1005	ERRORE	Impossibile caricare i dati perché il parametro del cluster <code>binlog_row_value_options</code> è impostato su PARTIAL_JSON, che non è supportato. Correggi il gruppo di parametri e riavvia l'istanza di scrittura per applicare la modifica, quindi ricrea l'integrazione.
Configurazione	REDSHIFT-INTEGRATION-EVENT-1006	WARNING	Impossibile analizzare e il filtro di integrazione. Correggi la sintassi del filtro.

## Quote e limiti in Amazon Redshift

Amazon Redshift prevede quote che limitano l'uso di diverse risorse nel tuo AWS account per regione. AWS Esiste un valore predefinito per ogni quota e alcune quote sono regolabili. Per le quote regolabili, puoi richiedere un aumento per il tuo AWS account in una AWS regione inviando un modulo di aumento del limite di [Amazon Redshift](#).

### Quote per gli oggetti Amazon Redshift

Amazon Redshift è caratterizzato da quote che limitano l'utilizzo di diversi tipi di oggetto. Esiste un valore predefinito per ciascuno.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
AWS account che è possibile autorizzare a ripristinare un'istanza per istantanea	20	No	Il numero massimo di AWS account che è possibile autorizzare per ripristinare un'istanza, per istantanea.
AWS account che è possibile autorizzare a ripristinare un'istanza per	100	No	Il numero massimo di AWS account che puoi autorizzare a ripristinare un'istanza, per chiave KMS. Ciò significa che se si hanno 10 snapshot crittografati con una singola chiave KMS, sarà possibile autorizzare 10 account AWS per ripristinare ogni snapshot o altre combinazioni fino a raggiungere 100 account, senza superare 20 account per ogni snapshot.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
AWS KMS key			
Ruoli IAM in cluster per Amazon Redshift per accedere ad altri servizi AWS	50 <sup>1</sup>	No	<p>Il numero massimo di ruoli IAM che puoi associare a un cluster per autorizzare Amazon Redshift ad accedere ad AWS altri servizi per l'utente proprietario del cluster e dei ruoli IAM.</p> <p><sup>1</sup> La quota è 10 nei seguenti casi Regioni AWS: us-iso-east -1, -1, us-iso-west us-isob-east -1.</p>
Livello di simultaneità (slot di query) per tutte le code WLM manuali definite dall'utente	50	No	Numero massimo di slot di query per tutte le code definite dall'utente definite dalla gestione manuale del carico di lavoro.
Cluster di dimensionamento simultaneo	10	Sì	Il numero massimo di cluster di dimensionamento simultaneo.
Nodi DC2 in un cluster	128	Sì	Numero massimo di nodi DC2 che è possibile assegnare a un cluster. Per ulteriori informazioni sui limiti correnti per ogni tipo di nodo, consultare <a href="#">Cluster e nodi in Amazon Redshift</a> .

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Abbonamenti a eventi	20	Sì	Il numero massimo di abbonamenti agli eventi per questo account nella AWS regione corrente.
Nodi	200	Sì	Il numero massimo di nodi in tutte le istanze di database per questo account nella regione corrente AWS .
Gruppi di parametri	20	No	Il numero massimo di gruppi di parametri per questo account nella AWS regione corrente.
Nodi RA3 in un cluster	128	Sì	Numero massimo di nodi RA3 che è possibile assegnare a un cluster. Per ulteriori informazioni sui limiti correnti per ogni tipo di nodo, consultare <a href="#">Cluster e nodi in Amazon Redshift</a> .
Endpoint VPC gestiti da RedShift connessi a un cluster	30	Sì	Il numero massimo di endpoint VPC gestiti da Redshift che è possibile connettere a un cluster. Per ulteriori informazioni sull'uso di endpoint VPC gestiti da Redshift, consultare <a href="#">Utilizzo degli endpoint VPC gestiti da RedShift</a> .
Assegnatari al cluster a cui si accede tramite un endpoint VPC gestito da RedShift	5	Sì	Il numero massimo di assegnatari che un proprietario del cluster può autorizzare per la creazione di un endpoint VPC gestito da RedShift per un cluster. Per ulteriori informazioni sull'uso di endpoint VPC gestiti da Redshift, consultare <a href="#">Utilizzo degli endpoint VPC gestiti da RedShift</a> .

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Endpoint VPC gestiti da RedShift per autorizzazione	5	Sì	Il numero massimo di endpoint VPC gestiti da Redshift che è possibile creare per l'autorizzazione. Per ulteriori informazioni sull'uso di endpoint VPC gestiti da Redshift, consultare <a href="#">Utilizzo degli endpoint VPC gestiti da RedShift</a> .
Nodi riservati	200	Sì	Il numero massimo di nodi riservati per questo account nella AWS regione corrente.
Schemi in ogni database per cluster	9.900	No	Numero massimo di schemi che è possibile creare in ogni database, per cluster. Tuttavia, gli schemi <code>pg_temp_*</code> non contano ai fini di questa quota.
Gruppi di sicurezza	20	Sì	Il numero massimo di gruppi di sicurezza per questo account nella AWS regione corrente.
Dimensione e riga singola durante il caricamento da COPY	4	No	La dimensione massima (in MB) di una riga singola durante il caricamento tramite il comando COPY.
Snapshot	700	Sì	Il numero massimo di istantanee utente per questo account nella AWS regione corrente.
Gruppi di sottoreti	20	Sì	Il numero massimo di gruppi di sottoreti per questo account nella regione corrente AWS .

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Sottorete in un gruppo di sottoreti	20	Sì	Numero massimo di sottoreti per un gruppo di sottoreti.
Tabelle per il tipo di nodo cluster large	9.900	No	Numero massimo di tabelle per il tipo di nodo cluster di grandi dimensioni. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.
Tabelle per il tipo di nodo cluster xlarge	9.900	No	Numero massimo di tabelle per il tipo di nodo cluster xlarge. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Tabelle per tipo di nodo del cluster x1plus con cluster a nodo singolo.	9.900	No	Il numero massimo di tabelle per il tipo di nodo cluster x1plus con un cluster a nodo singolo. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee e includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.
Tabelle per tipo di nodo del cluster x1plus con cluster a più nodi.	20.000	No	Il numero massimo di tabelle per il tipo di nodo cluster x1plus con un cluster a più nodi. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee e includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Tabelle per il tipo di nodo cluster 4xlarge	200.000	No	Numero massimo di tabelle per il tipo di nodo cluster 4xlarge. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.
Tabelle per il tipo di nodo cluster 8xlarge	200.000	No	Numero massimo di tabelle per il tipo di nodo cluster 8xlarge. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.
Tabelle per il tipo di nodo cluster 16xlarge	200.000	No	Numero massimo di tabelle per il tipo di nodo cluster 16xlarge. Questo limite include tabelle permanenti, tabelle temporanee, tabelle di unità di condivisione dati e visualizzazioni materializzate. Le tabelle esterne vengono conteggiate come tabelle temporanee. Le tabelle temporanee includono tabelle temporanee definite dall'utente e tabelle temporanee create da Amazon Redshift durante l'elaborazione delle query o la manutenzione del sistema. Le visualizzazioni e le tabelle di sistema non sono incluse in questo limite.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Numero di database	60	No	Il numero massimo consentito di database in un cluster di Amazon Redshift. Ciò esclude i database creati dalle unità di condivisione dati.
Timeout per sessioni inattive o non attive	4 ore	No	Questa impostazione si applica al cluster. Per informazioni sull'impostazione del valore di timeout della sessione di inattività per un utente, consultare e <a href="#">ALTER USER</a> nella Guida per gli sviluppatori di database di Amazon Redshift Database. L'impostazione utente ha la precedenza sull'impostazione del cluster.
Timeout per transazioni inattive	6 ore	No	Il periodo massimo di inattività per una transazione aperta prima che Amazon Redshift termini la sessione associata alla transazione. Questa impostazione ha la precedenza su tutte le impostazioni di timeout per inattività definite dall'utente. Si applica al cluster.
Procedure archiviate e in un database	10.000	No	Il numero massimo di procedure archiviate. Consulta <a href="#">Limiti e differenze per il supporto alle procedure archiviate</a> per altri limiti.
Numero massimo di connessioni per nodi RA3	2.000	No	Il numero massimo di connessioni a un cluster RA3. (Ciò si applica in particolare ai tipi di nodo ra3.xlplus, ra3.4xlarge, e ra3.16xlarge.) Il numero massimo di connessioni consentite varia in base al tipo di nodo.
Numero massimo di connessioni per i nodi DC2	Può variare	No	Il numero massimo di connessioni a un cluster dc2.large è 500. Il numero massimo di raccolte per un cluster dc2.8xlarge è 2000.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Numero di ruoli Amazon Redshift in un cluster	1.000	Sì	Il numero massimo di ruoli Amazon Redshift che puoi creare per cluster. Per ulteriori informazioni sui ruoli di controllo degli accessi basato sui ruoli (RBAC), consulta <a href="#">Controllo accessi basato sui ruoli (RBAC)</a> nella Guida per sviluppatori di database di Amazon Redshift

## Quote per gli oggetti Amazon Redshift Serverless

Amazon Redshift dispone di quote che limitano l'utilizzo di diversi tipi di oggetto nell'istanza Amazon Redshift Serverless. Esiste un valore predefinito per ciascuno.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Numero di database	100	No	Il numero massimo consentito di database in uno spazio di nomi di Amazon Redshift serverless. Ciò esclude i database creati dalle unità di condivisione dati.
Numero di schemi	9.900	No	Il numero massimo consentito di schemi in un'istanza di Amazon Redshift Serverless.
Numero di tabelle	200.000	No	Il numero massimo consentito di tabelle in un'istanza di Amazon Redshift Serverless.
Timeout per sessioni inattive o non attive	1 ora	No	Per informazioni sull'impostazione del valore di timeout della sessione di inattività per un utente, consultare <a href="#">ALTER USER</a> nella Guida per gli sviluppatori di database di Amazon Redshift Database. L'impostazione definita dall'utente ha la precedenza.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Timeout per una query in esecuzione	86.399 secondi (24 ore)	No	Tempo massimo di esecuzione di una query prima che Amazon Redshift la termini.
Timeout per transazioni inattive	6 ore	No	Il periodo massimo di inattività per una transazione aperta prima che Amazon Redshift Serverless termini la sessione associata alla transazione. Questa impostazione ha la precedenza su tutte le impostazioni di timeout per inattività definite dall'utente.
Numero massimo di connessioni	2000	No	Il numero massimo di connessioni consentite per connettersi a un gruppo di lavoro.
Numero di gruppi di lavoro	25	Sì	Numero di gruppi di lavoro supportati.
Numero di spazi dei nomi	25	Sì	Numero di spazi dei nomi supportati.
Numero di ruoli Amazon Redshift in un gruppo di lavoro	1.000	Sì	Il numero massimo di ruoli Amazon Redshift che puoi creare per gruppo di lavoro. Per ulteriori informazioni sui ruoli di controllo degli accessi basati sui ruoli (RBAC), consulta <a href="#">Controllo accessi basato sui ruoli (RBAC)</a> nella Guida per sviluppatori di database di Amazon Redshift

Per ulteriori informazioni su come la fatturazione serverless di Amazon Redshift è influenzata dalla configurazione del timeout, consulta [Fatturazione per Amazon Redshift Serverless](#).

## Quote per l'API di dati Amazon Redshift

Amazon Redshift dispone di quote che limitano l'utilizzo dell'API di dati Amazon Redshift. Esiste un valore predefinito per ciascuno. Per ulteriori informazioni sull'API di dati Amazon Redshift, consulta [Uso dell'API dati di Amazon Redshift](#).

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Transazioni al secondo (TPS) per l'API BatchExecuteStatement	20	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API CancelStatement	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API DescribeStatement	100	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Transazioni al secondo (TPS) per l'API DescribeTable	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API ExecuteStatement	30	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API GetStatementResult	20	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API ListDatabases	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Transazioni al secondo (TPS) per l'API ListSchemas	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API ListStatements	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.
Transazioni al secondo (TPS) per l'API ListTables	3	No	Il numero massimo di richieste di operazioni al secondo che è possibile effettuare senza essere sottoposti a throttling.

## Quote per gli oggetti dell'editor di query v2

Amazon Redshift dispone di quote che limitano l'utilizzo di diversi tipi di oggetto nell'editor di query v2 di Amazon Redshift. Esiste un valore predefinito per ciascuno.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Connessioni	500	Sì	Numero massimo di connessioni che è possibile creare utilizzando l'editor della query v2 in questo account nella regione corrente.
Principi attivi per account	50	Sì	Numero massimo di responsabili simultanei che possono utilizzare l'editor di query v2 in questo account nella regione corrente.
Query salvate	2.500	Sì	Numero massimo di query salvate che è possibile creare utilizzando l'editor della query v2 in questo account nella regione corrente.
Versioni di query	20	Sì	Numero massimo di versioni per query che è possibile creare utilizzando l'editor della query v2 in questo account nella regione corrente.
Grafici salvati	500	Sì	Numero massimo di grafici salvati che è possibile creare utilizzando l'editor della query v2 in questo account nella regione corrente.
Righe recuperate per query	100.000	No	Il numero massimo di righe recuperate per query dall'editor di query v2 in questo account nella regione corrente.
Dimensioni dei dati recuperati per query	5	No	Dimensione massima, in megabyte, dei dati recuperati per query dall'editor di query v2 in questo account nella regione corrente.
Connessioni socket simultanee per principale	10	Sì	Numero massimo di connessioni simultanee socket per l'editor della query v2 che un singolo principale può stabilire nella regione corrente. Valutare se aumentare questa quota se si ricevono errori che le connessioni socket superano il limite.

Nome quota	AWS valore predefinito	Regolabile	Descrizione
Connessioni simultanee socket per account	250	Sì	Numero massimo di connessioni simultanee socket per l'editor della query v2 che tutti i principali dell'account possono stabilire nella regione corrente. Valutare se aumentare questa quota se si ricevono errori che le connessioni socket superano il limite.
Numero massimo di connessioni simultanee	3	No	Numero massimo di connessioni al database per utente (incluse le sessioni isolate). Questo valore può essere impostato da 1 a 10 dall'amministratore dell'editor di query v2 in Account settings (Impostazioni account). Se raggiungi il limite impostato dall'amministratore, valuta la possibilità di utilizzare sessioni condivise anziché isolate durante l'esecuzione di SQL. Per ulteriori informazioni sulle connessioni, consulta <a href="#">Apertura editor di query v2</a> . Per ulteriori informazioni sull'impostazione del limite, consulta <a href="#">Modifica delle impostazioni dell'account</a> .

## Quote e limiti per oggetti Amazon Redshift Spectrum

Amazon Redshift Spectrum ha le seguenti quote e limiti:

- Il numero massimo di database per AWS account quando si utilizza un. AWS Glue Data Catalog. Per questo valore, vedere le [Quote di servizio AWS Glue](#) in Riferimenti generali di Amazon Web Services.
- Il numero massimo di tabelle per database quando si utilizza un oggetto AWS Glue Data Catalog. Per questo valore, vedere le [Quote di servizio AWS Glue](#) in Riferimenti generali di Amazon Web Services.
- Il numero massimo di partizioni per tabella quando si utilizza un file AWS Glue Data Catalog. Per questo valore, vedere le [Quote di servizio AWS Glue](#) in Riferimenti generali di Amazon Web Services.

- Il numero massimo di partizioni per AWS account quando si utilizza un AWS Glue Data Catalog. Per questo valore, vedere le [Quote di servizio AWS Glue](#) in Riferimenti generali di Amazon Web Services.
- Il numero massimo di colonne per le tabelle esterne quando si utilizza un AWS Glue Data Catalog, 1.597 quando le pseudocolonne sono abilitate e 1.600 quando le pseudocolonne non sono abilitate.
- La dimensione massima di un valore di stringa in un file ION o JSON quando si utilizza un è 16 KB. AWS Glue Data Catalog Se si raggiunge questo limite, la stringa può essere troncata.
- È possibile aggiungere un massimo di 100 partizioni utilizzando una singola istruzione ALTER TABLE.
- Tutti i dati S3 devono trovarsi nella stessa AWS regione del cluster Amazon Redshift.
- I timestamp in ION e JSON devono utilizzare il formato [ISO8601](#).
- La compressione esterna dei file ORC non è supportata.
- I SERDE di testo, OpenCSV e Regex non supportano delimitatori ottali maggiori di "\177"
- È necessario specificare un predicato nella colonna della partizione per evitare le letture in tutte le partizioni.

Ad esempio, il predicato seguente filtra la colonna `ship_dtm`, ma non applica il filtro alla colonna della partizione `ship_yyyymm`:

```
WHERE ship_dtm > '2018-04-01'.
```

Per ignorare le partizioni superflue, è necessario aggiungere un predicato WHERE `ship_yyyymm = '201804'`. Questo predicato limita le operazioni di lettura alla partizione `\ship_yyyymm=201804\`.

Questi limiti non si applicano a un metastore Apache Hive.

## Vincoli per la denominazione

Nella tabella seguente sono descritti i vincoli di denominazione in Amazon Redshift.

Cluster identifier (Identificatore del cluster)

- Un identificatore di un cluster deve contenere solo caratteri minuscoli.

	<ul style="list-style-type: none"><li>• Deve contenere da 1 –a 63 caratteri alfanumerici o trattini.</li><li>• Il primo carattere deve essere una lettera.</li><li>• Non può terminare con un trattino o contenere due trattini consecutivi.</li><li>• Deve essere univoco per tutti i cluster all'interno di un account AWS .</li></ul>
Nome del database	<ul style="list-style-type: none"><li>• Un nome di database deve contenere da 1 a 64 caratteri alfanumerici.</li><li>• Deve contenere solo lettere minuscole.</li><li>• Non può essere una parola riservata. Un elenco di parole riservate è disponibile in <a href="#">Parole riservate</a> nella Guida per gli sviluppatori di database di Amazon Redshift.</li></ul>
Nome endpoint di un endpoint VPC gestito da RedShift	<ul style="list-style-type: none"><li>• Il nome di un endpoint deve contenere da 1 a 30 caratteri.</li><li>• I caratteri validi sono A-Z, a-z, 0–9 e - (trattino).</li><li>• Il primo carattere deve essere una lettera.</li><li>• Il nome non può contenere due trattini consecutivi o terminare con un trattino.</li></ul>

Nome utente amministratore	<ul style="list-style-type: none"><li>• Un nome utente amministratore deve contenere solo caratteri minuscoli.</li><li>• Deve contenere da 1 a 128 caratteri alfanumerici.</li><li>• Il primo carattere deve essere una lettera.</li><li>• Non può essere una parola riservata. Un elenco di parole riservate è disponibile in <a href="#">Parole riservate</a> nella Guida per gli sviluppatori di database di Amazon Redshift.</li></ul>
Password amministratore	<ul style="list-style-type: none"><li>• Una password amministratore deve contenere da 8 a 64 caratteri.</li><li>• Deve contenere almeno una lettera maiuscola.</li><li>• Deve contenere almeno una lettera minuscola.</li><li>• Deve contenere un numero.</li><li>•</li></ul> <p>Può essere qualsiasi carattere ASCII (codice ASCII da 33 a 126) tranne ' (virgolette singole), " (virgolette doppie), \, / o @.</p>
Nome del gruppo di parametri	<ul style="list-style-type: none"><li>• Il nome di un gruppo di parametri deve contenere da 1 a 255 caratteri alfanumerici o trattini.</li><li>• Deve contenere solo caratteri minuscoli.</li><li>• Il primo carattere deve essere una lettera.</li><li>• Non può terminare con un trattino o contenere due trattini consecutivi.</li></ul>

Nome del gruppo di sicurezza del cluster	<ul style="list-style-type: none"><li>• Il nome di un gruppo di sicurezza di un cluster non deve contenere più di 255 caratteri alfanumerici o trattini.</li><li>• Deve contenere solo caratteri minuscoli.</li><li>• Non deve essere <b>Default</b>.</li><li>• Deve essere unico per tutti i gruppi di sicurezza creati dal tuo AWS account.</li></ul>
Nome del gruppo di sottoreti	<ul style="list-style-type: none"><li>• Il nome di un gruppo di sottoreti non deve contenere più di 255 caratteri alfanumerici o trattini.</li><li>• Deve contenere solo caratteri minuscoli.</li><li>• Non deve essere <b>Default</b>.</li><li>• Deve essere univoco per tutti i gruppi di sottoreti creati dal tuo AWS account.</li></ul>
Identificatore dello snapshot del cluster	<ul style="list-style-type: none"><li>• Un identificatore di uno snapshot di un cluster non deve contenere più di 255 caratteri alfanumerici o trattini.</li><li>• Deve contenere solo caratteri minuscoli.</li><li>• Non deve essere <b>Default</b>.</li><li>• Deve essere univoco per tutti gli identificatori di snapshot creati dall'account. AWS</li></ul>

# Assegnazione di tag alle risorse in Amazon Redshift nella .

## Argomenti

- [Panoramica del tagging](#)
- [Gestione di tag delle risorse tramite la console](#)
- [Gestione dei tag tramite l'API di Amazon Redshift](#)

## Panoramica del tagging

In AWS, i tag sono etichette definite dall'utente costituite da coppie chiave-valore. Amazon Redshift supporta l'assegnazione di tag per fornire i metadati sulle risorse in modo immediato e di classificare i report di fatturazione in base all'allocazione dei costi. Per utilizzare i tag per l'allocazione dei costi, è necessario prima attivarli nel servizio. AWS Billing and Cost Management Per ulteriori informazioni sulla configurazione e sull'uso di tag per scopi di fatturazione, consultare [Utilizzo dei tag per l'allocazione dei costi per report di fatturazione personalizzati](#) e [Configurazione del report mensile di allocazione dei costi](#).

