
Amazon Redshift

Guía de administración de clústeres



Amazon Redshift: Guía de administración de clústeres

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas comerciales que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Amazon Redshift	1
¿Es la primera vez que usa Amazon Redshift?	1
Información general sobre la administración de Amazon Redshift	1
Administración de clústeres	2
Obtención de acceso a clústeres y seguridad	2
Monitoreo de clústeres	3
Databases	4
Clústeres	5
Descripción general de los clústeres de Amazon Redshift	5
Clústeres y nodos	5
Usar EC2-VPC al crear el clúster	9
EC2-VPC	10
EC2-Classic	10
Lance un clúster	10
Información general sobre los tipos de nodo RA3	10
Uso de almacenamiento gestionado por Amazon Redshift	11
Administración de tipos de nodo RA3	11
Disponibilidad del tipo de nodo RA3 enAWSRegiones	12
Actualización a tipos de nodo RA3	12
Actualización de tipos de nodo DC1 a tipos de nodo DC2	14
Actualización de un clúster DS2 en EC2-Classic a EC2-VPC	15
Consideraciones sobre regiones y zonas de disponibilidad	15
Mantenimiento de clústeres	16
Períodos de mantenimiento	16
Posponer el mantenimiento	17
Elección de pistas de mantenimiento del clúster	17
Administración de versiones del clúster	18
Reversión de la versión del clúster	19
Determinación de la versión de mantenimiento del clúster	20
Alarma predeterminada de espacio en disco	21
Estado del clúster	22
Información general sobre cómo administrar los clústeres	23
Cambio de tamaño de clústeres	23
Pausa y reanudación de clústeres	31
Cambio de nombre de los clústeres	32
Cierre y eliminación de clústeres	33
Trabajo con AQUA	33
Administrar mediante laAWS CLI	34
Administrar con las operaciones de la API de Amazon Redshift	34
¿Cuándo se usa AQUA?	35
Administración de los límites de uso	37
Administración de la reubicación del clúster	38
Habilitación de la reubicación	39
Limitations	39
Administración de la reubicación mediante la consola	39
Gestión de la reubicación mediante la CLI de Amazon Redshift	41
Trabajar con endpoints VPC administrados por RedShift	41
Consideraciones	42
Administración mediante la consola de Redshift	43
Administración de medianteAWS CLI	44
Administrar con las operaciones de la API de Amazon Redshift	44
Administración de clústeres a través de la consola	44
Creación de un clúster	47
Modificación de un clúster	59

Eliminación de un clúster	61
Reinicio de un clúster	63
Redimensionamiento de un clúster	64
Actualizar la versión de lanzamiento de un clúster	66
Obtención de información acerca de la configuración del clúster	67
Obtención de información general acerca del estado del clúster	67
Crear una instantánea de un clúster	69
Crear o editar una alarma de espacio en disco	70
Uso de los datos de rendimiento del clúster	71
Administración de clústeres a través de la AWS CLI API de Amazon Redshift	72
Administración de clústeres con la herramienta de AWS SDK for Java	72
Administración de clústeres en una VPC	75
Overview	75
Creación de un clúster en una VPC	77
Administración de grupos de seguridad de VPC para un clúster	79
Grupos de subredes del clúster	80
Historial de versiones del clúster	87
Consulta a una base de datos	88
Consulta de una base de datos mediante el editor de consultas	88
Consideraciones	89
Habilitar el acceso	89
Conexión con el editor de consultas	90
Conectar con el editor de consultas antiguo	91
Uso del editor de consultas	92
Programación de una consulta	95
Establecer los permisos para programar una consulta	96
Autenticación de una consulta programada	97
Conexión a un clúster mediante herramientas de cliente SQL	98
Configuración de conexiones en Amazon Redshift	99
Configuración de las opciones de seguridad para las conexiones	151
Conexión a clústeres desde herramientas y código cliente	157
Solución de problemas de conexión en Amazon Redshift	169
Uso de la API de datos	175
Uso de la API de datos	175
Autorización del acceso	175
Almacenamiento de credenciales en un secreto	177
Creación de un punto de enlace de la Amazon VPC	177
Consideraciones al llamar a la API de datos	179
Llamadas a la API de datos	181
Solución de problemas de la API de datos	196
Programación de operaciones de API de datos con Amazon EventBridge	197
Supervisión de la API de datos	198
Enhanced VPC Routing	202
Uso de los puntos de enlace de la VPC	203
Habilitación de Enhanced VPC Routing	203
Uso de Amazon Redshift Spectrum con Enhanced VPC Routing	206
Consideraciones para usar Enhanced VPC Routing para Redshift Spectrum	207
Grupos de parámetros	210
Overview	210
Acerca de los grupos de parámetros	210
Valores de parámetros predeterminados	211
Configuración de los valores de parámetros mediante la AWS CLI	212
Configuración de la administración de cargas de trabajo	213
Propiedades dinámicas y estáticas de WLM	213
Propiedades del parámetro wlm_json_configuration	213
Configuración del parámetro wlm_json_configuration mediante la AWS CLI	218
Administración de grupos de parámetros mediante la consola	223