I tag non sono obbligatori per le risorse in Amazon Redshift, ma sono utili per fornire il contesto. È possibile applicare tag alle risorse con metadati relativi a centri di costo, nomi dei progetti e altre informazioni rilevanti correlate alla risorsa. Supponi, ad esempio, di voler tenere traccia delle risorse che appartengono a un ambiente di test e di quelle che appartengono a un ambiente di produzione. Puoi creare una chiave denominata `environment` e specificare il valore `test` o `production` per identificare le risorse usate in ogni ambiente. Se utilizzi il tagging in altri AWS servizi o disponi di categorie standard per la tua attività, ti consigliamo di creare le stesse coppie chiave-valore per le risorse in Amazon Redshift per motivi di coerenza.

I tag per le risorse vengono conservati quando ridimensioni un cluster e dopo il ripristino di uno snapshot di un cluster nella stessa regione. Tuttavia, i tag non vengono conservati se copi uno snapshot in un'altra regione, pertanto è necessario ricreare i tag nella nuova regione. Se elimini una risorsa, i tag associati vengono eliminati.

Ogni risorsa dispone di un set di tag, ovvero una raccolta di uno o più tag assegnati alla risorsa. Ogni risorsa può avere fino a 50 tag per set di tag. Puoi aggiungere tag quando crei una risorsa e dopo che la risorsa è stata creata. È possibile aggiungere tag ai tipi di risorse seguenti in Amazon Redshift:

- CIDR/IP

- Cluster
- Gruppo di sicurezza del cluster
- Regola per il traffico in ingresso del gruppo di sicurezza del cluster
- Gruppo di sicurezza Amazon EC2
- Connessione al modulo di sicurezza hardware (HSM)
- Certificato client HSM
- Gruppo di parametri
- Snapshot
- Subnet group (Gruppo di sottoreti)

Per utilizzare i tag dalla console Amazon Redshift, l'utente può collegare la policy gestita da AWS `AmazonRedshiftFullAccess`. Per un esempio di policy IAM con autorizzazioni di assegnazione tag limitate che possono essere allegate a un utente della console Amazon Redshift, consultare [Esempio 7: consentire a un utente di taggare le risorse con la console Amazon Redshift](#). Per ulteriori informazioni sull'etichettatura, consulta [What is AWS Resource Groups?](#) .

## Requisiti per il tagging

I tag hanno i requisiti seguenti:

- Alle chiavi non può essere anteposto il prefisso `aws:`.
- Le chiavi devono essere univoche per un set di tag.
- Una chiave deve essere costituita da un numero di caratteri compreso tra 1 e 128.
- Un valore deve essere costituito da un numero di caratteri compreso tra 0 e 256.
- Non è necessario che i valori siano univoci per un set di tag.
- I caratteri consentiti per le chiavi e i valori sono lettere Unicode, cifre, spazi e uno qualsiasi dei simboli seguenti: `_ . : / = + - @`.
- Per chiavi e valori viene fatta distinzione tra maiuscole e minuscole.

# Gestione di tag delle risorse tramite la console

Come gestire i tag sulle risorse di Amazon Redshift

1. [Accedi AWS Management Console e apri la console Amazon Redshift all'indirizzo https://console.aws.amazon.com/redshiftv2/.](https://console.aws.amazon.com/redshiftv2/)
2. Dal menu di navigazione, scegliere Configurations (Configurazioni), quindi scegliere Manage tags (Gestisci tag).
3. Inserisci le tue scelte per le risorse e scegli quali tag aggiungere, modificare o eliminare. Quindi scegli Manage tags of the resources that you chose (Gestisci i tag delle risorse selezionate).

Le risorse che è possibile taggare includono cluster, gruppi di parametri, gruppi di sottoreti, certificati client HSM, connessioni HSM e snapshot.

4. Nella pagina di navigazione Gestisci tag, scegliere Esamina e applica modifiche ai tag, quindi scegliere Applica per salvare le modifiche.

## Gestione dei tag tramite l'API di Amazon Redshift

Puoi utilizzare le seguenti AWS CLI operazioni per gestire i tag in Amazon Redshift.

- [create-tags](#)
- [delete-tags](#)
- [describe-tags](#)

È possibile usare le seguenti operazioni API di Amazon Redshift seguenti per gestire i tag.

- [CreateTags](#)
- [DeleteTags](#)
- [DescribeTags](#)
- [Tag](#)
- [TaggedResource](#)

È inoltre possibile usare le API di Amazon Redshift seguenti per gestire e visualizzare i tag per una risorsa specifica:

- [CreateCluster](#)
- [CreateClusterParameterGroup](#)
- [CreateClusterSecurityGroup](#)
- [CreateClusterSnapshot](#)
- [CreateClusterSubnetGroup](#)
- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DescribeClusters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeClusterSecurityGroups](#)
- [DescribeClusterSnapshots](#)
- [DescribeClusterSubnetGroups](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

# Versioni dei cluster per Amazon Redshift

Amazon Redshift rilascia regolarmente versioni dei cluster. I cluster di Amazon Redshift vengono sottoposti a patch durante la finestra di manutenzione del sistema. La tempistica della patch dipende dalle impostazioni della finestra di manutenzione Regione AWS e dell'utente. È possibile visualizzare o modificare le impostazioni della finestra di manutenzione dalla console di Amazon Redshift. Per ulteriori informazioni sulla manutenzione, consulta [Manutenzione del cluster](#).

È possibile visualizzare la versione del cluster nella console di Amazon Redshift nella scheda Maintenance (Manutenzione) dei dettagli del cluster. Oppure è possibile visualizzare la versione del cluster nell'output del comando SQL:

```
SELECT version();
```

## Argomenti

- [Patch 18.1 di Amazon Redshift](#)
- [Patch 180 di Amazon Redshift](#)
- [Patch 179 di Amazon Redshift](#)
- [Patch 178 di Amazon Redshift](#)
- [Patch 177 di Amazon Redshift](#)
- [Patch 176 di Amazon Redshift](#)
- [Patch 175 di Amazon Redshift](#)
- [Patch 174 di Amazon Redshift](#)
- [Patch 173 di Amazon Redshift](#)
- [Patch 172 di Amazon Redshift](#)
- [Patch 171 di Amazon Redshift](#)
- [Patch 170 di Amazon Redshift](#)
- [Patch 169 di Amazon Redshift](#)
- [Patch 168 di Amazon Redshift](#)

## Patch 18.1 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.69497 - Versione Amazon Redshift Serverless - Rilasciata il 18 giugno 2024
- 1.0.69451 - Versione attuale del brano - Rilasciata il 18 giugno 2024
- 1.0.69076 — Versione Amazon Redshift Serverless — Rilasciata il 14 giugno 2024
- 1.0.69065 - Versione attuale del brano - Rilasciata il 14 giugno 2024
- 1.0.68555 — Versione Amazon Redshift Serverless — Rilasciata il 31 maggio 2024
- 1.0.68540 - Versione attuale del brano - Rilasciata il 31 maggio 2024
- 1.0.68328 — Versione Amazon Redshift Serverless — Rilasciata il 23 maggio 2024
- 1.0.68205 - Versione attuale del brano - Rilasciata il 23 maggio 2024
- 1.0.67796 — Versione Amazon Redshift Serverless — Rilasciata il 15 maggio 2024
- 1.0.67788 - Versione attuale del brano - Rilasciata il 15 maggio 2024
- 1.0.67308 — Versione Amazon Redshift Serverless — Rilasciata il 1° maggio 2024
- 1.0.67305 - Versione attuale del brano - Rilasciata il 1 maggio 2024

## Nuove funzionalità e miglioramenti in questa patch

- Introduce il supporto per modificare la chiave di distribuzione e la chiave di ordinamento delle viste materializzate.
- Introduce il supporto per le funzioni 'lower\_attribute\_names ()' e 'upper\_attribute\_names ()' che modificano le maiuscole e minuscole dei nomi degli attributi per i valori degli oggetti SUPER.
- Risolve un problema in CREATE TABLE LIKE quando si utilizza una colonna di identità. In precedenza, la nuova tabella ereditava l'identificatore dalla tabella di origine. Ciò causava problemi se la tabella di origine venisse successivamente eliminata, poiché l'identificatore non sarebbe più valido nella nuova tabella.
- Risolve un problema che impediva la visualizzazione di alcune tabelle esterne in SVV\_ALL\_TABLES.
- Migliora il tempo di avvio del cluster e accelera l'inizializzazione delle query per carichi di lavoro simultanei elevati.
- Risolve un problema con la query federata che causava errori durante il passaggio delle funzioni split\_part () alla fonte federata a RDS e Aurora MySQL
- Supporta le modifiche alla chiave di distribuzione avviate dall'utente tramite i comandi DISTKEY ALTER TABLE... ALTER DISTSTYLE KEY su cluster di scalabilità simultanea forniti e calcolo con scalabilità automatica senza server.

- Supporta viste materializzate aggiornate manualmente che prevedono l'aggregazione sulla scalabilità simultanea fornita e l'elaborazione con scalabilità automatica senza server.
- Aggiunge il supporto per Zero-ETL per gestire record di dimensioni fino a 16 MB e per supportare valori SUPER fino a 16 MB.
- Migliora i messaggi di errore durante la sincronizzazione iniziale in Zero-ETL di Aurora MySQL fornendo dettagli aggiuntivi come schema e nome della tabella.
- Introduce il supporto per l'etichettatura con Amazon Redshift ML CREATE MODEL. Con questo miglioramento, ora puoi etichettare SageMaker le risorse Amazon utilizzate da Amazon Redshift ML. L'etichettatura ti aiuta a gestire, identificare, organizzare, cercare e filtrare le risorse.
- Migliora le prestazioni delle query che coinvolgono le funzioni definite dall'utente (UDF) Lambda ottimizzando l'elaborazione dei dati con AWS Lambda
- Riduce l'utilizzo della memoria durante l'inserimento dei dati in tabelle ordinate di cluster senza server e ridimensionati in modo elastico.
- Aggiunge il supporto per le nuove righe (\n) nella colonna nella vista SYS\_QUERY\_HISTORY e per la colonna query\_text nella vista SYS\_QUERY\_TEXT. text

## Patch 180 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.68870 — Versione finale — Rilasciata il 3 giugno 2024
- 1.0.68520 - Versione trailing track - Rilasciata il 28 maggio 2024
- 1.0.67699 - Versione trailing track - Rilasciata il 15 maggio 2024
- 1.0.66960 - Versione trailing track - Rilasciata il 21 aprile 2024
- 1.0.66954 - Versione attuale del brano - Rilasciata il 21 aprile 2024
- 1.0.66276 - Versione attuale del brano - Rilasciata il 12 aprile 2024
- 1.0.66290 — Versione Amazon Redshift Serverless — Rilasciata il 10 aprile 2024
- 1.0.63590 - Versione attuale del brano - Rilasciata il 19 febbraio 2024
- 1.0.63567 - Versione Amazon Redshift Serverless - Rilasciata il 16 febbraio 2024
- 1.0.63282 - Versione Amazon Redshift Serverless - Rilasciata il 13 febbraio 2024
- 1.0.63269 - Versione attuale del brano - Rilasciata il 13 febbraio 2024
- 1.0.63215 — Versione Amazon Redshift Serverless — Rilasciata il 12 febbraio 2024
- 1.0.63205 - Versione attuale del brano - Rilasciata il 12 febbraio 2024

- 1.0.63030 — Versione Amazon Redshift Serverless — Rilasciata il 7 febbraio 2024
- 1.0.62913 - Versione attuale del brano - Rilasciata il 7 febbraio 2024
- 1.0.62922 — Versione Amazon Redshift Serverless — Rilasciata il 5 febbraio 2024
- 1.0.62878 - Versione attuale del brano - Rilasciata il 5 febbraio 2024
- 1.0.62698 — Versione Amazon Redshift Serverless — Rilasciata il 31 gennaio 2024
- 1.0.62614 - Versione attuale del brano - Rilasciata il 31 gennaio 2024
- 1.0.61687: versione di Amazon Redshift serverless - Rilasciata il 5 gennaio 2024
- 1.0.61678: versione attuale traccia - Rilasciata il 5 gennaio 2024
- 1.0.61567: versione di Amazon Redshift serverless - Rilasciata il 31 dicembre 2023
- 1.0.61559: versione attuale traccia - Rilasciata il 31 dicembre 2023
- 1.0.61430: versione di Amazon Redshift serverless - Rilasciata il 29 dicembre 2023
- 1.0.61395: versione attuale traccia - Rilasciata il 29 dicembre 2023

## Nuove funzionalità e miglioramenti in questa patch

- È stato modificato `CURRENT_USER` in modo che non tronchi più il nome utente restituito a 64 caratteri.
- È stata aggiunta la possibilità di applicare politiche di mascheramento dei dati alle viste standard e alle viste con associazione tardiva.
- È stata aggiunta la possibilità di applicare il mascheramento dinamico dei dati (DDM) agli attributi scalari nelle colonne con tipo di dati `SUPER`.
- È stata aggiunta la funzione SQL `OBJECT_TRANSFORM`. Per ulteriori informazioni, consulta [OBJECT\\_TRANSFORM function](#) nella Guida per sviluppatori di database di Amazon Redshift.
- Aggiunge la possibilità di applicare un controllo AWS Lake Formation granulare degli accessi ai dati annidati e di eseguire query con l'analisi dei data lake di Amazon Redshift.
- È stato aggiunto il tipo di dati `INTERVAL`.
- È stato aggiunto `CONTINUE_HANDLER`, che è un tipo di gestore di eccezioni che controlla il flusso di una stored procedure. Ti consente di acquisire e gestire le eccezioni senza terminare il blocco di istruzioni esistente.
- È stata aggiunta la possibilità di definire le autorizzazioni per un ambito (schema o database) oltre che per i singoli oggetti. Ciò consente agli utenti e ai ruoli di ottenere un'autorizzazione su tutti gli oggetti attuali e futuri dell'ambito.

- È stata aggiunta la possibilità di creare un database da un unità di condivisione dati con autorizzazioni che consentono agli amministratori lato consumer di assegnare autorizzazioni individuali per gli oggetti di database condivisi a utenti e ruoli lato consumer.
- È stato aggiunto il supporto per il tipo di dati SUPER restituiti dai modelli BYOM remoto. Ciò amplia la gamma di SageMaker modelli accettati per includere quelli con formati di restituzione più complessi.
- Sono state modificate le funzioni esterne per trasmettere ora in modo implicito numeri con o senza frazioni al tipo di dati numerici della colonna. Per le colonne int2, int4 e int8, i numeri con frazioni vengono accettati con troncamento, a meno che il numero non sia compreso nell'intervallo. Per le colonne float4 e float8, i numeri sono accettati senza frazioni.
- Aggiunge tre funzioni spaziali che funzionano con il sistema di griglia di indicizzazione geospaziale gerarchica H3: H3\_Lat, H3\_ e H3\_Polyfill. FromLong FromPoint

## Patch 179 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.62317 — Versione Serverless di Amazon Redshift — Rilasciata il 29 gennaio 2024
- 1.0.62312 - Versione finale - Rilasciata il 29 gennaio 2024
- 1.0.61631: versione di Amazon Redshift serverless - Rilasciata il 5 gennaio 2024
- 1.0.61626: versione attuale traccia - Rilasciata il 5 gennaio 2024
- 1.0.61191: versione attuale traccia - Rilasciata il 16 dicembre 2023
- 1.0.61150: versione di Amazon Redshift serverless - Rilasciata il 16 dicembre 2023
- 1.0.60982: versione di Amazon Redshift serverless - Rilasciata il 13 dicembre 2023
- 1.0.60854: versione attuale traccia - Rilasciata il 10 dicembre 2023
- 1.0.60354: versione di Amazon Redshift serverless - Rilasciata il 22 novembre 2023
- 1.0.60353: versione attuale traccia - Rilasciata il 21 novembre 2023
- 1.0.60293: versione di Amazon Redshift serverless - Rilasciata il 21 novembre 2023
- 1.0.60292: versione attuale traccia - Rilasciata il 22 novembre 2023
- 1.0.60161: versione di Amazon Redshift serverless - Rilasciata il 18 novembre 2023
- 1.0.60140: versione attuale traccia - Rilasciata il 18 novembre 2023
- 1.0.60139: versione di Amazon Redshift serverless - Rilasciata il 18 novembre 2023
- 1.0.59947: versione di Amazon Redshift serverless - Rilasciata il 16 novembre 2023

- 1.0.59945: versione attuale traccia - Rilasciata il 16 novembre 2023
- 1.0.59118: versione di Amazon Redshift serverless - Rilasciata il 9 novembre 2023
- 1.0.59117: versione attuale traccia - Rilasciata il 9 novembre 2023

## Nuove funzionalità e miglioramenti in questa patch

- È stato aggiunto il supporto in modo che gli utenti federati con le autorizzazioni appropriate possano visualizzare le viste di sistema del mascheramento dei dati dinamici e di sicurezza a livello di riga, tra cui:
  - SVV\_ATTACHED\_MASKING\_POLICY
  - SVV\_MASKING\_POLICY
  - SVV\_RLS\_ATTACHED\_POLICY
  - SVV\_RLS\_POLICY
  - SVV\_RLS\_RELATION
- È stata aggiunta la funzionalità per generare un errore se una query contiene solo funzioni scalari nella clausola FROM.
- Sono state aggiunte le istruzioni CREATE TABLE AS (CTAS) con funzionalità di tabelle di destinazione permanenti ai cluster con dimensionamento simultaneo. I cluster con dimensionamento simultaneo ora supportano più query.
- Sono state aggiunte le seguenti tabelle di sistema per tenere traccia dello stato della ridistribuzione delle tabelle dopo aver eseguito il ridimensionamento classico sui cluster RA3:
  - La tabella di sistema SYS\_RESTORE\_STATE mostra l'avanzamento della ridistribuzione a livello di tabella.
  - La tabella di sistema SYS\_RESTORE\_LOG mostra la velocità di trasmissione effettiva storica della ridistribuzione dei dati.
- È stata migliorata la discrepanza delle sezioni riducendo al minimo le tabelle EVEN dopo l'esecuzione del ridimensionamento classico sui tipi di nodo RA3. Ciò è applicabile anche ai cluster con la patch 178 che eseguono il ridimensionamento classico.
- È stato aggiunto il supporto per UNLOAD with EXTENSION sui cluster con dimensionamento simultaneo.
- Migliora le prestazioni per le query che contengono  $\lambda$  UDF in ingresso e in join. HashJoins  
NestLoop
- Sono state migliorate le prestazioni del ridimensionamento elastico sui tipi di nodo RA3.

- Sono state migliorate le prestazioni delle query sulla condivisione dei dati.
- Sono state migliorate le prestazioni delle query di analisi avviate manualmente in cluster con provisioning e gruppi di lavoro serverless sottoposti al ridimensionamento elastico.
- Sono state migliorate le prestazioni delle query WLM automatiche con una migliore previsione delle risorse nella gestione del carico di lavoro.
- Rimuove la funzionalità di avvio dei cluster in VPC con tenancy dedicata. Questa modifica non influisce sulla tenancy delle istanze EC2 nel VPC. Puoi modificare la tenancy del tuo VPC come predefinita con `modify-vpc-tenancy` AWS CLI il comando.
- È stato aggiunto il supporto per l'aggiornamento manuale delle viste materializzate sui cluster con dimensionamento simultaneo sottoposti a provisioning e sulle risorse di calcolo con dimensionamento automatico serverless.
- È stato aggiunto il supporto per i valori letterali INTERVAL alla funzione EXTRACT. Ad esempio, `EXTRACT('hours' from Interval '50 hours')` restituisce 2 perché 50 ore vengono interpretate come 2 giorni e 2 ore e viene estratta la componente oraria di 2.