Creación de un grupo de parámetros	224
Modificación de un grupo de parámetros	225
Creación o modificación de una regla de monitoreo de consultas mediante la consola	228
Eliminación de un grupo de parámetros	232
Asociación de un grupo de parámetros con un clúster	233
Administración de grupos de parámetros mediante la herramientaAWS SDK for Java	233
Administración de grupos de parámetros mediante laAWS CLI/API de Amazon Redshift	237
Instantáneas	238
Overview	238
Instantáneas automatizadas	239
Programación de instantáneas automatizadas	239
Formato de la programación de instantáneas	239
Instantáneas manuales	241
Administración del almacenamiento de instantáneas	241
Exclusión de tablas de instantáneas	242
Copia de instantáneas en otroAWSRegión	242
Restauración de un clúster desde una instantánea	243
Restauración de una tabla a partir de una instantánea	245
Uso compartido de instantáneas	248
Administración de instantáneas mediante la consola	250
Creación de una programación de instantáneas	250
Creación de una instantánea manual	252
Cambiar el periodo de retención de instantáneas manuales	254
Eliminación de instantáneas manuales	255
Copia de una instantánea automatizada	256
Restauración de un clúster desde una instantánea	258
Compartir una instantánea de un clúster	260
Configuración de la copia de una instantánea entre regiones para un clúster no cifrado	262
Configuración de la copia de una instantánea entre regiones para unAWS KMS—clúster cifrado ...	263
Modificación del período de retención para una copia de instantáneas entre regiones	264
Administración de instantáneas mediante la herramientaAWS SDK for Java	265
Administración de instantáneas mediante laAWS CLI/Amazon Redshift API y Amazon Redshift	268
Integración con unaAWSSocio	269
Integración con unaAWSAsociado que utiliza la consola de Amazon Redshift	269
Adquisición de nodos reservados de	271
Overview	271
Consideraciones sobre ofertas de nodos reservados	271
Comparación del precio entre ofertas de nodos reservados	272
Cómo funcionan los nodos reservados	273
Nodos reservados y facturación unificada	273
Ejemplos de nodos reservados	273
Adquisición de una oferta de nodo reservado con la consola de	275
Actualizar nodos reservados con AWS CLI	278
Adquisición de una oferta de nodo reservado mediante Java	279
Adquisición de una oferta de nodo reservado mediante laAWS CLIy la API de Amazon Redshift	282
Seguridad	283
Protección de los datos	284
Cifrado de datos	285
Tokenización de datos	303
Privacidad del tráfico entre redes	303
Administración de identidades y accesos	304
Authentication	304
Control de acceso	305
Información general sobre la administración del acceso	305
Usar políticas basadas en identidad (políticas de IAM)	311
Referencia de permisos de la API de Amazon Redshift	322
Uso de roles vinculados a servicios	322