## Patch 178 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.63327 - Versione attuale del brano - Rilasciata il 9 febbraio 2024
- 1.0.63313 - Versione finale del brano - Rilasciata il 9 febbraio 2024
- 1.0.60977: versione finale traccia - Rilasciata il 15 dicembre 2023
- 1.0.59596: versione attuale traccia - Rilasciata il 9 novembre 2023
- 1.0.58593: versione di Amazon Redshift serverless - Rilasciata il 23 ottobre 2023
- 1.0.58558: versione attuale traccia - Rilasciata il 23 ottobre 2023
- 1.0.57864: versione attuale traccia - Rilasciata il 12 ottobre 2023
- 1.0.57850: versione di Amazon Redshift serverless - Rilasciata il 12 ottobre 2023
- 1.0.56952: versione attuale traccia - Rilasciata il 25 settembre 2023
- 1.0.56970: versione di Amazon Redshift serverless - Rilasciata il 25 settembre 2023

## Nuove funzionalità e miglioramenti in questa patch

- Amazon Redshift ora ha migliorato le prestazioni delle query di condivisione dei dati velocizzando l'aggiornamento dei metadati sulle istanze consumer mentre vengono apportate modifiche simultanee ai dati sull'istanza producer.
- Aggiunge il supporto per l'aggiornamento automatico e incrementale delle viste materializzate su istanze consumer di condivisione dei dati di Amazon Redshift quando le tabelle di base della vista materializzata si riferiscono ai dati condivisi.
- Aggiunge il supporto per l'archiviazione di oggetti di grandi dimensioni fino a 16 MB nel tipo di dati SUPER. Durante l'importazione da file origine JSON, PARQUET, TEXT e CSV, è possibile caricare dati o documenti semi strutturati come valori nel tipo di dati SUPER, fino a 16 MB.
- Aggiunge il supporto per il dimensionamento elastico per la scalabilità da e verso un cluster Amazon Redshift RA3 a nodo singolo.
- I cluster Amazon Redshift RA3 a nodo singolo ora possono trarre vantaggio dai miglioramenti della crittografia, riducendo il tempo complessivo di crittografia e migliorando la disponibilità del data warehouse durante il processo di crittografia.
- Migliora il supporto per le query durante l'annullamento della nidificazione e l'unpivoting dei dati archiviati nel tipo di dati SUPER.
- Migliora le prestazioni di aggiornamento delle viste materializzate con tipi di dati SUPER.
- Aggiunge il supporto per l'aggregazione di valori letterali INTERVAL con la funzione ANY\_VALUE.
- L'importazione di dati in streaming ora supporta il seguente nuovo comando SQL per eliminare i dati di streaming: `DELETE FROM streaming_materialized_views WHERE <where filter clause>`.
- La funzione DECODE sostituisce un valore specifico con un altro valore specifico o un valore predefinito, in base al risultato di una condizione di uguaglianza. DECODE ora richiede i seguenti tre parametri:
  - expression
  - cerca
  - result
- Aggiunge funzionalità alle stored procedure per consentire di rilevare gli errori di conversione del tipo di dati di overflow e di gestirli all'interno di un blocco di gestione delle eccezioni.
- Ora riceverai un errore durante le query di sicurezza a livello di riga o delle relazioni protette dal mascheramento dinamico dei dati se modifichi `enable_case_sensitive_identifier` in modo che sia diverso dall'impostazione predefinita della sessione. Inoltre, la seguente configurazione

viene bloccata quando vengono applicate policy di sicurezza a livello di riga o politiche di mascheramento dinamico dei dati nel cluster o nello spazio dei nomi serverless fornito:

```
ALTER USER <current_user> SET case-sensitive identifier.
```

- Il comando MERGE ora supporta una sintassi semplificata che richiede solo la tabella di destinazione e di origine. Per ulteriori informazioni, consulta [MERGE](#) nella Guida per gli sviluppatori di database di Amazon Redshift.
- Aggiunge il supporto per l'associazione di politiche di mascheramento dinamico dei dati identiche a più utenti o ruoli con la stessa priorità o senza specificare la priorità.
- Ora puoi specificare COLLATION quando aggiungi una nuova colonna tramite ALTER TABLE ADD COLUMN.
- Risolve il problema che ritarda l'applicazione delle regole QMR sui cluster con dimensionamento simultaneo e Amazon Redshift serverless.
- Query federate Amazon Redshift ha esteso il supporto per il pushdown del fuso orario con timestamp su Amazon RDS per PostgreSQL e Amazon Aurora PostgreSQL.
- Ora puoi usare i nomi di database Amazon RDS per MySQL e Aurora MySQL che iniziano con cifre per le query federate.
- Aggiunge la vista SYS\_ANALYZE\_HISTORY che contiene i dettagli dei record delle operazioni ANALYZE.
- Aggiunge la vista SYS\_ANALYZE\_COMPRESSION\_HISTORY, che contiene i dettagli dei record per le operazioni di analisi della compressione durante i comandi COPY o ANALYZE COMPRESSION.
- Aggiunge la vista SYS\_SESSION\_HISTORY, che contiene i dettagli dei record relativi alle sessioni attive, cronologiche e riavviate.
- Aggiunge la vista SYS\_TRANSACTION\_HISTORY, che contiene i dettagli dei record relativi all'analisi a livello di transazione che fornisce il tempo impiegato per il commit, il numero di blocchi di unità di condivisione dati impegnati e il livello di isolamento.
- Aggiunge la vista SVV\_REDSHIFT\_SCHEMA\_QUOTA, che contiene i record relativi alle quote e all'utilizzo corrente del disco per ogni schema in un database.
- Aggiunge la vista SYS\_PROCEDURE\_CALL, che contiene i record relativi alle chiamate delle stored procedure, tra cui l'ora di inizio, l'ora di fine, lo stato della chiamata delle stored procedure e la gerarchia per le chiamate di stored procedure nidificate.
- Aggiunge la vista SYS\_CROSS\_REGION\_DATASHARING\_USAGE, che contiene i record relativi al monitoraggio dell'utilizzo della condivisione dei dati tra regioni.

- Aggiunge la vista `SYS_PROCEDURE_MESSAGES`, che contiene i record relativi al tracciamento delle informazioni sui messaggi relativi alle stored procedure registrati.
- Aggiunge la vista `SYS_UDF_LOG`, che contiene i record relativi al tracciamento dei messaggi di log del sistema provenienti da chiamate di funzioni, errori, avvisi o tracce definiti dall'utente, ove applicabile.
- Aggiunge le nuove colonne `IS_RECURSIVE`, `IS_NESTED`, `S3LIST_TIME` e `GET_PARTITION_TIME` a `SYS_EXTERNAL_QUERY_DETAIL`.
- È stata aggiunta `MaxRPU`, una nuova impostazione di controllo dei costi di calcolo per Redshift serverless. Con `MaxRPU`, puoi facoltativamente specificare una soglia di calcolo massima per controllare i costi del data warehouse in momenti diversi, selezionando il livello di calcolo massimo che Redshift serverless può usare per il dimensionamento di ogni gruppo di lavoro.
- È stato corretto l'output del valore letterale `INTERVAL` con stringhe di intervalli numerici. Ad esempio, un intervallo che specifica `INTERVAL '1' YEAR` ora restituisce `1 YEAR` anziché `"00:00:00`. Inoltre, l'output del valore letterale `INTERVAL` viene troncato al componente `INTERVAL` più piccolo specificato. Ad esempio, `INTERVAL '1 day 1 hour 1 minute 1.123 seconds' HOUR TO MINUTE` viene troncato in `1 day 01:01:00`.

## Patch 177 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.57922: versione finale traccia - Rilasciata il 12 ottobre 2023
- 1.0.57799: versione di Amazon Redshift serverless - Rilasciata il 10 ottobre 2023
- 1.0.57798: versione attuale traccia - Rilasciata il 10 ottobre 2023
- 1.0.57085: versione finale traccia - Rilasciata il 26 settembre 2023
- 1.0.56899: versione di Amazon Redshift serverless - Rilasciata il 21 settembre 2023
- 1.0.56754: versione attuale traccia - Rilasciata il 21 settembre 2023
- 1.0.56242: versione attuale traccia - Rilasciata l'11 settembre 2023
- 1.0.55539: versione di Amazon Redshift serverless - Rilasciata il 28 agosto 2023
- 1.0.55524: versione attuale traccia - Rilasciata il 28 agosto 2023
- 1.0.54899 - Versione attuale traccia - Rilasciata il 15 agosto 2023
- 1.0.54899: versione attuale traccia - Rilasciata il 14 agosto 2023

- 1.0.54899 - Versione attuale traccia - Rilasciata il 15 agosto 2023
- 1.0.54239 - Versione attuale traccia - Rilasciata il 3 agosto 2023
- 1.0.54321 - Versione di Amazon Redshift serverless - Rilasciata il 3 agosto 2023

## Nuove funzionalità e miglioramenti in questa patch

- Aggiunge la vista `SYS_MV_STATE` che contiene una riga per ogni transizione di stato di una vista materializzata. `SYS_MV_STATE` può essere utilizzato per il monitoraggio degli aggiornamenti MV per le istanze fornite da Amazon Redshift Serverless e Amazon Redshift.
- Aggiunge la vista `SYS_USERLOG`, che registra i dettagli delle modifiche a un utente del database per `Create user`, `Drop user`, `Alter user (rename)`, `Alter user (alter properties)`.
- Aggiunge la vista `SYS_COPY_REPLACEMENTS` che mostra un log che registra il momento in cui dei caratteri UTF-8 non validi sono stati sostituiti dal comando `COPY` con l'opzione `ACCEPTINVCHARS`.
- Aggiunge la vista `SVL_SPATIAL_SIMPLIFY` che contiene informazioni sugli oggetti della geometria spaziale semplificata utilizzando il comando `COPY`.
- Aggiunge la vista `SYS_VACUUM_HISTORY`, che è possibile utilizzare per visualizzare i dettagli e i risultati delle operazioni `VACUUM`.
- Aggiunge la vista `SYS_SCHEMA_QUOTA_VIOLATIONS` per registrare occorrenza, timestamp, `XID` e altre informazioni utili quando viene superata una quota dello schema.
- Aggiunge la vista `SYS_RESTORE_STATE`, che è possibile utilizzare per monitorare l'avanzamento della ridistribuzione di ogni tabella nel cluster durante il ridimensionamento classico asincrono.
- Aggiunge la vista `SYS_EXTERNAL_QUERY_ERROR` che restituisce informazioni sugli errori di scansione di Redshift Spectrum.
- Aggiunge il parametro `tag` al comando `CREATE MODEL`, in modo da poter ora tenere traccia dei costi di formazione con processi di formazione autopilot.
- Aggiunge nomi di dominio personalizzati (`CNAME`) per i cluster Amazon Redshift.
- Aggiunge il supporto di anteprima per Apache Iceberg, consentendo ai clienti di eseguire query di analisi sulle tabelle Apache Iceberg all'interno di Amazon Redshift.
- Aggiunge il supporto per l'utilizzo di ruoli utente con gruppi di parametri nella gestione del carico di lavoro (`WLM`).
- Aggiunge il supporto per il montaggio automatico di AWS Glue Data Catalog, semplificando per i clienti l'esecuzione di query nei loro data lake.

- Aggiunge funzionalità tali che l'utilizzo di funzioni di raggruppamento senza una clausola GROUP BY o l'utilizzo di operazioni di raggruppamento in una clausola WHERE genera un errore.
- Aggiunge funzionalità alle procedure memorizzate per consentire di rilevare gli errori di divisione per zero e di gestirli all'interno di un blocco di gestione delle eccezioni.
- Risolve un bug che impediva alle query di utilizzare il dimensionamento simultaneo per scrivere dati su tabelle quando la tabella di origine è una tabella di condivisione dati.
- Corregge l'identificatore con distinzione tra maiuscole e minuscole documentato in `enable_case_sensitive_identifier` per funzionare ora con le istruzioni MERGE.
- Risolve il bug per cui una query sulla funzione `pg_get_late_binding_view_cols ()` potrebbe essere ignorata di tanto in tanto. Ora puoi sempre annullare tali richieste.
- Migliora le prestazioni per le domande di condivisione dei dati rivolte ai consumatori durante l'esecuzione di processi sottovuoto sul produttore.
- Migliora le prestazioni per la condivisione dei dati e le query di scalabilità simultanea, in particolare in caso di modifiche simultanee dei dati sul produttore o in caso di trasferimento su un'istanza di scalabilità simultanea collegata al consumatore.

## Patch 176 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.56738: versione finale traccia - Rilasciata il 21 settembre 2023
- 1.0.55837: versione finale traccia - Rilasciata l'11 settembre 2023
- 1.0.54776 - Versione attuale traccia - Rilasciata il 15 agosto 2023
- 1.0.54052: versione attuale traccia - Rilasciata il 26 luglio 2023
- 1.0.53642: versione di Amazon Redshift serverless - Rilasciata il 20 luglio 2023
- 1.0.53301: versione attuale traccia - Rilasciata il 20 luglio 2023
- 1.0.52943: versione di Amazon Redshift serverless - Rilasciata il 7 luglio 2023
- 1.0.52931: versione attuale traccia - Rilasciata il 7 luglio 2023
- 1.0.52194: versione di Amazon Redshift serverless - Rilasciata il 21 giugno 2023
- Versione attuale traccia 1.0.51986 - Rilasciata il 16 giugno 2023
- Versione attuale traccia 1.0.51594 - Rilasciata il 9 giugno 2023

## Nuove funzionalità e miglioramenti in questa patch

- Migliore gestione degli errori durante la scrittura di GROUP BY () per un set di raggruppamento vuoto. Questo aspetto è stato ignorato in precedenza e ora restituisce un errore del parser.
- Miglioramenti delle prestazioni per l'aggiornamento incrementale delle viste materializzate con colonne SUPER.
- ALTER TABLE <target\_tbl> APPEND FROM <streaming\_mv>: il comando SQL (ATA) ora supporta lo spostamento di tutti i record da una vista materializzata in streaming (MV) come origine, oltre alle tabelle come origine, in una tabella di destinazione. Il supporto per ATA sulle MV in streaming consente agli utenti di eliminare rapidamente tutti i record di una MV in streaming spostandoli su un'altra tabella per gestire la crescita dei dati.
- TRUNCATE <streaming\_mv>: il comando SQL ora supporta il troncamento di tutti i record in una vista materializzata in streaming (MV), oltre alle tabelle. TRUNCATE elimina tutti i record nella MV in streaming, lasciando intatta la struttura della MV in streaming. L'esecuzione di TRUNCATE su MV in streaming consente ai clienti di eliminare rapidamente tutti i record di una MV in streaming per gestire la crescita dei dati.
- È stata aggiunta la funzionalità per la clausola QUALIFY al comando SELECT.
- Supporto al machine learning di Redshift per la previsione delle serie temporali mediante integrazione con Amazon Forecast.
- AWS Glue Data Catalog il montaggio automatico è supportato per semplificare l'interrogazione di un data lake senza passaggi aggiuntivi per creare riferimenti a schemi esterni.
- È ora supportata la modifica di una policy RLS. Consulta la documentazione per ulteriori dettagli in [ALTER RLS POLICY](#).
- Le funzioni Lambda definite dall'utente ora supportano il parametro funzione-volatilità STABLE nell'istruzione CREATE FUNCTION. Quando il parametro STABLE viene utilizzato nell'istruzione CREATE FUNCTION e la funzione Lambda definita dall'utente viene richiamata più volte, con gli stessi argomenti, il numero previsto di chiamate di funzioni Lambda definite dall'utente viene ridotto. La categoria di volatilità della funzione STABLE è illustrata più dettagliatamente nei [parametri CREATE FUNCTION](#).
- Molteplici miglioramenti delle prestazioni delle funzioni Lambda definite dall'utente. In particolare, è stato migliorato il supporto per il raggruppamento di record durante le query su una tabella protetta da una policy di sicurezza a livello di riga (RLS).

- Riduzione del tempo complessivo di crittografia per i cluster Amazon Redshift RA3 e miglioramento della disponibilità del data warehouse durante la crittografia. Per ulteriori informazioni, consulta [Crittografia dei database di Amazon Redshift](#).
- Una nuova vista di sistema SYS\_MV\_REFRESH\_HISTORY è stata aggiunta a Redshift. La vista SYS\_MV\_REFRESH\_HISTORY contiene una riga per l'attività di aggiornamento delle viste materializzate. Utilizzando SYS\_MV\_REFRESH\_HISTORY, puoi controllare la cronologia degli aggiornamenti delle viste materializzate. SYS\_MV\_REFRESH\_HISTORY è visibile a tutti gli utenti. Gli utenti con privilegi avanzati visualizzano tutte le righe; gli utenti regolari visualizzano solo i propri dati.

Una nuova colonna SPILLED\_BLOCK\_LOCAL\_DISK è stata aggiunta alla vista di sistema SYS\_QUERY\_DETAIL. La nuova colonna SPILLED\_BLOCK\_LOCAL\_DISK aiuta i clienti a determinare i blocchi riversati sul disco locale. Puoi utilizzare SYS\_QUERY\_DETAIL per visualizzare i dettagli delle query a livello di fase. SYS\_QUERY\_DETAIL è visibile a tutti gli utenti. Gli utenti con privilegi avanzati visualizzano tutte le righe; gli utenti normali visualizzano solo i metadati a cui hanno accesso.

- Una nuova vista di sistema, SYS\_QUERY\_TEXT, è stata aggiunta ad Amazon Redshift Serverless e Amazon Redshift con provisioning. La vista SYS\_QUERY\_TEXT è simile a [SVL\\_STATEMENTTEXT](#) per i cluster con provisioning. Utilizza la colonna sequence nella vista SYS\_QUERY\_TEXT per ottenere il testo completo dell'istruzione SQL.

## Patch 175 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.53064: versione attuale traccia - Rilasciata il 7 luglio 2023
- Versione attuale traccia 1.0.51973 - Rilasciata il 16 giugno 2023
- Versione attuale traccia 1.0.51781 - Rilasciata il 10 giugno 2023
- Versione di Amazon Redshift serverless 1.0.51314 - Rilasciata il 3 giugno 2023
- Versione attuale traccia 1.0.51304 - Rilasciata il 2 giugno 2023
- Versione attuale traccia 1.0.50708 - Rilasciata il 19 maggio 2023
- Versione attuale traccia 1.0.50300 - Rilasciata l'8 maggio 2023
- Versione di Amazon Redshift serverless 1.0.49710 - Rilasciata il 28 aprile 2023
- Versione attuale traccia 1.0.49676 - Rilasciata il 28 aprile 2023

## Nuove funzionalità e miglioramenti in questa patch

- Correzioni di bug minori.
- L'ingestione di streaming di Amazon Redshift ora supporta l'ingestione di streaming tra regioni in cui l'argomento di origine ( Amazon Kinesis Data Streams KDS) o Amazon Managed Streaming for Apache Kafka (MSK) può trovarsi in una regione diversa da quella in cui si AWS trova il data warehouse Amazon Redshift. AWS La documentazione in [Nozioni di base sull'importazione dati in streaming da Amazon Kinesis Data Streams](#) è stata rivista e spiega come viene utilizzata la parola chiave REGION.
- Regolazione dell'ora legale in Egitto.
- Tempi complessivi migliorati per la crittografia dei cluster RA3.

## Patch 174 di Amazon Redshift

### 1.0.51296: rilasciata il 2 giugno 2023

Release sulla traccia finale. Nessuna nota di rilascio.

### 1.0.50468: rilasciata il 12 maggio 2023

Versione di manutenzione. Nessuna nota di rilascio.

### 1.0.49780, 1.0.49868 e 1.0.49997: rilasciata il 28 aprile 2023

Note di rilascio per questa versione:

- Supporto batch migliorato per funzione Lambda definita dall'utente.
- Batch incrementale per funzione Lambda definita dall'utente.
- Nuovo comando MERGE SQL per applicare le modifiche dei dati di origine alle tabelle Amazon Redshift.
- Nuova funzionalità di mascheramento dinamico dei dati per semplificare il processo di protezione dei dati sensibili in un data warehouse Amazon Redshift.
- Nuovo controllo centralizzato degli accessi per la condivisione dei dati con Lake Formation che consente di gestire le concessioni di autorizzazioni, visualizzare i controlli di accesso e controllare le autorizzazioni sulle tabelle e le viste nelle condivisioni di dati Amazon Redshift utilizzando le API di Lake Formation e la console. AWS

- Regolazione dell'ora legale in Egitto.

## 1.0.49087 - Rilasciata il 12 aprile 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.48805 - Rilasciata il 5 aprile 2023

Note di rilascio per questa versione:

- Amazon Redshift ha introdotto ulteriori miglioramenti delle prestazioni per le query con un elevato numero di stringhe utilizzando BYTEDICT, una nuova codifica di compressione in Amazon Redshift che velocizza l'elaborazione dei dati basata su stringhe da 5x a 63x rispetto a codifiche di compressione alternative come LZO o ZSTD. Per ulteriori informazioni su questa funzionalità, consulta la [codifica dei dizionari a byte](#) nella Guida per gli sviluppatori di database di Amazon Redshift.

## 1.0.48004 - Rilasciata il 17 marzo 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.47470 - Rilasciata l'11 marzo 2023

Note di rilascio per questa versione:

- Migliora le prestazioni delle query su `pg_catalog.svv_table_info`. Aggiunge anche una nuova colonna `create_time`. Quando si crea una tabella, questa colonna archivia il timestamp di data/ora in formato UTC.
- Aggiunge il supporto per specificare il timeout a livello di sessione su una query federata.

## Patch 173 di Amazon Redshift

## 1.0.49788 - Rilasciata il 28 aprile 2023

Note di rilascio per questa versione:

- Regolazione dell'ora legale in Egitto.

## 1.0.49074 - Rilasciata il 12 aprile 2023

Note di rilascio per questa versione:

- Configurazione del fuso orario aggiornata alla versione 2022g della libreria IANA.

## 1.0.48766 - Rilasciata il 5 aprile 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.48714 - Rilasciata il 5 aprile 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.48022 - Rilasciata il 17 marzo 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.47357 - Rilasciata il 7 marzo 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.46987: rilasciata il 24 febbraio 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.46806: rilasciata il 18 febbraio 2023

Versione di manutenzione. Nessuna nota di rilascio.

## 1.0.46607: rilasciata il 13 febbraio 2023

Note di rilascio per questa versione:

- Ora le tabelle con chiavi di ordinamento interleaving impostate manualmente vengono automaticamente convertite in chiavi di ordinamento composte se lo stile di distribuzione è stato impostato su DISTSTYLE KEY, per migliorare le prestazioni di queste tabelle. Questa operazione viene eseguita al momento del ripristino di uno snapshot in Amazon Redshift Serverless.

## 1.0.45698: rilasciata il 20 gennaio 2023

Note di rilascio per questa versione:

- Aggiunge un parametro di estensione di file al comando UNLOAD, in modo che le estensioni dei file vengano aggiunte automaticamente ai nomi dei file.
- Supporta la protezione degli oggetti protetti da RLS (sicurezza a livello di riga) per impostazione predefinita quando li si aggiunge a un'unità di condivisione dati o se fanno già parte di un'unità di questo tipo. Gli amministratori possono ora disattivare RLS (sicurezza a livello di riga) per le unità di condivisione dati per consentire ai consumer di accedere all'oggetto protetto.
- Aggiunge nuove tabelle di sistema per il monitoraggio: SVV\_ML\_MODEL\_INFO, SVV\_MV\_DEPENDENCY e SYS\_LOAD\_DETAIL. Inoltre aggiunge le colonne data\_skewness e time\_skewness alla tabella di sistema SYS\_QUERY\_DETAIL.

## Patch 172 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.46534: rilasciata il 18 febbraio 2023
- 1.0.46523: rilasciata il 13 febbraio 2023
- 1.0.46206: rilasciata il 1 febbraio 2023
- 1.0.45603: rilasciata il 20 gennaio 2023
- 1.0.44924: rilasciata il 19 dicembre 2022
- 1.0.44903: rilasciata il 18 dicembre 2022
- 1.0.44540: rilasciata il 13 dicembre 2022
- 1.0.44126: rilasciata il 23 novembre 2022
- 1.0.43980: rilasciata il 17 novembre 2022

## Nuove funzionalità e miglioramenti in questa patch

- Le tabelle create da CTAS sono AUTO per impostazione predefinita.
- Aggiunge il supporto per la sicurezza a livello di riga (RLS) nelle viste materializzate.
- Aumenta il timeout S3 per migliorare la condivisione dei dati tra regioni.
- Aggiunge la nuova funzione spaziale ST\_GeomFromGeohash.

- Migliora la selezione automatica della chiave di distribuzione dalle chiavi primarie composite per migliorare out-of-the-box le prestazioni.
- Aggiunge la chiave primaria automatica alla chiave di distribuzione per le tabelle con chiavi primarie composite, migliorando out-of-the-box le prestazioni.
- Migliora la scalabilità simultanea per consentire la scalabilità di un numero maggiore di query anche quando i dati cambiano.
- Migliora le prestazioni delle query sulla condivisione dei dati.
- Aggiunge parametri di probabilità del machine learning per i modelli di classificazione.
- Aggiunge nuove tabelle di sistema per il monitoraggio: SVV\_USER\_INFO, SVV\_MV\_INFO, SYS\_CONNECTION\_LOG, SYS\_DATASHARE\_USAGE\_PRODUCER, SYS\_DATASHARE\_USAGE\_CONSUMER e SYS\_DATASHARE\_CHANGE\_LOG.
- Aggiunge il supporto per le query delle colonne VARBYTE nelle tabelle esterne per i tipi di file Parquet e ORC.

## Patch 171 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.43931: rilasciata il 16 novembre 2022
- 1.0.43551: rilasciata il 5 novembre 2022
- 1.0.43331: rilasciata il 29 settembre 2022
- 1.0.43029: rilasciata il 26 settembre 2022

## Nuove funzionalità e miglioramenti in questa patch

- Supporto per CONNECT BY: aggiunge il supporto per il costrutto CONNECT BY SQL, che consente di eseguire query in modo ricorsivo sui dati gerarchici nel data warehouse in base alla relazione padre-figlio all'interno di quel set di dati.

## Patch 170 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.43922: rilasciata il 21 novembre 2022

- 1.0.43573: rilasciata il 7 novembre 2022
- 1.0.41881: rilasciata il 20 settembre 2022
- 1.0.41465: rilasciata il 7 settembre 2022
- 1.0.40325: rilasciata il 27 luglio 2022

## Nuove funzionalità e miglioramenti in questa patch

- ST\_GeomfromGeo JSON: costruisce un oggetto geometrico spaziale Amazon Redshift da VARCHAR nella rappresentazione GeoJSON.

## Patch 169 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.41050: rilasciata il 7 settembre 2022
- 1.0.40083: rilasciata il 16 luglio 2022
- 1.0.39734: rilasciata il 7 luglio 2022
- 1.0.39380: rilasciata il 23 giugno 2022
- 1.0.39251: rilasciata il 15 giugno 2022
- 1.0.39009: rilasciata l'8 giugno 2022

## Nuove funzionalità e miglioramenti in questa patch

- Aggiunge role come parametro per il comando Alter Default Privileges (Modifica privilegi predefiniti) per supportare il controllo degli accessi basato sui ruoli.
- Aggiunge il parametro ACCEPTINVCHARS per supportare la sostituzione di caratteri UTF-8 non validi durante la copia da file Parquet e ORC.
- Aggiunge la funzione OBJECT(k,v) per costruire oggetti SUPER da coppie chiave-valore.

## Patch 168 di Amazon Redshift

Versioni dei cluster in questa patch:

- 1.0.38698 - Rilasciata il 25 maggio 2022

- 1.0.38551 - Rilasciata il 20 maggio 2022
- 1.0.38463 - Rilasciata il 18 maggio 2022
- 1.0.38361 - Rilasciata il 13 maggio 2022
- 1.0.38199: rilasciata il 9 maggio 2022
- 1.0.38112 - Rilasciata il 6 maggio 2022
- 1.0.37684 - Rilasciata il 20 aprile 2022

## Nuove funzionalità e miglioramenti in questa patch

- Aggiunto il supporto per il tipo di modello Linear Learner in Amazon Redshift ML.
- Aggiunta l'opzione SNAPSHOT per il livello di isolamento delle transazioni SQL.
- Aggiunto `farmhashFingerprint64` come nuovo algoritmo di hashing per i dati VARBYTE e VARCHAR.
- Supporto della funzione AVG nell'aggiornamento incrementale delle viste materializzate.
- Supporto delle sottoquery correlate su tabelle esterne in Redshift Spectrum.
- Per migliorare le prestazioni delle out-of-the-box query, Amazon Redshift sceglie automaticamente una chiave primaria a colonna singola per tabelle specifiche come chiave di distribuzione.

# Esempi di codice per Amazon Redshift con SDK AWS

I seguenti esempi di codice mostrano come usare Amazon Redshift con un kit di sviluppo AWS software (SDK).

Le operazioni sono estratti di codice da programmi più grandi e devono essere eseguite nel contesto. Sebbene le operazioni mostrino come richiamare le singole funzioni del servizio, è possibile visualizzarle contestualizzate negli scenari correlati e negli esempi tra servizi.

Scenari: esempi di codice che mostrano come eseguire un'attività specifica richiamando più funzioni all'interno dello stesso servizio.

Esempi cross-service: applicazioni di esempio che funzionano su più servizi Servizi AWS.

Per un elenco completo di guide ed esempi di codice per sviluppatori AWS SDK, consulta. [Utilizzo di questo servizio con un SDK AWS](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

Nozioni di base

## Salve Amazon Redshift

I seguenti esempi di codice mostrano come iniziare a usare Amazon Redshift.

Java

SDK per Java 2.x

### Note

C'è altro su. [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import
    software.amazon.awssdk.services.redshift.paginators.DescribeClustersIterable;

/**
```

```
* Before running this Java V2 code example, set up your development
* environment, including your credentials.
*
* For more information, see the following documentation topic:
*
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-
started.html
*/
public class HelloRedshift {

    public static void main(String[] args) {
        Region region = Region.US_EAST_1;
        RedshiftClient redshiftClient = RedshiftClient.builder()
            .region(region)
            .build();

        listClustersPaginator(redshiftClient);
    }

    public static void listClustersPaginator(RedshiftClient redshiftClient) {
        DescribeClustersIterable clustersIterable =
redshiftClient.describeClustersPaginator();
        clustersIterable.stream()
            .flatMap(r -> r.clusters().stream())
            .forEach(cluster -> System.out
                .println(" Cluster identifier: " + cluster.clusterIdentifier() +
" status = " + cluster.clusterStatus()));
    }
}
```

- Per i dettagli sull'API, consulta [DescribeClusters](#) in AWS SDK for Java 2.x API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è di più su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
import boto3

def hello_redshift(redshift_client):
    """
    Use the AWS SDK for Python (Boto3) to create an Amazon Redshift client and
    list
    the clusters in your account. This list might be empty if you haven't created
    any clusters.
    This example uses the default settings specified in your shared credentials
    and config files.

    :param redshift_client: A Boto3 Redshift Client object.
    """
    print("Hello, Redshift! Let's list your clusters:")
    paginator = redshift_client.get_paginator("describe_clusters")
    clusters = []
    for page in paginator.paginate():
        clusters.extend(page["Clusters"])

    print(f"{len(clusters)} cluster(s) were found.")

    for cluster in clusters:
        print(f"  {cluster['ClusterIdentifier']}")

if __name__ == "__main__":
    hello_redshift(boto3.client("redshift"))
```

- Per i dettagli sull'API, consulta [DescribeClusters](#) in AWS SDK for Python (Boto3) API Reference.

## Esempi di codice

- [Azioni per Amazon Redshift tramite SDK AWS](#)
  - [Utilizzo CreateCluster con un AWS SDK o una CLI](#)
  - [Utilizzo CreateTable con un AWS SDK o una CLI](#)
  - [Utilizzo DeleteCluster con un AWS SDK o una CLI](#)
  - [Utilizzo DescribeClusters con un AWS SDK o una CLI](#)

- [Utilizzo DescribeStatement con un AWS SDK o una CLI](#)
- [Utilizzo GetStatementResult con un AWS SDK o una CLI](#)
- [Utilizzo Insert con un AWS SDK o una CLI](#)
- [Utilizzo ModifyCluster con un AWS SDK o una CLI](#)
- [Utilizzo Query con un AWS SDK o una CLI](#)
- [Scenari per Amazon Redshift che utilizzano SDK AWS](#)
  - [Inizia a usare tabelle, elementi e query di Amazon Redshift](#)
- [Esempi di servizi multipli per Amazon AWS Redshift che utilizzano SDK](#)
  - [Come creare un tracker di articoli Amazon Redshift](#)

## Azioni per Amazon Redshift tramite SDK AWS

I seguenti esempi di codice mostrano come eseguire singole azioni Amazon Redshift con AWS gli SDK. Questi estratti chiamano l'API Amazon Redshift e sono estratti di codice da programmi più grandi che devono essere eseguiti nel contesto. Ogni esempio include un collegamento a GitHub, dove puoi trovare le istruzioni per la configurazione e l'esecuzione del codice.

Gli esempi seguenti includono solo le operazioni più comunemente utilizzate. Per un elenco completo, consulta l'[Amazon Redshift API](#) Reference.

### Esempi

- [Utilizzo CreateCluster con un AWS SDK o una CLI](#)
- [Utilizzo CreateTable con un AWS SDK o una CLI](#)
- [Utilizzo DeleteCluster con un AWS SDK o una CLI](#)
- [Utilizzo DescribeClusters con un AWS SDK o una CLI](#)
- [Utilizzo DescribeStatement con un AWS SDK o una CLI](#)
- [Utilizzo GetStatementResult con un AWS SDK o una CLI](#)
- [Utilizzo Insert con un AWS SDK o una CLI](#)
- [Utilizzo ModifyCluster con un AWS SDK o una CLI](#)
- [Utilizzo Query con un AWS SDK o una CLI](#)

## Utilizzo **CreateCluster** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `CreateCluster`.

### CLI

#### AWS CLI

L' `Parameters` This esempio `Create a Cluster with Minimal` crea un cluster con il set minimo di parametri. Per impostazione predefinita, l'output è in formato JSON. Comando:

```
aws redshift create-cluster --node-type dw.hs1.xlarge --number-of-nodes 2 --
master-username adminuser --master-user-password TopSecret1 --cluster-identifier
mycluster
```

Risultato:

```
{
  "Cluster": {
    "NodeType": "dw.hs1.xlarge",
    "ClusterVersion": "1.0",
    "PubliclyAccessible": "true",
    "MasterUsername": "adminuser",
    "ClusterParameterGroups": [
      {
        "ParameterApplyStatus": "in-sync",
        "ParameterGroupName": "default.redshift-1.0"
      }
    ],
    "ClusterSecurityGroups": [
      {
        "Status": "active",
        "ClusterSecurityGroupName": "default"
      }
    ],
    "AllowVersionUpgrade": true,
    "VpcSecurityGroups": [],
    "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
    "AutomatedSnapshotRetentionPeriod": 1,
    "ClusterStatus": "creating",
    "ClusterIdentifier": "mycluster",
    "DBName": "dev",
    "NumberOfNodes": 2,
    "PendingModifiedValues": {
```

```
        "MasterUserPassword": "\\****"
    }
},
"ResponseMetadata": {
    "RequestId": "7cf4bcfc-64dd-11e2-bea9-49e0ce183f07"
}
}
```

- Per i dettagli sull'API, consulta [CreateCluster](#) Command Reference.AWS CLI

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Crea il cluster .

```
public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {
```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Per i dettagli sull'API, [CreateCluster](#) consulta AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

### Crea il client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

### Crea il cluster .

```
// Import required AWS SDK clients and commands for Node.js
import { CreateClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "./libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME", // Required
  NodeType: "NODE_TYPE", //Required
  MasterUsername: "MASTER_USER_NAME", // Required - must be lowercase
  MasterUserPassword: "MASTER_USER_PASSWORD", // Required - must contain at least
  one uppercase letter, and one number
  ClusterType: "CLUSTER_TYPE", // Required
```

```

IAMRoleARN: "IAM_ROLE_ARN", // Optional - the ARN of an IAM role with
permissions your cluster needs to access other AWS services on your behalf, such
as Amazon S3.
ClusterSubnetGroupName: "CLUSTER_SUBNET_GROUPNAME", //Optional - the name of a
cluster subnet group to be associated with this cluster. Defaults to 'default'
if not specified.
DBName: "DATABASE_NAME", // Optional - defaults to 'dev' if not specified
Port: "PORT_NUMBER", // Optional - defaults to '5439' if not specified
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new CreateClusterCommand(params));
    console.log(
      "Cluster " + data.Cluster.ClusterIdentifier + " successfully created",
    );
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();

```

- Per i dettagli sull'API, [CreateCluster](#) consulta AWS SDK for JavaScript API Reference.

## Kotlin

### SDK per Kotlin

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

### Crea il cluster .

```

suspend fun createCluster(
    clusterId: String?,
    masterUsernameVal: String?,
    masterUserPasswordVal: String?,

```

```

) {
    val clusterRequest =
        CreateClusterRequest {
            clusterIdentifier = clusterId
            masterUsername = masterUsernameVal
            masterUserPassword = masterUserPasswordVal
            nodeType = "ds2.xlarge"
            publiclyAccessible = true
            numberOfNodes = 2
        }

    RedshiftClient { region = "us-east-1" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.createCluster(clusterRequest)
        println("Created cluster ${clusterResponse.cluster?.clusterIdentifier}")
    }
}

```

- Per i dettagli sull'API, [CreateCluster](#) consulta AWS SDK for Kotlin API reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```

class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

```

```
def create_cluster(
    self,
    cluster_identifier,
    node_type,
    master_username,
    master_user_password,
    publicly_accessible,
    number_of_nodes,
):
    """
    Creates a cluster.

    :param cluster_identifier: The name of the cluster.
    :param node_type: The type of node in the cluster.
    :param master_username: The master username.
    :param master_user_password: The master user password.
    :param publicly_accessible: Whether the cluster is publicly accessible.
    :param number_of_nodes: The number of nodes in the cluster.
    :return: The cluster.
    """

    try:
        cluster = self.client.create_cluster(
            ClusterIdentifier=cluster_identifier,
            NodeType=node_type,
            MasterUsername=master_username,
            MasterUserPassword=master_user_password,
            PubliclyAccessible=publicly_accessible,
            NumberOfNodes=number_of_nodes,
        )
        return cluster
    except ClientError as err:
        logging.error(
            "Couldn't create a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

Il codice seguente crea un'istanza dell' `RedshiftWrapper` oggetto.

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Per i dettagli sull'API, consulta [CreateCluster AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **CreateTable** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `CreateTable`.

### Java

#### SDK per Java 2.x

#### Note

C'è altro su [GitHub](#). Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
        .clusterIdentifier(clusterId)
        .dbUser(userName)
        .database(databaseName)
        .sql("CREATE TABLE Movies ("
            + "id INT PRIMARY KEY, "
            + "title VARCHAR(100), "
            + "year INT)")
        .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");
    }
}
```

```

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}

```

- Per i dettagli sull'API, [CreateTable](#) consulta AWS SDK for Java 2.x API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```

def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_idenfifier=cluster_id,
        database_name=database,
        user_name=username,
        sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
    )

    print("Table created: Movies")

```

### Chiamata di oggetti Wrapper. ExecuteStatement

```

class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.

```

```
    """
    self.client = client

    def execute_statement(
        self, cluster_identifier, database_name, user_name, sql,
        parameter_list=None
    ):
        """
        Executes a SQL statement.

        :param cluster_identifier: The cluster identifier.
        :param database_name: The database name.
        :param user_name: The user's name.
        :param sql: The SQL statement.
        :param parameter_list: The optional SQL statement parameters.
        :return: The SQL statement result.
        """

        try:
            kwargs = {
                "ClusterIdentifier": cluster_identifier,
                "Database": database_name,
                "DbUser": user_name,
                "Sql": sql,
            }
            if parameter_list:
                kwargs["Parameters"] = parameter_list
            response = self.client.execute_statement(**kwargs)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't execute statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Il codice seguente crea un'istanza dell'oggetto. `RedshiftDataWrapper`

```
client = boto3.client("redshift-data")
```

```
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Per i dettagli sull'API, consulta [CreateTable AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **DeleteCluster** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `DeleteCluster`.

### CLI

#### AWS CLI

L' `Snapshot` Questo esempio Elimina un cluster senza un cluster finale elimina un cluster, forzando l'eliminazione dei dati in modo che non venga creata alcuna istantanea finale del cluster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --skip-final-cluster-snapshot
```

L' `Snapshot` Questo esempio Elimina un cluster, `Allowing a Final Cluster` elimina un cluster, ma specifica uno snapshot finale del cluster. Comando:

```
aws redshift delete-cluster --cluster-identifier mycluster --final-cluster-snapshot-identifier myfinalsnapshot
```

- Per i dettagli sull'API, vedere in Command Reference. [DeleteCluster](#) AWS CLI

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

### Elimina il cluster.

```
public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
    try {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();

        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Per i dettagli sull'API, [DeleteCluster](#) consulta AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

#### Crea il client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

#### Crea il cluster .

```
// Import required AWS SDK clients and commands for Node.js
import { DeleteClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  SkipFinalClusterSnapshot: false,
  FinalClusterSnapshotIdentifier: "CLUSTER_SNAPSHOT_ID",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DeleteClusterCommand(params));
    console.log("Success, cluster deleted. ", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Per i dettagli sull'API, [DeleteCluster](#) consulta AWS SDK for JavaScript API Reference.

## Kotlin

### SDK per Kotlin

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Elimina il cluster.

```
suspend fun deleteRedshiftCluster(clusterId: String?) {
    val request =
        DeleteClusterRequest {
            clusterIdentifier = clusterId
            skipFinalClusterSnapshot = true
        }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val response = redshiftClient.deleteCluster(request)
        println("The status is ${response.cluster?.clusterStatus}")
    }
}
```

- Per i dettagli sull'API, [DeleteCluster](#) consulta AWS SDK for Kotlin API reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def delete_cluster(self, cluster_identifier):
        """
        Deletes a cluster.

        :param cluster_identifier: The cluster identifier.
        """
        try:
            self.client.delete_cluster(
                ClusterIdentifier=cluster_identifier,
                SkipFinalClusterSnapshot=True
            )
        except ClientError as err:
            logging.error(
                "Couldn't delete a cluster. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
            raise
```

Il codice seguente crea un'istanza dell' `RedshiftWrapper` oggetto.

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Per i dettagli sull'API, consulta [DeleteCluster AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo `DescribeClusters` con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `DescribeClusters`.