Uso de la autenticación de IAM para generar credenciales de usuario de base de datos	324
Autorizar a Amazon Redshift para acceder aAWSservices	363
Registro y monitoreo	373
Registro de auditoría de bases de datos	373
Validación de la conformidad	388
Resiliencia	388
Seguridad de la infraestructura	389
Aislamiento de red	303
Grupos de seguridad	390
Conexión con un punto de conexión de la VPC de tipo interfaz	405
Configuración y análisis de vulnerabilidades	409
Uso de las interfaces de administración de Amazon Redshift	410
Mediante AWS SDK for Java	411
Ejecución de ejemplos de Java con Eclipse	411
Ejecución de ejemplos de Java desde la línea de comandos	412
Configuración del punto de enlace	412
Firma de una solicitud HTTP	413
Ejemplo de cálculo de firma	414
Configuración de la CLI de Amazon Redshift	415
Instrucciones de instalación	415
Introducción al AWS Command Line Interface	416
Monitoreo del rendimiento del clúster de	421
Overview	421
Datos de rendimiento	422
Métricas de Amazon Redshift	422
Dimensiones de métricas de Amazon Redshift	428
Datos de rendimiento de carga y consultas de Amazon Redshift	429
Uso de los datos de rendimiento	430
Visualización de datos de rendimiento del clúster	431
Visualización de datos del historial de consultas	438
Visualización de datos de rendimiento de la base de datos	441
Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo	445
Visualización de consultas y cargas	448
Visualización de métricas de clúster durante las operaciones de carga	460
Análisis del rendimiento de las cargas de trabajo	462
Creación de una alarma	466
Uso de métricas de rendimiento en la consola de CloudWatch	469
Eventos	471
Overview	471
Visualización de eventos mediante la consola	471
Visualización de eventos mediante el panelAWS SDK for Java	473
Visualización de eventos mediante laAWS CLI/API de Amazon Redshift	474
Notificaciones de eventos	475
Overview	475
Categorías y mensajes de eventos de Amazon Redshift	477
Administración de notificaciones de eventos mediante la consola de Amazon Redshift	488
Administración de notificaciones de eventos mediante laAWS CLI y la API de Amazon Redshift	493
Cuotas y límites	494
Cuotas de Amazon Redshift	494
Cuotas y límites de Amazon Redshift Spectrum	497
Restricciones en la nomenclatura:	498
Etiquetado	500
Información general del proceso de etiquetado	500
Requisitos de etiquetado	501
Administración de etiquetas de recursos mediante la consola	501
Administración de etiquetas mediante la API de Amazon Redshift	505
Historial de revisión	506

..... dxxii

¿Qué es Amazon Redshift

Le damos la bienvenida a la Amazon Redshift Guía de administración de clústeres. Amazon Redshift es un servicio de data warehouse administrado de varios petabytes en la nube. Puede comenzar con solo unos cientos de gigabytes de datos y, luego, ampliarlos a un petabyte o más. Esto le permite usar los datos para adquirir nuevos desarrollos para su empresa y sus clientes.

El primer paso para crear un data warehouse es el lanzamiento de un conjunto de nodos, llamado clúster de Amazon Redshift. Después de aprovisionar el clúster, puede cargar su conjunto de datos y, luego, realizar consultas de análisis de datos. Independientemente del tamaño del conjunto de datos, Amazon Redshift ofrece un rendimiento de consultas rápido mediante las mismas herramientas basadas en SQL y aplicaciones de inteligencia empresarial que usted usa en la actualidad.

¿Es la primera vez que usa Amazon Redshift?

Si es la primera vez que usa Amazon Redshift, le recomendamos que empiece leyendo las siguientes secciones:

- [Información general sobre la administración de Amazon Redshift \(p. 1\)](#): en este tema se ofrece información general sobre Amazon Redshift.
- [Aspectos destacados del servicio y precios](#): en esta página de detalles del producto, encontrará una propuesta de valor, aspectos destacados del servicio y los precios de Amazon Redshift
- [Introducción a Amazon Redshift](#): en esta guía se enseñan los procesos de creación de clústeres, creación de tablas de base de datos, carga de datos y prueba de consultas.
- [Amazon Redshift Guía de administración de clústeres](#) (esta guía): en esta guía se muestra la manera de crear y administrar clústeres de Amazon Redshift
- [Guía para desarrolladores de bases de datos Amazon Redshift](#): si es desarrollador de bases de datos, en esta guía se explica la manera de diseñar, desarrollar, hacer consultas y mantener las bases de datos que componen el almacenamiento de datos.