### CLI

#### AWS CLI

L' `Clusters` This esempio `Get a Description of All` restituisce una descrizione di tutti i cluster dell'account. Per impostazione predefinita, l'output è in formato JSON. Comando:

```
aws redshift describe-clusters
```

Risultato:

```
{
  "Clusters": [
    {
      "NodeType": "dw.hs1.xlarge",
      "Endpoint": {
        "Port": 5439,
        "Address": "mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com"
      },
      "ClusterVersion": "1.0",
      "PubliclyAccessible": "true",
      "MasterUsername": "adminuser",
      "ClusterParameterGroups": [
        {
```

```

        "ParameterApplyStatus": "in-sync",
        "ParameterGroupName": "default.redshift-1.0"
    } ],
    "ClusterSecurityGroups": [
    {
        "Status": "active",
        "ClusterSecurityGroupName": "default"
    } ],
    "AllowVersionUpgrade": true,
    "VpcSecurityGroups": \[],
    "AvailabilityZone": "us-east-1a",
    "ClusterCreateTime": "2013-01-22T21:59:29.559Z",
    "PreferredMaintenanceWindow": "sat:03:30-sat:04:00",
    "AutomatedSnapshotRetentionPeriod": 1,
    "ClusterStatus": "available",
    "ClusterIdentifier": "mycluster",
    "DBName": "dev",
    "NumberOfNodes": 2,
    "PendingModifiedValues": {}
} ],
"ResponseMetadata": {
    "RequestId": "65b71cac-64df-11e2-8f5b-e90bd6c77476"
}
}

```

È inoltre possibile ottenere le stesse informazioni in formato testo utilizzando l'opzione.

Comando: `--output text`

`--output text` Opzione. Comando:

Opzione. comando:

```
aws redshift describe-clusters --output text
```

Risultato:

```

dw.hs1.xlarge      1.0      true      adminuser      True      us-east-1a
2013-01-22T21:59:29.559Z      sat:03:30-sat:04:00      1      available
mycluster          dev      2
ENDPOINT          5439      mycluster.coqoarplqhsn.us-east-1.redshift.amazonaws.com
in-sync           default.redshift-1.0
active            default

```

```
PENDINGMODIFIEDVALUES
RESPONSEMETADATA    934281a8-64df-11e2-b07c-f7fbdd006c67
```

- Per i dettagli sull'API, vedere [DescribeClusters](#) in AWS CLI Command Reference.

## Java

### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

### Descrivi il cluster.

```
public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
    boolean clusterReady = false;
    String clusterReadyStr;
    System.out.println("Waiting for cluster to become available. This may
take a few mins.");
    try {
        DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
            .clusterIdentifier(clusterId)
            .build();
        long startTime = System.currentTimeMillis();

        // Loop until the cluster is ready.
        while (!clusterReady) {
            DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
            List<Cluster> clusterList = clusterResponse.clusters();
            for (Cluster cluster : clusterList) {
                clusterReadyStr = cluster.clusterStatus();
                if (clusterReadyStr.contains("available"))
                    clusterReady = true;
                else {
                    long elapsedTimeMillis = System.currentTimeMillis() -
startTime;
```

```

        long elapsedSeconds = elapsedTimeMillis / 1000;
        long minutes = elapsedSeconds / 60;
        long seconds = elapsedSeconds % 60;

        System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
        TimeUnit.SECONDS.sleep(5);
    }
}

long elapsedTimeMillis = System.currentTimeMillis() - startTime;
long elapsedSeconds = elapsedTimeMillis / 1000;
long minutes = elapsedSeconds / 60;
long seconds = elapsedSeconds % 60;

System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

} catch (RedshiftException | InterruptedException e) {
    System.err.println(e.getMessage());
    System.exit(1);
}
}

```

- Per i dettagli sull'API, [DescribeClusters](#) consulta AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

### Crea il client.

```

import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.

```

```
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

Descrivi i tuoi cluster.

```
// Import required AWS SDK clients and commands for Node.js
import { DescribeClustersCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

const params = {
  ClusterIdentifier: "CLUSTER_NAME",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new DescribeClustersCommand(params));
    console.log("Success", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Per i dettagli sull'API, consulta [DescribeClusters AWS SDK for JavaScript API Reference](#).

## Kotlin

### SDK per Kotlin

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Descrivi il cluster.

```
suspend fun describeRedshiftClusters() {
    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse =
        redshiftClient.describeClusters(DescribeClustersRequest {})
        val clusterList = clusterResponse.clusters

        if (clusterList != null) {
            for (cluster in clusterList) {
                println("Cluster database name is ${cluster.dbName}")
                println("Cluster status is ${cluster.clusterStatus}")
            }
        }
    }
}
```

- Per i dettagli sull'API, [DescribeClusters](#) consulta AWS SDK for Kotlin API reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
        self.client = redshift_client

    def describe_clusters(self, cluster_identifier):
```

```
"""
Describes a cluster.

:param cluster_identifier: The cluster identifier.
:return: A list of clusters.
"""
try:
    kwargs = {}
    if cluster_identifier:
        kwargs["ClusterIdentifier"] = cluster_identifier

    paginator = self.client.get_paginator("describe_clusters")
    clusters = []
    for page in paginator.paginate(**kwargs):
        clusters.extend(page["Clusters"])

    return clusters

except ClientError as err:
    logging.error(
        "Couldn't describe a cluster. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise
```

Il codice seguente crea un'istanza dell' `RedshiftWrapper` oggetto.

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Per i dettagli sull'API, consulta [DescribeClusters AWSSDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **DescribeStatement** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `DescribeStatement`.

### Java

#### SDK per Java 2.x

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
    try {
        DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
            .id(sqlId)
            .build();

        String status;
        while (true) {
            DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
            status = response.statusAsString();
            System.out.println("..." + status);

            if (status.compareTo("FAILED") == 0 ) {
                System.out.println("The Query Failed. Ending program");
                System.exit(1);

            } else if (status.compareTo("FINISHED") == 0) {
                break;
            }
            TimeUnit.SECONDS.sleep(1);
        }

        System.out.println("The statement is finished!");
    } catch (RedshiftDataException | InterruptedException e) {
```

```
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Per i dettagli sull'API, [DescribeStatement](#) consulta AWS SDK for Java 2.x API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

    def describe_statement(self, statement_id):
        """
        Describes a SQL statement.

        :param statement_id: The SQL statement identifier.
        :return: The SQL statement result.
        """
        try:
            response = self.client.describe_statement(Id=statement_id)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't describe statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
```

```
        err.response["Error"]["Message"],
    )
    raise
```

Il codice seguente crea un'istanza dell' `RedshiftDataWrapper` oggetto.

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Per i dettagli sull'API, consulta [DescribeStatement AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo `GetStatementResult` con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `GetStatementResult`.

### Java

#### SDK per Java 2.x

#### Note

C'è altro su [GitHub](#). Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Controlla il risultato della dichiarazione.

```
public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
    try {
        GetStatementResultRequest resultRequest =
        GetStatementResultRequest.builder()
            .id(statementId)
```

```

        .build());

        // Extract and print the field values using streams.
        GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
        response.records().stream()
            .flatMap(List::stream)
            .map(Field::stringValue)
            .filter(value -> value != null)
            .forEach(value -> System.out.println("The Movie title field is "
+ value));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

```

- Per i dettagli sull'API, consulta [GetStatementResult](#) in AWS SDK for Java 2.x API Reference.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```

class RedshiftDataWrapper:
    """Encapsulates Amazon Redshift data."""

    def __init__(self, client):
        """
        :param client: A Boto3 RedshiftDataWrapper client.
        """
        self.client = client

```

```
def get_statement_result(self, statement_id):
    """
    Gets the result of a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        result = {
            "Records": [],
        }
        paginator = self.client.get_paginator("get_statement_result")
        for page in paginator.paginate(Id=statement_id):
            if "ColumnMetadata" not in result:
                result["ColumnMetadata"] = page["ColumnMetadata"]
            result["Records"].extend(page["Records"])
        return result
    except ClientError as err:
        logging.error(
            "Couldn't get statement result. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

Il codice seguente crea un'istanza dell' `RedshiftDataWrapper` oggetto.

```
client = boto3.client("redshift-data")
redshift_data_wrapper = RedshiftDataWrapper(client)
```

- Per i dettagli sull'API, consulta [GetStatementResult](#) in AWS SDK for Python (Boto3) API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **Insert** con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare `Insert`.

Java

SDK per Java 2.x

### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) iter.next();
        int year = currentNode.get("year").asInt();
        String title = currentNode.get("title").asText();

        // Use SqlParameter to avoid SQL injection.
        List<SqlParameter> parameterList = new ArrayList<>();
        String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year)";

        // Create the parameters.
        SqlParameter idParam = SqlParameter.builder()
            .name("id")
            .value(String.valueOf(t))
            .build();

        SqlParameter titleParam= SqlParameter.builder()
```

```
        .name("title")
        .value(title)
        .build();

SqlParameter yearParam = SqlParameter.builder()
    .name("year")
    .value(String.valueOf(year))
    .build();
parameterList.add(idParam);
parameterList.add(titleParam);
parameterList.add(yearParam);

try {
    ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
    .clusterIdentifier(clusterId)
    .sql(sqlStatement)
    .database(databaseName)
    .dbUser(userName)
    .parameters(parameterList)
    .build();

    redshiftDataClient.executeStatement(insertStatementRequest);
    System.out.println("Inserted: " + title + " (" + year + ")");
    t++;

} catch (RedshiftDataException e) {
    System.err.println("Error inserting data: " + e.getMessage());
    System.exit(1);
}
}
System.out.println(t + " records were added to the Movies table. ");
}
```

- Per i dettagli sull'API, consulta [Insert](#) in AWS SDK for Java 2.x API Reference.

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **ModifyCluster** con un AWS SDK o una CLI

I seguenti esempi di codice mostrano come utilizzare `ModifyCluster`.

### CLI

#### AWS CLI

Associare un gruppo di sicurezza a un Cluster. Questo esempio mostra come associare un gruppo di sicurezza del cluster al Cluster. Comando specificato:

```
aws redshift modify-cluster --cluster-identifier mycluster --cluster-security-groups mysecuritygroup
```

Modifica la finestra di manutenzione per Cluster. Questo mostra come modificare la finestra di manutenzione settimanale preferita per un cluster in modo che diventi la finestra di manutenzione minima di quattro ore che inizia la domenica alle 23:15 e termina il lunedì alle 3:15. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --preferred-maintenance-window Sun:23:15-Mon:03:15
```

Modifica la password principale: nell' Cluster. Questo esempio viene illustrato come modificare la password principale per un Cluster. Comando:

```
aws redshift modify-cluster --cluster-identifier mycluster --master-user-password A1b2c3d4
```

- Per i dettagli sull'API, vedere [ModifyCluster](#) in AWS CLI Command Reference.

### Java

#### SDK per Java 2.x

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

## Modifica un cluster.

```
public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
    try {
        ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .preferredMaintenanceWindow("wed:07:30-wed:08:00")
            .build();

        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

- Per i dettagli sull'API, [ModifyCluster](#) consulta AWS SDK for Java 2.x API Reference.

## JavaScript

### SDK per JavaScript (v3)

#### Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

## Crea il client.

```
import { RedshiftClient } from "@aws-sdk/client-redshift";
// Set the AWS Region.
```

```
const REGION = "REGION";
//Set the Redshift Service Object
const redshiftClient = new RedshiftClient({ region: REGION });
export { redshiftClient };
```

## Modifica un cluster.

```
// Import required AWS SDK clients and commands for Node.js
import { ModifyClusterCommand } from "@aws-sdk/client-redshift";
import { redshiftClient } from "../libs/redshiftClient.js";

// Set the parameters
const params = {
  ClusterIdentifier: "CLUSTER_NAME",
  MasterUserPassword: "NEW_MASTER_USER_PASSWORD",
};

const run = async () => {
  try {
    const data = await redshiftClient.send(new ModifyClusterCommand(params));
    console.log("Success was modified.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

- Per i dettagli sull'API, [ModifyCluster](#) consulta AWS SDK for JavaScript API Reference.

## Kotlin

### SDK per Kotlin

#### Note

C'è altro su GitHub. Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

## Modifica un cluster.

```
suspend fun modifyCluster(clusterId: String?) {
    val modifyClusterRequest =
        ModifyClusterRequest {
            clusterIdentifier = clusterId
            preferredMaintenanceWindow = "wed:07:30-wed:08:00"
        }

    RedshiftClient { region = "us-west-2" }.use { redshiftClient ->
        val clusterResponse = redshiftClient.modifyCluster(modifyClusterRequest)
        println(
            "The modified cluster was successfully modified and has
            ${clusterResponse.cluster?.preferredMaintenanceWindow} as the maintenance
            window",
        )
    }
}
```

- Per i dettagli sull'API, consulta il riferimento [ModifyCluster](#) all'API AWS SDK for Kotlin.

## Python

### SDK per Python (Boto3)

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
class RedshiftWrapper:
    """
    Encapsulates Amazon Redshift cluster operations.
    """

    def __init__(self, redshift_client):
        """
        :param redshift_client: A Boto3 Redshift client.
        """
```

```
self.client = redshift_client

def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
    """
    Modifies a cluster.

    :param cluster_identifier: The cluster identifier.
    :param preferred_maintenance_window: The preferred maintenance window.
    """
    try:
        self.client.modify_cluster(
            ClusterIdentifier=cluster_identifier,
            PreferredMaintenanceWindow=preferred_maintenance_window,
        )
    except ClientError as err:
        logging.error(
            "Couldn't modify a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

Il codice seguente crea un'istanza dell' `RedshiftWrapper` oggetto.

```
client = boto3.client("redshift")
redshift_wrapper = RedshiftWrapper(client)
```

- Per i dettagli sull'API, consulta [ModifyCluster AWS SDK for Python \(Boto3\) API Reference](#).

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Utilizzo **Query** con un AWS SDK o una CLI

Il seguente esempio di codice mostra come utilizzare `Query`.

## Java

### SDK per Java 2.x

#### Note

C'è altro su [GitHub](#) Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

Interroga una tabella.

```
public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                       String database,
                                       String dbUser,
                                       int year,
                                       String clusterId) {

    try {
        String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam= SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
    return "";
}
```

```
}
```

- Per ulteriori informazioni sulle API, consulta [Query](#) nella Documentazione di riferimento delle API AWS SDK for Java 2.x .

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Scenari per Amazon Redshift che utilizzano SDK AWS

I seguenti esempi di codice mostrano come implementare scenari comuni in Amazon Redshift con AWS SDK. Questi scenari mostrano come eseguire attività specifiche richiamando più funzioni all'interno di Amazon Redshift. Ogni scenario include un collegamento a GitHub, dove puoi trovare istruzioni su come configurare ed eseguire il codice.

### Esempi

- [Inizia a usare tabelle, elementi e query di Amazon Redshift](#)

## Inizia a usare tabelle, elementi e query di Amazon Redshift

I seguenti esempi di codice mostrano come lavorare con tabelle, elementi e query di Amazon Redshift.

### Java

#### SDK per Java 2.x

#### Note

C'è altro su. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
import com.fasterxml.jackson.core.JsonFactory;
import com.fasterxml.jackson.databind.JsonNode;
import com.fasterxml.jackson.databind.ObjectMapper;
```

```
import com.fasterxml.jackson.databind.node.ObjectNode;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.redshift.RedshiftClient;
import software.amazon.awssdk.services.redshift.model.Cluster;
import software.amazon.awssdk.services.redshift.model.CreateClusterRequest;
import software.amazon.awssdk.services.redshift.model.CreateClusterResponse;
import software.amazon.awssdk.services.redshift.model.DeleteClusterRequest;
import software.amazon.awssdk.services.redshift.model.DeleteClusterResponse;
import software.amazon.awssdk.services.redshift.model.DescribeClustersRequest;
import software.amazon.awssdk.services.redshift.model.DescribeClustersResponse;
import software.amazon.awssdk.services.redshift.model.ModifyClusterRequest;
import software.amazon.awssdk.services.redshift.model.ModifyClusterResponse;
import software.amazon.awssdk.services.redshift.model.RedshiftException;
import software.amazon.awssdk.services.redshiftdata.RedshiftDataClient;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.DescribeStatementResponse;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.ExecuteStatementResponse;
import software.amazon.awssdk.services.redshiftdata.model.Field;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultRequest;
import
    software.amazon.awssdk.services.redshiftdata.model.GetStatementResultResponse;
import software.amazon.awssdk.services.redshiftdata.model.ListDatabasesRequest;
import software.amazon.awssdk.services.redshiftdata.model.RedshiftDataException;
import software.amazon.awssdk.services.redshiftdata.model.SqlParameter;
import
    software.amazon.awssdk.services.redshiftdata.paginators.ListDatabasesIterable;
import com.fasterxml.jackson.core.JsonParser;
import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.Iterator;
import java.util.List;
import java.util.Scanner;
import java.util.concurrent.TimeUnit;

/**
 * Before running this Java V2 code example, set up your development
 * environment, including your credentials.
```

```
*
* For more information, see the following documentation topic:
*
* https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/get-started.html
*
*
This Java example performs these tasks:
*
* 1. Prompts the user for a unique cluster ID or use the default value.
* 2. Creates a Redshift cluster with the specified or default cluster Id value.
* 3. Waits until the Redshift cluster is available for use.
* 4. Lists all databases using a pagination API call.
* 5. Creates a table named "Movies" with fields ID, title, and year.
* 6. Inserts a specified number of records into the "Movies" table by reading the Movies JSON file.
* 7. Prompts the user for a movie release year.
* 8. Runs a SQL query to retrieve movies released in the specified year.
* 9. Modifies the Redshift cluster.
* 10. Prompts the user for confirmation to delete the Redshift cluster.
* 11. If confirmed, deletes the specified Redshift cluster.
*/

public class RedshiftScenario {
    public static final String DASHES = new String(new char[80]).replace("\0", "-");
    public static void main(String[] args) throws Exception {
        final String usage = ""

            Usage:
                <jsonFilePath>\s

            Where:
                jsonFilePath - The path to the Movies JSON file (you can locate that file in ../../../../resources/sample_files/movies.json)
                """;

        if (args.length != 1) {
            System.out.println(usage);
            System.exit(1);
        }

        String jsonFilePath = args[0];
        String userName;
```

```
String userPassword;
String databaseName = "dev" ;
Scanner scanner = new Scanner(System.in);

Region region = Region.US_EAST_1;
RedshiftClient redshiftClient = RedshiftClient.builder()
    .region(region)
    .build();

RedshiftDataClient redshiftDataClient = RedshiftDataClient.builder()
    .region(region)
    .build();

System.out.println(DASHES);
System.out.println("Welcome to the Amazon Redshift SDK Getting Started
scenario.");
System.out.println("""
This Java program demonstrates how to interact with Amazon Redshift by
using the AWS SDK for Java (v2).\s
Amazon Redshift is a fully managed, petabyte-scale data warehouse service
hosted in the cloud.

The program's primary functionalities include cluster creation,
verification of cluster readiness,\s
list databases, table creation, data population within the table, and
execution of SQL statements.
Furthermore, it demonstrates the process of querying data from the Movie
table.\s

Upon completion of the program, all AWS resources are cleaned up.
""");

System.out.println("Lets get started...");
System.out.println("Please enter your user name (default is awsuser)");
String user = scanner.nextLine();
userName = user.isEmpty() ? "awsuser" : user;
System.out.println(DASHES);
System.out.println("Please enter your user password (default is
AwsUser1000)");
String userpass = scanner.nextLine();
userPassword = userpass.isEmpty() ? "AwsUser1000" : userpass;
System.out.println(DASHES);

System.out.println(DASHES);
```

```
System.out.println("A Redshift cluster refers to the collection of
computing resources and storage that work together to process and analyze large
volumes of data.");
System.out.println("Enter a cluster id value (default is redshift-
cluster-movies): ");
String userClusterId = scanner.nextLine();
String clusterId = userClusterId.isEmpty() ? "redshift-cluster-movies" :
userClusterId;
createCluster(redshiftClient, clusterId, userName, userPassword);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Wait until "+clusterId +" is available.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
waitForClusterReady(redshiftClient, clusterId);
System.out.println(DASHES);

System.out.println(DASHES);
String databaseInfo = ""
    When you created $clusteridD, the dev database is created by default
and used in this scenario.\s

    To create a custom database, you need to have a CREATEDB privilege.\s
    For more information, see the documentation here: https://
docs.aws.amazon.com/redshift/latest/dg/r\_CREATE\_DATABASE.html.
    """".replace("$clusteridD", clusterId);

System.out.println(databaseInfo);
System.out.print("Press Enter to continue...");
scanner.nextLine();
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("List databases in "+clusterId);
System.out.print("Press Enter to continue...");
scanner.nextLine();
listAllDatabases(redshiftDataClient, clusterId, userName, databaseName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Now you will create a table named Movies.");
System.out.print("Press Enter to continue...");
scanner.nextLine();
```

```
createTable(redshiftDataClient, clusterId, databaseName, userName);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Populate the Movies table using the Movies.json
file.");
System.out.println("Specify the number of records you would like to add
to the Movies Table.");
System.out.println("Please enter a value between 50 and 200.");
int numRecords;
do {
    System.out.print("Enter a value: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a value between
50 and 200.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    numRecords = scanner.nextInt();
} while (numRecords < 50 || numRecords > 200);
popTable(redshiftDataClient, clusterId, databaseName, userName,
jsonFilePath, numRecords);
System.out.println(DASHES);

System.out.println(DASHES);
System.out.println("Query the Movies table by year. Enter a value between
2012-2014.");
int movieYear;
do {
    System.out.print("Enter a year: ");
    while (!scanner.hasNextInt()) {
        System.out.println("Invalid input. Please enter a valid year
between 2012 and 2014.");
        System.out.print("Enter a year: ");
        scanner.next();
    }
    movieYear = scanner.nextInt();
    scanner.nextLine();
} while (movieYear < 2012 || movieYear > 2014);

String id = queryMoviesByYear(redshiftDataClient, databaseName, userName,
movieYear, clusterId);
System.out.println("The identifier of the statement is " + id);
checkStatement(redshiftDataClient, id);
```

```
    getResults(redshiftDataClient, id);
    System.out.println(DASHES);

    System.out.println(DASHES);
    System.out.println("Now you will modify the Redshift cluster.");
    System.out.print("Press Enter to continue...");
    scanner.nextLine();
    modifyCluster(redshiftClient, clusterId);
    System.out.println(DASHES);

    System.out.println(DASHES);
    System.out.println("Would you like to delete the Amazon Redshift cluster?
(y/n)");
    String delAns = scanner.nextLine().trim();
    if (delAns.equalsIgnoreCase("y")) {
        System.out.println("You selected to delete " +clusterId);
        System.out.print("Press Enter to continue...");
        scanner.nextLine();
        deleteRedshiftCluster(redshiftClient, clusterId);
    } else {
        System.out.println("The "+clusterId +" was not deleted");
    }
    System.out.println(DASHES);

    System.out.println(DASHES);
    System.out.println("This concludes the Amazon Redshift SDK Getting
Started scenario.");
    System.out.println(DASHES);
}

public static void listAllDatabases(RedshiftDataClient redshiftDataClient,
String clusterId, String dbUser, String database) {
    try {
        ListDatabasesRequest databasesRequest =
ListDatabasesRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(dbUser)
            .database(database)
            .build();

        ListDatabasesIterable listDatabasesIterable =
redshiftDataClient.listDatabasesPaginator(databasesRequest);
        listDatabasesIterable.stream()
            .flatMap(r -> r.databases().stream())
```

```
        .forEach(db -> System.out
            .println("The database name is : " + db));

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void deleteRedshiftCluster(RedshiftClient redshiftClient,
String clusterId) {
    try {
        DeleteClusterRequest deleteClusterRequest =
DeleteClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .skipFinalClusterSnapshot(true)
            .build();

        DeleteClusterResponse response =
redshiftClient.deleteCluster(deleteClusterRequest);
        System.out.println("The status is " +
response.cluster().clusterStatus());

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void popTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName, String fileName, int number)
throws IOException {
    JsonParser parser = new JsonFactory().createParser(new File(fileName));
    com.fasterxml.jackson.databind.JsonNode rootNode = new
ObjectMapper().readTree(parser);
    Iterator<JsonNode> iter = rootNode.iterator();
    ObjectNode currentNode;
    int t = 0;
    while (iter.hasNext()) {
        if (t == number)
            break;
        currentNode = (ObjectNode) iter.next();
        int year = currentNode.get("year").asInt();
        String title = currentNode.get("title").asText();
    }
}
```

```
        // Use SqlParameter to avoid SQL injection.
        List<SqlParameter> parameterList = new ArrayList<>();
        String sqlStatement = "INSERT INTO Movies
VALUES( :id , :title, :year)";

        // Create the parameters.
        SqlParameter idParam = SqlParameter.builder()
            .name("id")
            .value(String.valueOf(t))
            .build();

        SqlParameter titleParam= SqlParameter.builder()
            .name("title")
            .value(title)
            .build();

        SqlParameter yearParam = SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();
        parameterList.add(idParam);
        parameterList.add(titleParam);
        parameterList.add(yearParam);

        try {
            ExecuteStatementRequest insertStatementRequest =
ExecuteStatementRequest.builder()
                .clusterIdentifier(clusterId)
                .sql(sqlStatement)
                .database(databaseName)
                .dbUser(userName)
                .parameters(parameterList)
                .build();

            redshiftDataClient.executeStatement(insertStatementRequest);
            System.out.println("Inserted: " + title + " (" + year + ")");
            t++;

        } catch (RedshiftDataException e) {
            System.err.println("Error inserting data: " + e.getMessage());
            System.exit(1);
        }
    }
}
```

```
        System.out.println(t + " records were added to the Movies table. ");
    }

    public static void checkStatement(RedshiftDataClient redshiftDataClient,
String sqlId) {
        try {
            DescribeStatementRequest statementRequest =
DescribeStatementRequest.builder()
                .id(sqlId)
                .build();

            String status;
            while (true) {
                DescribeStatementResponse response =
redshiftDataClient.describeStatement(statementRequest);
                status = response.statusAsString();
                System.out.println("..." + status);

                if (status.compareTo("FAILED") == 0 ) {
                    System.out.println("The Query Failed. Ending program");
                    System.exit(1);

                } else if (status.compareTo("FINISHED") == 0) {
                    break;
                }
                TimeUnit.SECONDS.sleep(1);
            }

            System.out.println("The statement is finished!");

        } catch (RedshiftDataException | InterruptedException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void modifyCluster(RedshiftClient redshiftClient, String
clusterId) {
        try {
            ModifyClusterRequest modifyClusterRequest =
ModifyClusterRequest.builder()
                .clusterIdentifier(clusterId)
                .preferredMaintenanceWindow("wed:07:30-wed:08:00")
                .build();
```

```
        ModifyClusterResponse clusterResponse =
redshiftClient.modifyCluster(modifyClusterRequest);
        System.out.println("The modified cluster was successfully modified
and has "
            + clusterResponse.cluster().preferredMaintenanceWindow() + " as
the maintenance window");

    } catch (RedshiftException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static String queryMoviesByYear(RedshiftDataClient redshiftDataClient,
                                        String database,
                                        String dbUser,
                                        int year,
                                        String clusterId) {

    try {
        String sqlStatement = " SELECT * FROM Movies WHERE year = :year";
        SqlParameter yearParam= SqlParameter.builder()
            .name("year")
            .value(String.valueOf(year))
            .build();

        ExecuteStatementRequest statementRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .database(database)
            .dbUser(dbUser)
            .parameters(yearParam)
            .sql(sqlStatement)
            .build();

        ExecuteStatementResponse response =
redshiftDataClient.executeStatement(statementRequest);
        return response.id();

    } catch (RedshiftDataException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}
```

```
        return "";
    }

    public static void getResults(RedshiftDataClient redshiftDataClient, String
statementId) {
        try {
            GetStatementResultRequest resultRequest =
GetStatementResultRequest.builder()
                .id(statementId)
                .build();

            // Extract and print the field values using streams.
            GetStatementResultResponse response =
redshiftDataClient.getStatementResult(resultRequest);
            response.records().stream()
                .flatMap(List::stream)
                .map(Field::stringValue)
                .filter(value -> value != null)
                .forEach(value -> System.out.println("The Movie title field is "
+ value));

        } catch (RedshiftDataException e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }

    public static void waitForClusterReady(RedshiftClient redshiftClient, String
clusterId) {
        boolean clusterReady = false;
        String clusterReadyStr;
        System.out.println("Waiting for cluster to become available. This may
take a few mins.");
        try {
            DescribeClustersRequest clustersRequest =
DescribeClustersRequest.builder()
                .clusterIdentifier(clusterId)
                .build();
            long startTime = System.currentTimeMillis();

            // Loop until the cluster is ready.
            while (!clusterReady) {
                DescribeClustersResponse clusterResponse =
redshiftClient.describeClusters(clustersRequest);
```

```

        List<Cluster> clusterList = clusterResponse.clusters();
        for (Cluster cluster : clusterList) {
            clusterReadyStr = cluster.clusterStatus();
            if (clusterReadyStr.contains("available"))
                clusterReady = true;
            else {
                long elapsedTimeMillis = System.currentTimeMillis() -
startTime;

                long elapsedSeconds = elapsedTimeMillis / 1000;
                long minutes = elapsedSeconds / 60;
                long seconds = elapsedSeconds % 60;

                System.out.printf("Elapsed Time: %02d:%02d - Waiting for
cluster... %n", minutes, seconds);
                TimeUnit.SECONDS.sleep(5);
            }
        }

        long elapsedTimeMillis = System.currentTimeMillis() - startTime;
        long elapsedSeconds = elapsedTimeMillis / 1000;
        long minutes = elapsedSeconds / 60;
        long seconds = elapsedSeconds % 60;

        System.out.println(String.format("Cluster is available! Total Elapsed
Time: %02d:%02d", minutes, seconds));

    } catch (RedshiftException | InterruptedException e) {
        System.err.println(e.getMessage());
        System.exit(1);
    }
}

public static void createTable(RedshiftDataClient redshiftDataClient, String
clusterId, String databaseName, String userName) {
    try {
        ExecuteStatementRequest createTableRequest =
ExecuteStatementRequest.builder()
            .clusterIdentifier(clusterId)
            .dbUser(userName)
            .database(databaseName)
            .sql("CREATE TABLE Movies ("
                + "id INT PRIMARY KEY, "
                + "title VARCHAR(100), "

```

```

        + "year INT)")
        .build();

        redshiftDataClient.executeStatement(createTableRequest);
        System.out.println("Table created: Movies");

    } catch (RedshiftDataException e) {
        System.err.println("Error creating table: " + e.getMessage());
        System.exit(1);
    }
}

public static void createCluster(RedshiftClient redshiftClient, String
clusterId, String masterUsername,
                                String masterUserPassword) {
    try {
        CreateClusterRequest clusterRequest = CreateClusterRequest.builder()
            .clusterIdentifier(clusterId)
            .masterUsername(masterUsername)
            .masterUserPassword(masterUserPassword)
            .nodeType("ra3.4xlarge")
            .publiclyAccessible(true)
            .numberOfNodes(2)
            .build();

        CreateClusterResponse clusterResponse =
redshiftClient.createCluster(clusterRequest);
        System.out.println("Created cluster " +
clusterResponse.cluster().clusterIdentifier());

    } catch (RedshiftException e) {

        System.err.println(e.getMessage());
        System.exit(1);
    }
}
}
}

```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API AWS SDK for Java 2.x .
  - [createCluster](#)

- [Descrivi i cluster](#)
- [Descrivi la dichiarazione](#)
- [Esegui dichiarazione](#)
- [ottenere StatementResult](#)
- [elenco DatabasesPaginator](#)
- [modifica Cluster](#)

## Python

### SDK per Python (Boto3)

#### Note

C'è altro da fare. GitHub Trova l'esempio completo e scopri di più sulla configurazione e l'esecuzione nel [Repository di esempi di codice AWS](#).

```
class RedshiftScenario:
    """Runs an interactive scenario that shows how to get started with
    Redshift."""

    def __init__(self, redshift_wrapper, redshift_data_wrapper):
        self.redshift_wrapper = redshift_wrapper
        self.redshift_data_wrapper = redshift_data_wrapper

    def redshift_scenario(self, json_file_path):
        database_name = "dev"

        print(DASHES)
        print("Welcome to the Amazon Redshift SDK Getting Started example.")
        print(
            """
            This Python program demonstrates how to interact with Amazon Redshift
            using the AWS SDK for Python (Boto3).

            Amazon Redshift is a fully managed, petabyte-scale data warehouse
            service hosted in the cloud.

            The program's primary functionalities include cluster creation,
```

verification of cluster readiness, listing databases, table creation, populating data within the table, and executing SQL statements.

It also demonstrates querying data from the Movies table.

Upon completion, all AWS resources are cleaned up.

```
"""
)
if not os.path.isfile(json_file_path):
    logging.error(f"The file {json_file_path} does not exist.")
    return

print("Let's get started...")
user_name = q.ask("Please enter your user name (default is awsuser):")
user_name = user_name if user_name else "awsuser"

print(DASHES)
user_password = q.ask(
    "Please enter your user password (default is AwsUser1000):"
)
user_password = user_password if user_password else "AwsUser1000"

print(DASHES)
print(
    """A Redshift cluster refers to the collection of computing resources
and storage that work
    together to process and analyze large volumes of data."""
)
cluster_id = q.ask(
    "Enter a cluster identifier value (default is redshift-cluster-
movies): "
)
cluster_id = cluster_id if cluster_id else "redshift-cluster-movies"

self.redshift_wrapper.create_cluster(
    cluster_id, "ra3.4xlarge", user_name, user_password, True, 2
)

print(DASHES)
print(f"Wait until {cluster_id} is available. This may take a few
minutes...")
q.ask("Press Enter to continue...")

self.wait_cluster_available(cluster_id)
```

```
print(DASHES)

print(
    f"""
    When you created {cluster_id}, the dev database is created by default and
    used in this scenario.

    To create a custom database, you need to have a CREATEDB privilege.
    For more information, see the documentation here:
    https://docs.aws.amazon.com/redshift/latest/dg/r_CREATE_DATABASE.html.
    """
)
q.ask("Press Enter to continue...")
print(DASHES)

print(DASHES)
print(f"List databases in {cluster_id}")
q.ask("Press Enter to continue...")
databases = self.redshift_data_wrapper.list_databases(
    cluster_id, database_name, user_name
)
print(f"The cluster contains {len(databases)} database(s).")
for database in databases:
    print(f"    Database: {database}")
print(DASHES)

print(DASHES)
print("Now you will create a table named Movies.")
q.ask("Press Enter to continue...")

self.create_table(cluster_id, database_name, user_name)

print(DASHES)

print("Populate the Movies table using the Movies.json file.")
print(
    "Specify the number of records you would like to add to the Movies
    Table."
)
print("Please enter a value between 50 and 200.")

while True:
    try:
```

```
        num_records = int(q.ask("Enter a value: ", q.is_int))
        if 50 <= num_records <= 200:
            break
        else:
            print("Invalid input. Please enter a value between 50 and
200.")
    except ValueError:
        print("Invalid input. Please enter a value between 50 and 200.")

self.populate_table(
    cluster_id, database_name, user_name, json_file_path, num_records
)

print(DASHES)
print("Query the Movies table by year. Enter a value between 2012-2014.")

while True:
    movie_year = int(q.ask("Enter a year: ", q.is_int))
    if 2012 <= movie_year <= 2014:
        break
    else:
        print("Invalid input. Please enter a valid year between 2012 and
2014.")

# Function to query database
sql_id = self.query_movies_by_year(
    database_name, user_name, movie_year, cluster_id
)

print(f"The identifier of the statement is {sql_id}")

print("Checking statement status...")
self.wait_statement_finished(sql_id)
result = self.redshift_data_wrapper.get_statement_result(sql_id)

self.display_movies(result)

print(DASHES)

print(DASHES)
print("Now you will modify the Redshift cluster.")
q.ask("Press Enter to continue...")

preferred_maintenance_window = "wed:07:30-wed:08:00"
```

```
self.redshift_wrapper.modify_cluster(cluster_id,
preferred_maintenance_window)

print(DASHES)

print(DASHES)
delete = q.ask("Do you want to delete the cluster? (y/n) ", q.is_yesno)

if delete:
    print(f"You selected to delete {cluster_id}")
    q.ask("Press Enter to continue...")
    self.redshift_wrapper.delete_cluster(cluster_id)
else:
    print(f"Cluster {cluster_id}cluster_id was not deleted")

print(DASHES)
print("This concludes the Amazon Redshift SDK Getting Started scenario.")
print(DASHES)

def create_table(self, cluster_id, database, username):
    self.redshift_data_wrapper.execute_statement(
        cluster_idenfifier=cluster_id,
        database_name=database,
        user_name=username,
        sql="CREATE TABLE Movies (statement_id INT PRIMARY KEY, title
VARCHAR(100), year INT)",
    )

    print("Table created: Movies")

def populate_table(self, cluster_id, database, username, file_name, number):
    with open(file_name) as f:
        data = json.load(f)

    i = 0
    for record in data:
        if i == number:
            break

        statement_id = i
        title = record["title"]
        year = record["year"]
        i = i + 1
```

```

        parameters = [
            {"name": "statement_id", "value": str(statement_id)},
            {"name": "title", "value": title},
            {"name": "year", "value": str(year)},
        ]

        self.redshift_data_wrapper.execute_statement(
            cluster_identifier=cluster_id,
            database_name=database,
            user_name=username,
            sql="INSERT INTO Movies VALUES(:statement_id, :title, :year)",
            parameter_list=parameters,
        )

        print(f"{i} records inserted into Movies table")

def wait_cluster_available(self, cluster_id):
    """
    Waits for a cluster to be available.

    :param cluster_id: The cluster identifier.

    Note: The cluster_available waiter can also be used.
    It is not used in this case to allow an elapsed time message.
    """
    cluster_ready = False
    start_time = time.time()

    while not cluster_ready:
        time.sleep(30)
        cluster = self.redshift_wrapper.describe_clusters(cluster_id)
        status = cluster[0]["ClusterStatus"]
        if status == "available":
            cluster_ready = True
        elif status != "creating":
            raise Exception(
                f"Cluster {cluster_id} creation failed with status {status}."
            )

    elapsed_seconds = int(round(time.time() - start_time))
    minutes = int(elapsed_seconds // 60)
    seconds = int(elapsed_seconds % 60)

    print(f"Elapsed Time: {minutes}:{seconds:02d} - status {status}...")

```

```
        if minutes > 30:
            raise Exception(
                f"Cluster {cluster_id} is not available after 30 minutes."
            )

def query_movies_by_year(self, database, username, year, cluster_id):
    sql = "SELECT * FROM Movies WHERE year = :year"

    params = [{"name": "year", "value": str(year)}]

    response = self.redshift_data_wrapper.execute_statement(
        cluster_identifier=cluster_id,
        database_name=database,
        user_name=username,
        sql=sql,
        parameter_list=params,
    )

    return response["Id"]

@staticmethod
def display_movies(response):
    metadata = response["ColumnMetadata"]
    records = response["Records"]

    title_column_index = None
    for i in range(len(metadata)):
        if metadata[i]["name"] == "title":
            title_column_index = i
            break

    if title_column_index is None:
        print("No title column found.")
        return

    print(f"Found {len(records)} movie(s).")
    for record in records:
        print(f"    {record[title_column_index]['stringValue']}")

def wait_statement_finished(self, sql_id):
    while True:
        time.sleep(1)
        response = self.redshift_data_wrapper.describe_statement(sql_id)
```

```

        status = response["Status"]
        print(f"Statement status is {status}.")

        if status == "FAILED":
            print(f"The query failed because {response['Error']}. Ending
program")
            raise Exception("The Query Failed. Ending program")
        elif status == "FINISHED":
            break

```

Funzione principale che mostra l'implementazione dello scenario.

```

def main():
    redshift_client = boto3.client("redshift")
    redshift_data_client = boto3.client("redshift-data")
    redshift_wrapper = RedshiftWrapper(redshift_client)
    redshift_data_wrapper = RedshiftDataWrapper(redshift_data_client)
    redshift_scenario = RedshiftScenario(redshift_wrapper, redshift_data_wrapper)
    redshift_scenario.redshift_scenario(
        f"{os.path.dirname(__file__)}/../../resources/sample_files/
movies.json"
    )

```

Le funzioni wrapper utilizzate nello scenario.

```

def create_cluster(
    self,
    cluster_identifier,
    node_type,
    master_username,
    master_user_password,
    publicly_accessible,
    number_of_nodes,
):
    """
    Creates a cluster.

```

```
:param cluster_identifier: The name of the cluster.
:param node_type: The type of node in the cluster.
:param master_username: The master username.
:param master_user_password: The master user password.
:param publicly_accessible: Whether the cluster is publicly accessible.
:param number_of_nodes: The number of nodes in the cluster.
:return: The cluster.
"""

try:
    cluster = self.client.create_cluster(
        ClusterIdentifier=cluster_identifier,
        NodeType=node_type,
        MasterUsername=master_username,
        MasterUserPassword=master_user_password,
        PubliclyAccessible=publicly_accessible,
        NumberOfNodes=number_of_nodes,
    )
    return cluster
except ClientError as err:
    logging.error(
        "Couldn't create a cluster. Here's why: %s: %s",
        err.response["Error"]["Code"],
        err.response["Error"]["Message"],
    )
    raise

def describe_clusters(self, cluster_identifier):
    """
    Describes a cluster.

    :param cluster_identifier: The cluster identifier.
    :return: A list of clusters.
    """
    try:
        kwargs = {}
        if cluster_identifier:
            kwargs["ClusterIdentifier"] = cluster_identifier

        paginator = self.client.get_paginator("describe_clusters")
        clusters = []
        for page in paginator.paginate(**kwargs):
            clusters.extend(page["Clusters"])
```

```
        return clusters

    except ClientError as err:
        logging.error(
            "Couldn't describe a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

    def execute_statement(
        self, cluster_identifier, database_name, user_name, sql,
        parameter_list=None
    ):
        """
        Executes a SQL statement.

        :param cluster_identifier: The cluster identifier.
        :param database_name: The database name.
        :param user_name: The user's name.
        :param sql: The SQL statement.
        :param parameter_list: The optional SQL statement parameters.
        :return: The SQL statement result.
        """

        try:
            kwargs = {
                "ClusterIdentifier": cluster_identifier,
                "Database": database_name,
                "DbUser": user_name,
                "Sql": sql,
            }
            if parameter_list:
                kwargs["Parameters"] = parameter_list
            response = self.client.execute_statement(**kwargs)
            return response
        except ClientError as err:
            logging.error(
                "Couldn't execute statement. Here's why: %s: %s",
                err.response["Error"]["Code"],
                err.response["Error"]["Message"],
            )
```

```
        raise

def describe_statement(self, statement_id):
    """
    Describes a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        response = self.client.describe_statement(Id=statement_id)
        return response
    except ClientError as err:
        logging.error(
            "Couldn't describe statement. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def get_statement_result(self, statement_id):
    """
    Gets the result of a SQL statement.

    :param statement_id: The SQL statement identifier.
    :return: The SQL statement result.
    """
    try:
        result = {
            "Records": [],
        }
        paginator = self.client.get_paginator("get_statement_result")
        for page in paginator.paginate(Id=statement_id):
            if "ColumnMetadata" not in result:
                result["ColumnMetadata"] = page["ColumnMetadata"]
            result["Records"].extend(page["Records"])
        return result
    except ClientError as err:
        logging.error(
            "Couldn't get statement result. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

```
    )
    raise

def modify_cluster(self, cluster_identifier, preferred_maintenance_window):
    """
    Modifies a cluster.

    :param cluster_identifier: The cluster identifier.
    :param preferred_maintenance_window: The preferred maintenance window.
    """
    try:
        self.client.modify_cluster(
            ClusterIdentifier=cluster_identifier,
            PreferredMaintenanceWindow=preferred_maintenance_window,
        )
    except ClientError as err:
        logging.error(
            "Couldn't modify a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def list_databases(self, cluster_identifier, database_name, database_user):
    """
    Lists databases in a cluster.

    :param cluster_identifier: The cluster identifier.
    :param database_name: The database name.
    :param database_user: The database user.
    :return: The list of databases.
    """
    try:
        paginator = self.client.get_paginator("list_databases")
        databases = []
        for page in paginator.paginate(
            ClusterIdentifier=cluster_identifier,
            Database=database_name,
            DbUser=database_user,
        ):
            databases.extend(page["Databases"])
```

```
        return databases
    except ClientError as err:
        logging.error(
            "Couldn't list databases. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise

def delete_cluster(self, cluster_identifier):
    """
    Deletes a cluster.

    :param cluster_identifier: The cluster identifier.
    """
    try:
        self.client.delete_cluster(
            ClusterIdentifier=cluster_identifier,
            SkipFinalClusterSnapshot=True
        )
    except ClientError as err:
        logging.error(
            "Couldn't delete a cluster. Here's why: %s: %s",
            err.response["Error"]["Code"],
            err.response["Error"]["Message"],
        )
        raise
```

- Per informazioni dettagliate sull'API, consulta i seguenti argomenti nella Documentazione di riferimento delle API SDK AWS per Python (Boto3).
  - [createCluster](#)
  - [Descrivi i cluster](#)
  - [Descrivi la dichiarazione](#)
  - [Esegui dichiarazione](#)
  - [ottenere StatementResult](#)
  - [elenco DatabasesPaginator](#)
  - [modifica Cluster](#)

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta [Utilizzo di questo servizio con un SDK AWS](#). Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

## Esempi di servizi multipli per Amazon AWS Redshift che utilizzano SDK

Le seguenti applicazioni di esempio utilizzano AWS gli SDK per combinare Amazon Redshift con altri Servizi AWS. Ogni esempio include un link a GitHub, dove puoi trovare istruzioni su come configurare ed eseguire l'applicazione.

### Esempi

- [Come creare un tracker di articoli Amazon Redshift](#)

## Come creare un tracker di articoli Amazon Redshift

Gli esempi di codice seguenti mostrano come creare un'applicazione Web che traccia e segnala gli elementi di lavoro tramite un database Amazon Redshift.

### Java

#### SDK per Java 2.x

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon Redshift.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati di Amazon Redshift e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su [GitHub](#).

Servizi utilizzati in questo esempio

- Amazon Redshift
- Amazon SES

## Kotlin

### SDK per Kotlin

Mostra come creare un'applicazione Web che traccia e segnala gli elementi di lavoro archiviati in un database Amazon Redshift.

Per il codice sorgente completo e le istruzioni su come configurare un'API Spring REST che interroga i dati di Amazon Redshift e per l'utilizzo da parte di un'applicazione React, consulta l'esempio completo su. [GitHub](#)

Servizi utilizzati in questo esempio

- Amazon Redshift
- Amazon SES

Per un elenco completo delle guide per sviluppatori AWS SDK e degli esempi di codice, consulta. [Utilizzo di questo servizio con un SDK AWS](#) Questo argomento include anche informazioni su come iniziare e dettagli sulle versioni precedenti dell'SDK.

# Cronologia dei documenti

## Note

Per una descrizione delle nuove funzionalità di Amazon Redshift, consulta [What's new](#).

La tabella seguente descrive le importanti modifiche alla documentazione apportate alla Amazon Redshift Management Guide dopo giugno 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Versione API: 2012-12-01

Per un elenco delle modifiche alla Guida per gli sviluppatori di Amazon Redshift consultare [Cronologia del documento Guida per gli sviluppatori di database di Amazon Redshift](#).

Per ulteriori informazioni sulle nuove caratteristiche, incluso un elenco delle correzioni e dei numeri di versione dei cluster associati per ogni release, consultare [Cronologia delle versioni del cluster](#).

Modifica	Descrizione	Data
<a href="#">È stata rilasciata la patch 181 di Amazon Redshift.</a>	Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta la <a href="#">patch 181 di Amazon Redshift</a> .	1 maggio 2024
<a href="#">Aggiornamento delle policy gestite dell'editor di query v2</a>	Aggiornamenti a AmazonRedshiftQueryEditorV2 FullAccess , AmazonRedshiftQueryEditorV2	21 febbraio 2024

NoSharing AmazonRedshiftQueryEditorV2ReadSharing , e politiche AmazonRedshiftQueryEditorV2ReadWriteSharing gestite con autorizzazioni redshift-serverless:ListNamespaces e redshift-serverless:ListWorkgroups

[Aggiorna la policy di accesso gestito in sola lettura di Amazon Redshift](#)

Aggiornamenti alla policy AmazonRedshiftReadOnlyAccess gestita con autorizzazione redshift:ListRecommendations a elencare i consigli di Amazon Redshift Advisor.

7 febbraio 2024

[Rilasciata la patch 180 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 180 di Amazon Redshift.](#)

29 dicembre 2023

[Rilasciata la patch 179 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 179 di Amazon Redshift.](#)

9 novembre 2023

[Aggiornamento delle policy gestite da Amazon Redshift](#)

Aggiornamenti alla policy gestita da AmazonRedshiftServiceLinkedRolePolicy con le autorizzazioni ec2:AssignIpv6Addresses e ec2:UnassignIpv6Addresses .

31 ottobre 2023

[Rilasciata la patch 178 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 178 di Amazon Redshift.](#)

25 settembre 2023

[Aggiornamento delle policy gestite dell'editor di query v2](#)

Aggiornamenti alle policy gestite AmazonRedshiftQueryEditorV2NoSharing , AmazonRedshiftQueryEditorV2ReadSharing e AmazonRedshiftQueryEditorV2ReadWriteSharing con autorizzazioni sqlworkbench:GetAutocompletionMetadata e sqlworkbench:GetAutocompletionResource .

16 agosto 2023

[Aggiornamento della policy gestita di Amazon Redshift](#)

Aggiornamenti alla politica AmazonRedshiftServiceLinkedRolePolicy gestita per la concessione delle autorizzazioni AWS Secrets Manager per creare e gestire credenziali segrete di amministrazione.

14 agosto 2023

[Rilasciata la patch 177 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 177 di Amazon Redshift](#).

3 agosto 2023

[Rilasciata la patch 176 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 176 di Amazon Redshift.](#)

8 giugno 2023

[Rilasciata la patch 175 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 175 di Amazon Redshift.](#)

28 aprile 2023

[Aggiornamento della policy gestita di Amazon Redshift](#)

Aggiornamenti alla policy gestita AmazonRedshiftServiceLinkedRolePolicy per rimuovere le autorizzazioni per le operazioni relative alla rete ec2. Questi erano specificamente associati al tag Purpose: RedshiftMigrateToVpc resource.

27 aprile 2023

[Aggiornamento della policy gestita dell'API dati di Amazon Redshift](#)

Aggiornamenti alla policy gestita AmazonRedshiftDataFullAccess con l'autorizzazione redshift:GetClusterCredentialsWithIAM .

7 aprile 2023

[Aggiornamento delle policy gestite dell'editor di query v2](#)

Aggiornamenti a AmazonRedshiftQueryEditorV2NoSharing , AmazonRedshiftQueryEditorV2ReadSharing e policy gestite AmazonRedshiftQueryEditorV2ReadWriteSharing con autorizzazione sqlworkbench:GetSchemaInference .

21 marzo 2023

[Rilasciata la patch 174 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 174 di Amazon Redshift.](#)

11 marzo 2023

[Aggiornamento delle policy gestite dell'editor di query v2](#)

Aggiornamenti a AmazonRedshiftQueryEditorV2 NoSharing , AmazonRedshiftQueryEditorV2 ReadSharing e policy gestite AmazonRedshiftQueryEditorV2 ReadWriteSharing con autorizzazione sqlworkbench:AssociateNotebookWithTab .

2 febbraio 2023

[Rilasciata la patch 173 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 173 di Amazon Redshift.](#)

20 gennaio 2023

[Rilasciata la patch 172 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 172 di Amazon Redshift.](#)

17 novembre 2022

[Rilasciata la patch 171 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 171 di Amazon Redshift.](#)

9 novembre 2022

[Rilasciata la patch 170 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 170 di Amazon Redshift.](#)

20 luglio 2022

[Rilasciata la patch 169 di Amazon Redshift.](#)

Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta [Patch 169 di Amazon Redshift.](#)

8 giugno 2022

<a href="#">Rilasciata la patch 168 di Amazon Redshift.</a>	Una nuova patch di Amazon Redshift è in fase di implementazione. Sono necessarie diverse settimane prima che una nuova versione diventi disponibile in tutti i servizi supportati da Amazon Redshift. Regioni AWS Per ulteriori informazioni su questa versione, consulta <a href="#">Amazon Redshift patch 168</a> (Patch 168 di Amazon Redshift).	19 aprile 2022
<a href="#">Support per i profili di autenticazione con i driver Amazon Redshift</a>	Ora puoi connetterti ad Amazon Redshift con un profilo di autenticazione.	2 agosto 2021
<a href="#">Supporto per endpoint cross-VPC per Amazon Redshift fornito da AWS PrivateLink</a>	Ora puoi utilizzare gli endpoint VPC gestiti da RedShift con Amazon Redshift.	1 aprile 2021
<a href="#">Support per i miglioramenti dell'editor di query di Amazon Redshift</a>	Ora puoi utilizzare l'editor della query con il routing VPC avanzato, i tempi di esecuzione e della query più lunghi e più tipi di nodi cluster.	17 febbraio 2021
<a href="#">Supporto per l'integrazione della console con i partner</a>	È possibile integrarsi con i partner utilizzando la console Amazon Redshift.	9 dicembre 2020
<a href="#">Supporto per la possibilità di spostare cluster tra le zone di disponibilità</a>	È ora possibile spostare i cluster RA3 tra le zone di disponibilità.	9 dicembre 2020
<a href="#">Supporto per tipi di nodi ra3.xlplus</a>	È ora possibile creare tipi di nodi ra3.xlplus.	9 dicembre 2020

<a href="#">Supporto per driver JDBC versione 2.0</a>	È ora possibile configurare il driver JDBC versione 2.0.	5 novembre 2020
<a href="#">Supporto per funzioni Lambda definite dall'utente e tokenizzazione</a>	Ora è possibile scrivere funzioni Lambda definite dall'utente per abilitare la tokenizzazione esterna dei dati.	26 ottobre 2020
<a href="#">Supporto per pianificare l'esecuzione di un'istruzione SQL</a>	È ora possibile pianificare una query sulla console Amazon Redshift.	22 ottobre 2020
<a href="#">Supporto per l'API dati per Amazon Redshift</a>	È ora possibile accedere ad Amazon Redshift utilizzando l'API dati integrata. Gli aggiornamenti della documentazione includono una Documentazione di riferimento dell' API dati di Amazon Redshift.	10 settembre 2020
<a href="#">Supporto per il monitoraggio delle query della console Amazon Redshift</a>	La guida per descrivere i nuovi grafici di monitoraggio delle query è stata aggiornata.	7 maggio 2020
<a href="#">Supporto per limiti di utilizzo</a>	Aggiornata la guida per descrivere i limiti di utilizzo.	23 aprile 2020
<a href="#">Autenticazione a più fattori</a>	Aggiornata la guida per descrivere il supporto per l'autenticazione a più fattori (MFA).	20 aprile 2020
<a href="#">Il ridimensionamento elastico ora supporta le modifiche al tipo di nodo</a>	Aggiornamento della descrizione del ridimensionamento elastico.	6 aprile 2020

---

<a href="#">Supporto per tipi di nodi ra3.4xlarge con archiviazione gestita</a>	Aggiornata la guida per includere i tipi di nodi ra3.4xlarge.	2 aprile 2020
<a href="#">Supporto per sospensione e ripresa</a>	Aggiornata la guida per descrivere le operazioni di sospensione e ripresa del cluster.	11 marzo 2020
<a href="#">Supporto per Microsoft Azure AD come provider di identità</a>	Aggiornata la guida per descrivere i passaggi per utilizzare Microsoft Azure AD come provider di identità.	10 febbraio 2020
<a href="#">Supporto per il tipo di nodo RA3</a>	È stata aggiornata la guida per descrivere il nuovo tipo di nodo RA3.	3 dicembre 2019
<a href="#">Supporto per la nuova console</a>	Aggiornata la guida per descrivere la nuova console di Amazon Redshift.	11 novembre 2019
<a href="#">Aggiornamenti delle informazioni di sicurezza</a>	Aggiornamenti alla documentazione delle informazioni sulla sicurezza.	24 giugno 2019
<a href="#">Miglioramenti degli snapshot</a>	Amazon Redshift ora supporta diversi miglioramenti per la gestione e la pianificazione degli snapshot.	4 aprile 2019

---

<a href="#">Dimensionamento simultaneo</a>	È possibile configurare la gestione del carico di lavoro (WLM) per abilitare la modalità dimensionamento simultaneo. Per ulteriori informazioni, consultare <a href="#">Configurazione della gestione del carico di lavoro</a> .	21 marzo 2019
<a href="#">Driver JDBC e ODBC aggiornati</a>	Amazon Redshift ora supporta nuove versioni dei driver JDBC e ODBC. Per ulteriori informazioni, consultare <a href="#">Configurazione di una connessione JDBC</a> e <a href="#">Configurazione di una connessione ODBC</a> .	4 febbraio 2019
<a href="#">Posticipazione della manutenzione</a>	Se è necessario ripianificare la finestra di manutenzione del cluster, è possibile posticipare la manutenzione fino a un massimo di 14 giorni. Qualora sia necessario aggiornare l'hardware o effettuare altri aggiornamenti obbligatori durante il periodo di posticipazione, ti invieremo una notifica e apporteremo le modifiche necessarie. Durante questi aggiornamenti il cluster non è disponibile. Per ulteriori informazioni sullo stato della manutenzione, consultare <a href="#">Posticipazione della manutenzione</a> .	20 novembre 2018

## [Notifica preventiva](#)

Amazon Redshift fornisce notifiche preventive per alcuni eventi. Questi eventi hanno una categoria di evento `pending`. Ad esempio, inviamo una notifica preventiva se è necessario un aggiornamento dell'hardware per uno dei nodi nel cluster. È possibile effettuare la sottoscrizione agli eventi in sospeso come per gli altri eventi Amazon Redshift. Per ulteriori informazioni, consultare [Sottoscrizione alle notifiche di eventi di Amazon Redshift](#).

20 novembre 2018

## [Elastic resize \(Ridimensionamento elastico\)](#)

Il ridimensionamento elastico è il metodo più rapido per ridimensionare un cluster. Il ridimensionamento aggiunge o elimina i nodi su un cluster esistente, quindi ridistribuisce automaticamente i dati sui nuovi nodi. Poiché non crea un nuovo cluster, l'operazione di ridimensionamento elastico viene completata rapidamente, solitamente in pochi minuti. Per ulteriori informazioni, consultare [Cluster di ridimensionamento](#).

15 novembre 2018

---

<a href="#">Nuovi driver ODBC</a>	I driver ODBC di Amazon Redshift sono stati aggiornati alla versione 1.4.3.1000. Per ulteriori informazioni, consultare <a href="#">Configurazione di una connessione ODBC</a> .	8 novembre 2018
<a href="#">Annullamento dell'operazione di ridimensionamento</a>	È ora possibile annullare un'operazione di ridimensionamento mentre è in corso. Per ulteriori informazioni, consultare <a href="#">Panoramica dell'operazione di ridimensionamento</a> .	2 novembre 2018
<a href="#">Modifica del cluster per modificare la crittografia</a>	Puoi modificare un cluster non crittografato per utilizzare la crittografia AWS Key Management Service (AWS KMS), utilizzando una chiave gestita o una chiave AWS gestita dal cliente. Quando si modifica il cluster per abilitare la crittografia KMS, Amazon Redshift migra automaticamente i dati a un nuovo cluster crittografato. È anche possibile ripristinare un cluster non crittografato in un cluster crittografato modificando il cluster.	16 ottobre 2018

---

<a href="#">Amazon Redshift Spectrum supporta il routing VPC avanzato</a>	È ora possibile utilizzare Redshift Spectrum con il routing VPC avanzato abilitato per il cluster. Potrebbe essere necessario eseguire fasi di configurazioni aggiuntive. Per ulteriori informazioni, consultare e <a href="#">Utilizzo di Amazon Redshift Spectrum con il routing VPC avanzato</a> .	10 ottobre 2018
<a href="#">Editor della query</a>	È possibile ora eseguire query SQL dalla console di gestione di Amazon Redshift.	4 ottobre 2018
<a href="#">Grafico di suddivisione dell'esecuzione dei carichi di lavoro</a>	È ora possibile ottenere una visualizzazione dettagliata delle prestazioni del carico di lavoro osservando la tabella di suddivisione dell'esecuzione del carico di lavoro nella console. Per ulteriori informazioni, consultare <a href="#">Analisi delle prestazioni del carico di lavoro</a> .	30 luglio 2018
<a href="#">Tracce di manutenzione</a>	È ora possibile stabilire se il cluster dovrà essere sempre aggiornato alla versione più recente di Amazon Redshift o a una versione precedent e selezionando una traccia di manutenzione. Per ulteriori informazioni, consultare <a href="#">Selezione delle tracce di manutenzione del cluster</a> .	26 luglio 2018

Nella tabella seguente sono descritte le modifiche importanti apportate alla Guida alla gestione di Amazon Redshift prima di luglio 2018.

Modifica	Descrizione	Data di rilascio
Nuove metriche CloudWatch	Nuove CloudWatch metriche aggiunte per il monitoraggio delle prestazioni delle query. Per ulteriori informazioni, consultare <a href="#">Monitoraggio di Amazon Redshift tramite metriche CloudWatch</a>	17 maggio 2018
Crittografia HSM	Amazon Redshift supporta solo la gestione delle chiavi AWS CloudHSM dei moduli di sicurezza hardware (HSM). Per ulteriori informazioni, consultare <a href="#">Crittografia dei database di Amazon Redshift</a> .	6 marzo 2018
Concatenazione del ruolo IAM	Se un ruolo IAM collegato al cluster non ha accesso alle risorse necessarie, è possibile concatenare un altro ruolo, possibilmente appartenente a un altro account. Il cluster quindi può assumere temporaneamente il ruolo concatenato per accedere ai dati. Concatenando i ruoli è anche possibile concedere l'accesso a più account. Ogni ruolo nella catena assume il ruolo successivo nella catena, fino a quando il cluster non assume il ruolo alla fine della catena. È possibile concatenare un massimo di 10 ruoli. Per ulteriori informazioni, consultare <a href="#">Concatenazione di ruoli IAM in Amazon Redshift</a> .	23 febbraio 2018
Nuovi tipi di nodo DC2	I tipi di nodo di calcolo ad alta densità (DC) di nuova generazione offrono prestazioni migliori rispetto a DC1 ma allo stesso prezzo. Per sfruttare i vantaggi delle prestazioni avanzate, puoi eseguire la migrazione di un cluster DC1 ai nuovi tipi di nodo DC2. Per ulteriori informazioni, consultare <a href="#">Cluster e nodi in Amazon Redshift</a> .	17 ottobre 2017
Certificati ACM	Amazon Redshift sta sostituendo i certificati SSL sui tuoi cluster con certificati emessi da AWS Certificate	18 settembre 2017

Modifica	Descrizione	Data di rilascio
	<p>Manager (ACM). ACM è un'autorità di certificazione (CA) pubblica considerata attendibile dalla maggior parte dei sistemi correnti. Potrebbe essere necessario aggiornare i certificati CA radice attendibili correnti per continuare a connettersi ai propri cluster utilizzando SSL. Per ulteriori informazioni, consultare <a href="#">Passaggio ai certificati ACM per connessioni SSL</a>.</p>	
Ruoli collegati ai servizi	<p>Un ruolo collegato ai servizi è un tipo di ruolo IAM univoco collegato direttamente ad Amazon Redshift. I ruoli collegati ai servizi sono predefiniti da Amazon Redshift e includono tutte le autorizzazioni richieste dal servizio per chiamare i AWS servizi per conto del tuo cluster Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Utilizzo di ruoli collegati ai servizi per Amazon Redshift</a>.</p>	18 settembre 2017
Autenticazione utente del database IAM	<p>È possibile configurare il sistema in modo da consentire agli utenti di creare credenziali utente e di accedere al database con le proprie credenziali IAM. Puoi anche configurare il sistema per consentire agli utenti di accedere utilizzando il servizio Single Sign-On federato mediante un provider di identità conforme allo standard SAML 2.0. Per ulteriori informazioni, consultare <a href="#">Utilizzo dell'autenticazione IAM per generare credenziali utente di database</a>.</p>	11 agosto 2017
Il ripristino del livello tabella ora supporta il routing VPC avanzato	<p>Nei cluster che utilizzano <a href="#">Routing VPC avanzato</a> è ora supportato il ripristino del livello tabella. Per ulteriori informazioni, consultare <a href="#">Ripristino di una tabella da uno snapshot</a>.</p>	19 luglio 2017

Modifica	Descrizione	Data di rilascio
Regole di monitoraggio delle query	Grazie alle regole di monitoraggio delle query WLM, è possibile definire i limiti delle prestazioni basati sui parametri per le code WLM e specificare l'azione da intraprendere quando una query oltrepassa tali limiti, ovvero registrazione, hop o interruzione. Le regole di monitoraggio delle query vengono definite come parte della configurazione della gestione del carico di lavoro (WLM). Per ulteriori informazioni, consultare <a href="#">Configurazione della gestione del carico di lavoro</a> .	21 Aprile 2017
Routing VPC avanzato	Quando si utilizza il routing VPC avanzato di Amazon Redshift, Amazon Redshift forza il passaggio di tutto il traffico dei comandi <a href="#">COPY</a> e <a href="#">UNLOAD</a> tra il cluster e i repository di dati attraverso Amazon VPC. Per ulteriori informazioni, consultare <a href="#">Routing VPC avanzato in Amazon Redshift</a> .	15 settembre 2016
Nuovi campi del registro delle connessioni	Nel log di audit del <a href="#">Log delle connessioni</a> sono presenti due nuovi campi per tenere traccia delle connessioni SSL. Se si caricano regolarmente i log di audit in una tabella di Amazon Redshift, sarà necessario aggiungere alla tabella di destinazione le seguenti nuove colonne: sslcompression e sslexpansion.	5 maggio 2016
Nuovi driver ODBC	I driver ODBC di Amazon Redshift sono stati aggiornati alla versione 1.2.7.1007. Per ulteriori informazioni, consultare <a href="#">Configurazione di una connessione ODBC</a> .	30 marzo 2016

Modifica	Descrizione	Data di rilascio
Ruoli IAM per COPY e UNLOAD	Ora puoi specificare uno o più ruoli AWS Identity and Access Management (IAM) che il cluster può utilizzare per l'autenticazione per accedere ad altri servizi. AWS I ruoli IAM offrono un'alternativa di autenticazione più sicura per i comandi COPY, UNLOAD o CREATE LIBRARY. Per ulteriori informazioni, consultare <a href="#">Autorizzazione di Amazon Redshift ad accedere ad AWS altri servizi per tuo conto</a> e <a href="#">Autorizzazione di operazioni COPY, UNLOAD, CREATE EXTERNAL FUNCTION e CREATE EXTERNAL SCHEMA utilizzan do ruoli IAM</a> .	29 marzo 2016
Ripristino dalla tabella	È possibile ripristinare un cluster da uno snapshot cluster in una nuova tabella in un cluster attivo. Per ulteriori informazioni, consultare <a href="#">Ripristino di una tabella da uno snapshot</a> .	10 marzo 2016
Utilizzo della condizione IAM nelle policy	È possibile limitare ulteriormente l'accesso alle risorse utilizzando l'elemento Condizione nelle policy IAM. Per ulteriori informazioni, consultare <a href="#">Utilizzo di condizioni di policy IAM per il controllo granulare degli accessi</a> .	10 dicembre 2015
Modifica dell'accesso pubblico	È possibile modificare un cluster in un VPC per specificare se deve essere accessibile pubblicamente. Per ulteriori informazioni, consultare <a href="#">Modifica di un cluster</a> .	20 Novembre 2015
Correzioni della documentazione	Sono state pubblicate diverse correzioni della documentazione.	28 agosto 2015

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Sono state aggiornate le linee guida per la risoluzione dei problemi relativi alla configurazione delle impostazioni di rete per garantire che gli host con dimensioni dell'unità di trasmissione massima (MTU) diverse possano stabilire la dimensione di pacchetto per una connessione. Per ulteriori informazioni, consultare <a href="#">Query bloccate e talvolta impossibilitate a raggiungere il cluster.</a>	25 agosto 2015
Aggiornamento della documentazione	È stata rivista un'intera sezione sui gruppi di parametri per una migliore organizzazione e per maggiore chiarezza. Per ulteriori informazioni, consultare <a href="#">Gruppi di parametri di Amazon Redshift.</a>	17 agosto 2015
Proprietà dinamiche di WLM	Il parametro di configurazione WLM ora supporta l'applicazione dinamica di alcune proprietà. Le altre proprietà rimangono modifiche statiche e richiedono il riavvio dei cluster associati per l'applicazione delle modifiche di configurazione. Per ulteriori informazioni, consultare <a href="#">Proprietà WLM dinamiche e statiche</a> e <a href="#">Gruppi di parametri di Amazon Redshift.</a>	3 agosto 2015
Copia i cluster crittografati KMS in un'altra regione AWS	Sono stati aggiunti contenuti sulla configurazione delle concessioni di copia delle istantanee per consentire la copia di cluster crittografati in un'altra regione. AWS KMS AWS Per ulteriori informazioni, consultare e <a href="#">Copia di istantanee crittografate in un'altra regione AWS KMSAWS.</a>	28 luglio 2015

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	È stata aggiornata la sezione sulla crittografia del database per spiegare meglio come Amazon Redshift utilizza AWS KMS gli HSM per la gestione delle chiavi e come funziona il processo di crittografia con ciascuna di queste opzioni. Per ulteriori informazioni, consultare <a href="#">Crittografia dei database di Amazon Redshift</a> .	28 luglio 2015
Nuovo tipo di nodo	Amazon Redshift offre ora un nuovo tipo di nodo, DS2. Sono stati aggiornati i riferimenti della documentazione ai tipi di nodo esistenti per l'utilizzo dei nuovi nomi introdotti in questa versione. È stata aggiornata anche la sezione per spiegare in modo più accurato le combinazioni dei tipi di nodo e per chiarire i limiti di quota predefiniti. Per ulteriori informazioni, consultare <a href="#">Cluster e nodi in Amazon Redshift</a> .	9 giugno 2015
Offerte di nodi riservati	È stato aggiunto contenuto sulle nuove offerte di nodi riservati. È stata aggiornata anche la sezione per spiegare in modo più accurato e per confrontare le offerte disponibili con esempi che illustrano l'impatto dei prezzi dei nodi riservati e on demand sulla fatturazione. Per ulteriori informazioni, consultare <a href="#">Panoramica</a> .	9 giugno 2015
Nuovi driver ODBC	I driver ODBC di Amazon Redshift sono stati aggiornati. È stata aggiunta una sezione per le versioni precedenti di questi driver e un collegamento alle relative note di rilascio. Per ulteriori informazioni, consultare <a href="#">Configurazione di una connessione ODBC</a> .	5 giugno 2015
Correzioni della documentazione	Sono state pubblicate diverse correzioni della documentazione.	30 Aprile 2015

Modifica	Descrizione	Data di rilascio
Nuova caratteristica	In questa versione di Amazon Redshift vengono introdotti nuovi driver ODBC e JDBC ottimizzati per l'utilizzo con Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Connessione a un data warehouse Amazon Redshift tramite strumenti client SQL</a> .	26 febbraio 2015
Nuova caratteristica	In questa versione di Amazon Redshift sono introdotti i parametri delle prestazioni dei cluster che consentono di visualizzare e analizzare i dettagli di esecuzione e delle query. Per ulteriori informazioni, consultare <a href="#">Visualizzazione di query e caricamenti</a> .	26 febbraio 2015
Aggiornamento della documentazione	È stata aggiunta una nuova policy di esempio che dimostra la concessione di autorizzazioni per azioni e risorse AWS di servizio comuni su cui si basa Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Esempi di policy gestite dal cliente</a> .	16 gennaio 2015
Aggiornamento della documentazione	Sono state aggiornate le linee guida relative all'impostazione dell'unità di trasmissione massima (MTU) per disabilitare i frame jumbo TCP/IP. Per ulteriori informazioni, consultare <a href="#">Utilizzo di EC2-VPC durante la creazione del cluster</a> e <a href="#">Query bloccate e talvolta impossibilitate a raggiungere il cluster</a> .	16 gennaio 2015
Aggiornamento della documentazione	È stato rivisto il contenuto del <code>wlm_json_configuration</code> parametro e fornito un esempio di sintassi per configurare questo parametro utilizzando i AWS CLI sistemi operativi Linux, Mac OS X e Microsoft Windows. Per ulteriori informazioni, consultare <a href="#">Configurazione della gestione del carico di lavoro</a> .	13 gennaio 2015
Aggiornamento della documentazione	Sono state aggiunte notifiche e descrizioni di eventi mancanti. Per ulteriori informazioni, consultare <a href="#">Categorie di eventi Amazon Redshift e messaggi di evento</a> .	8 gennaio 2015

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Sono state aggiornate le linee guida relative alle policy IAM per le operazioni e le risorse di Amazon Redshift. È stata aggiornata la sezione per una migliore organizzazione e per maggiore chiarezza. Per ulteriori informazioni, consultare <a href="#">Sicurezza di Amazon Redshift</a> .	21 Novembre 2014
Nuova caratteristica	Questa versione di Amazon Redshift introduce la possibilità di crittografare i cluster utilizzando le chiavi di crittografia di (). AWS Key Management Service AWS KMS AWS KMS combina hardware e software sicuri e ad alta disponibilità per fornire un sistema di gestione delle chiavi scalabile per il cloud. Per ulteriori informazioni AWS KMS e opzioni di crittografia per Amazon Redshift, consulta <a href="#">Crittografia dei database di Amazon Redshift</a> e <a href="#">Gestione dei cluster con la console</a>	12 novembre 2014
Nuova caratteristica	In questa versione di Amazon Redshift è stata introdotta la possibilità di applicare tag a risorse come cluster e snapshot. I tag consentono di fornire metadati definiti dall'utente per suddividere in categorie i report di fatturazione in base all'allocazione dei costi e per identificare immediatamente le risorse. Per ulteriori informazioni, consultare <a href="#">Assegnazione di tag alle risorse in Amazon Redshift nella ..</a>	4 Novembre 2014
Nuova caratteristica	È stato elevato a 128 il limite massimo di nodi per le dimensioni di nodo dw1.8xlarge e dw2.8xlarge. Per ulteriori informazioni, consultare <a href="#">Cluster e nodi in Amazon Redshift</a> .	30 ottobre 2014

Modifica	Descrizione	Data di rilascio
Aggiornamento della documentazione	Sono stati aggiunti collegamenti ai Microsoft Visual C++ 2010 Redistributable Package necessari per consentire ad Amazon Redshift di utilizzare i driver ODBC PostgreSQL. Per ulteriori informazioni, consultare <a href="#">Installazione e configurazione del driver ODBC di Amazon Redshift su Microsoft Windows</a> .	30 ottobre 2014
Nuova caratteristica	È stata aggiunta la possibilità di terminare query e caricamenti dalla console Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Visualizzazione di query e caricamenti</a> e <a href="#">Visualizzazione dei parametri del cluster durante le operazioni di caricamento</a> .	28 Ottobre 2014
Correzioni della documentazione	Sono state pubblicate diverse correzioni della documentazione.	17 Ottobre 2014
Nuovo contenuto	È stato aggiunto contenuto sulla chiusura e sull'eliminazione dei cluster. Per ulteriori informazioni, consultare <a href="#">Chiusura ed eliminazione di cluster</a> e <a href="#">Eliminazione di un cluster</a> .	14 agosto 2014
Aggiornamento della documentazione	È stato chiarito il comportamento dell'impostazione Allow Version Upgrade (Consenti aggiornamento della versione) per i cluster. Per ulteriori informazioni, consultare <a href="#">Panoramica di Amazon Redshift</a> .	14 agosto 2014
Aggiornamento della documentazione	Sono stati aggiornati procedure, screenshot e organizzazione dell'argomento relativo all'uso dei cluster nella console Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Gestione dei cluster con la console</a> .	11 luglio 2014

Modifica	Descrizione	Data di rilascio
Nuovo contenuto	È stato aggiunto un nuovo tutorial sul ridimensionamento dei cluster Amazon Redshift, inclusa una descrizione di come modificare le dimensioni di un cluster riducendo al minimo la quantità di tempo in cui il cluster è in modalità di sola lettura. Per ulteriori informazioni, consultare <a href="#">Ridimensionamento di cluster</a> .	27 giugno 2014
Nuova caratteristica	È stata aggiunta la possibilità di rinominare i cluster. Per ulteriori informazioni, consultare <a href="#">Ridenominazione dei cluster</a> e <a href="#">Modifica di un cluster</a> .	2 giugno 2014
Aggiornamento della documentazione	È stato aggiornato l'esempio di codice .NET per utilizzare il provider di dati ODBC quando ci si connette a un cluster in modo programmatico utilizzando .NET. Per ulteriori informazioni, consultare <a href="#">Connect al tuo data warehouse in modo programmatico</a> .	15 maggio 2014
Nuova caratteristica	Sono state aggiunte opzioni per selezionare un gruppo di sicurezza e un gruppo di parametri diversi quando si ripristina un cluster da uno snapshot. Per ulteriori informazioni, consultare <a href="#">Ripristino di un cluster da uno snapshot</a> .	12 maggio 2014
Nuova caratteristica	È stata aggiunta una nuova sezione per descrivere come configurare un CloudWatch allarme Amazon predefinito per monitorare la percentuale di spazio su disco utilizzata in un cluster Amazon Redshift. Questo allarme costituisce una nuova opzione nel processo di creazione del cluster. Per ulteriori informazioni, consultare <a href="#">Allarme predefinito dello spazio su disco</a> .	28 aprile 2014
Aggiornamento della documentazione	Chiarite le informazioni sul supporto Diffie-Hellman Exchange a curva ellittica (ECDHE) in Amazon Redshift. Per ulteriori informazioni, consultare <a href="#">Connessione tramite SSL</a> .	22 aprile 2014

Modifica	Descrizione	Data di rilascio
Nuova caratteristica	Aggiunta una dichiarazione sul supporto di Amazon Redshift per il protocollo di accordo Diffie-Hellman a curva ellittica (ECDHE). Per ulteriori informazioni, consultare <a href="#">Connessione tramite SSL</a> .	18 aprile 2014
Aggiornamento della documentazione	Sono stati aggiornati e riorganizzati gli argomenti nella sezione <a href="#">Connessione a un data warehouse Amazon Redshift tramite strumenti client SQL</a> . Sono state aggiunte ulteriori informazioni sulle connessioni JDBC e ODBC e una nuova sezione di risoluzione dei problemi di connessione.	15 Aprile 2014
Aggiornamento della documentazione	È stata aggiunta la versione negli esempi di policy IAM in tutta la guida.	3 Aprile 2014
Aggiornamento della documentazione	Sono state aggiunte informazioni su come funziona l'assegnazione del prezzo quando si ridimensiona un cluster. Per ulteriori informazioni, consultare <a href="#">Acquisto di nodi riservati di Amazon Redshift</a> .	2 aprile 2014
Nuova caratteristica	È stata aggiunta una sezione su un nuovo parametro, <code>max_cursor_result_set_size</code> , che imposta la dimensione massima del set di risultati, in megabyte, che è possibile archiviare per singolo cursore. Questo valore di parametro influisce anche sul numero di cursori attivi contemporaneamente per il cluster. Per ulteriori informazioni, consultare <a href="#">Gruppi di parametri di Amazon Redshift</a> .	28 marzo 2014
Nuova caratteristica	È stata aggiunta una spiegazione sul campo Cluster Version (Versione cluster), che ora include sia la versione del motore del cluster che il numero di versione del database. Per ulteriori informazioni, consultare <a href="#">Cluster con provisioning di Amazon Redshift</a> .	21 marzo 2014

Modifica	Descrizione	Data di rilascio
Nuova caratteristica	È stata aggiornata la procedura di ridimensionamento per mostrare le nuove informazioni sullo stato di avanzamento del processo di ridimensionamento nella scheda Status (Stato) del cluster. Per ulteriori informazioni, consultare <a href="#">Ridimensionamento di un cluster</a> .	21 marzo 2014
Aggiornamento della documentazione	È stata riorganizzata e aggiornata la sezione <a href="#">Cos'è Amazon Redshift?</a> ed è stata aggiornata la sezione <a href="#">Panoramica sui cluster con provisioning di Amazon Redshift</a> . Sono state pubblicate diverse correzioni della documentazione.	21 febbraio 2014
Nuova caratteristica	Sono stati aggiunti nuovi tipi di nodo e nuove dimensioni per il cluster Amazon Redshift ed è stato riscritto in base al feedback l'argomento sulla panoramica dei cluster correlato per una migliore organizzazione e per maggiore chiarezza. Per ulteriori informazioni, consultare <a href="#">Cluster con provisioning di Amazon Redshift</a> .	23 gennaio 2014
Nuova caratteristica	Sono state aggiunte informazioni sull'utilizzo di indirizzi IP elastici (EIP) per i cluster Amazon Redshift accessibili pubblicamente nei cloud privato virtuale. Per ulteriori informazioni sugli EIP in Amazon Redshift, consultare <a href="#">Gestione dei cluster in un VPC</a> e <a href="#">Creazione di un cluster in un VPC</a> .	20 dicembre 2013
Nuova caratteristica	Sono state aggiunte informazioni sui AWS CloudTrail log per Amazon Redshift. Per ulteriori informazioni sul supporto di Amazon Redshift per CloudTrail, consulta <a href="#">Registrazione con CloudTrail</a>	13 dicembre 2013

Modifica	Descrizione	Data di rilascio
Nuova caratteristica	Sono state aggiunte informazioni sul nuovo log delle attività utente e sul parametro di database <code>enable_user_activity_logging</code> per la funzione di creazione di log di audit in Amazon Redshift. Per ulteriori informazioni sulla creazione di log di audit del database, vedi <a href="#">Logging di controllo dei database</a> . Per ulteriori informazioni sui parametri di database, vedi <a href="#">Gruppi di parametri di Amazon Redshift</a> .	6 dicembre 2013
Nuova caratteristica	Aggiornato per descrivere la configurazione di Amazon Redshift per copiare automaticamente istantanee automatiche e manuali in una regione secondaria. AWS Per ulteriori informazioni sulla configurazione della copia di uno snapshot tra regioni, consultare <a href="#">Copia di snapshot in un'altra regione AWS</a> .	14 Novembre 2013
Nuova caratteristica	È stata aggiunta una sezione per descrivere la creazione di log di verifica di Amazon Redshift per la connessione e l'attività utente e l'archiviazione di tali log in Amazon S3. Per ulteriori informazioni sulla creazione di log di audit del database, vedi <a href="#">Logging di controllo dei database</a> .	11 Novembre 2013
Nuova caratteristica	È stata aggiunta una sezione per descrivere la crittografia di Amazon Redshift con le nuove funzionalità per la gestione delle chiavi di crittografia in un modulo di sicurezza hardware (HSM) e per la rotazione delle chiavi di crittografia. Per ulteriori informazioni su crittografia, HSM e rotazione delle chiavi, vedi <a href="#">Crittografia dei database di Amazon Redshift</a> , <a href="#">Crittografia per Amazon Redshift tramite moduli di sicurezza hardware (HSM)</a> e <a href="#">Rotazione delle chiavi di crittografia in Amazon Redshift</a> .	11 Novembre 2013

Modifica	Descrizione	Data di rilascio
Nuova caratteristica	È stato eseguito un aggiornamento per descrivere e la pubblicazione di notifiche degli eventi Amazon Redshift tramite Amazon SNS. Per ulteriori informazioni sulle notifiche di eventi Amazon Redshift, consultare e <a href="#">Notifiche di eventi Amazon Redshift</a> .	11 Novembre 2013
Nuova caratteristica	È stato eseguito un aggiornamento per descrivere le autorizzazioni a livello di risorsa IAM. Per informazioni sulle autorizzazioni IAM di Amazon Redshift, consultare e <a href="#">Sicurezza di Amazon Redshift</a> .	9 agosto 2013
Nuova caratteristica	È stato eseguito un aggiornamento per descrivere e i parametri dello stato del ripristino. Per ulteriori informazioni, consultare <a href="#">Ripristino di un cluster da uno snapshot</a> .	9 agosto 2013
Nuova caratteristica	È stato eseguito un aggiornamento per descrivere la condivisione degli snapshot del cluster e i parametri dello stato di creazione degli snapshot. Per ulteriori informazioni, consultare <a href="#">Condivisione di snapshot</a> .	17 luglio 2013
Correzioni della documentazione	Sono state pubblicate diverse correzioni della documentazione.	8 luglio 2013
Schermate della nuova console	La Guida alla gestione di Amazon Redshift è stata aggiornata per riflettere le modifiche apportate nella console Amazon Redshift.	22 Aprile 2013
Nuova guida	Questa è la prima versione della Guida alla gestione di Amazon Redshift.	14 febbraio 2013

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.