Existen varias maneras de administrar clústeres. Si prefiere administrar los clústeres de forma más interactiva, puede utilizar la consola de Amazon RedshiftAWS Command Line Interface(AWS CLI). Si es desarrollador de aplicaciones, puede usar la API de consulta de Amazon RedshiftAWSBibliotecas del kit de desarrollo de software (SDK) para administrar los clústeres mediante programación. Si utiliza la API de consulta de Amazon Redshift, debe autenticar todas las solicitudes HTTP o HTTPS enviadas a la API, firmándolas. Para obtener más información acerca de la firma de solicitudes, visite [Firma de una solicitud HTTP \(p. 413\)](#).

Para obtener más información acerca de la Command Line Interface (CLI, Interfaz de línea de comandos), la API y el Software Development Kit (SDK, Kit de desarrollo de software), visite los siguientes enlaces:

- [AWS CLI Referencia de los comandos de la](#)
- [Referencia de la API de Amazon Redshift](#)
- Referencias sobre los SDK de [Herramientas para Amazon Web Services](#).

Información general sobre la administración de Amazon Redshift

El servicio de Amazon Redshift administra todo el trabajo necesario para la configuración, el uso y el escalado de un data warehouse. Entre estas tareas se incluyen el aprovisionamiento de capacidad,

la monitorización y la realización de copias de seguridad del clúster, y la aplicación de parches y actualizaciones al motor de Amazon Redshift

Administración de clústeres

Un clúster de Amazon Redshift es un conjunto de nodos que incluye un nodo principal y uno o más nodos de computación. El tipo y la cantidad de nodos de computación que necesita depende del tamaño de los datos, la cantidad de consultas que ejecutará y el rendimiento de ejecución de consultas que necesite.

Creación y administración de clústeres

Según sus necesidades de data warehouse, puede comenzar con un clúster pequeño, de nodo único, y escalar con facilidad a un clúster más grande de nodos múltiples, a medida que cambien sus requisitos. Puede añadir o eliminar nodos de computación al clúster sin que se interrumpa el servicio. Para obtener más información, consulte [Clúster de Amazon Redshift \(p. 5\)](#).

Reserva de nodos de computación

Si desea que el clúster se siga ejecutando durante un año o más, puede ahorrar dinero si reserva los nodos de computación por un período de uno o tres años. La reserva de nodos de computación le ofrece ahorros significativos en comparación con las tasas por hora que se pagan al aprovisionar nodos de computación bajo demanda. Para obtener más información, consulte [Compra de nodos reservados de Amazon Redshift \(p. 271\)](#).

Creación de instantáneas de un clúster

Las snapshots son backups de un momento determinado de un clúster. Hay dos tipos de instantáneas: automatizadas y manuales. Amazon Redshift almacena estas instantáneas internamente en Amazon Simple Storage Service (Amazon S3) mediante una conexión de Capa de sockets seguros (SSL). Si necesita restaurar datos a partir de una instantánea, Amazon Redshift crea un nuevo clúster e importa los datos de la instantánea que usted especifique. Para obtener más información acerca de las instantáneas, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

Obtención de acceso a clústeres y seguridad

Hay distintas características relacionadas con la obtención de acceso a los clústeres y a la seguridad en Amazon Redshift. Estas características lo ayudan a controlar la obtención de acceso a su clúster, definir reglas de conectividad y cifrar datos y conexiones. Estas características se suman a las relacionadas con la obtención de acceso a la base de datos y a la seguridad en Amazon Redshift. Para obtener más información acerca de la seguridad de la base de datos, consulte [Administración de la seguridad de bases de datos](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

AWSCuentas y Credenciales de IAM

De forma predeterminada, solo los clústeres de Amazon Redshift que crea el clúster de. El clúster se encuentra bloqueado de manera tal que nadie más obtenga acceso. En su AWS, utilice la AWS Identity and Access Management (IAM) para crear cuentas de usuario y administrar los permisos de esas cuentas para controlar las operaciones del clúster de. Para obtener más información, consulte [Seguridad en Amazon Redshift \(p. 283\)](#).

Grupos de seguridad

De forma predeterminada, cualquier clúster que cree está cerrado para todos. Las credenciales de IAM solo controlan el acceso a los recursos relacionados con la API de Amazon Redshift: la consola de

Amazon Redshift, la interfaz de línea de comandos (CLI), la API y el SDK. Para habilitar el acceso al clúster desde herramientas de cliente SQL mediante JDBC u ODBC, se usan grupos de seguridad:

- Si utiliza la plataforma EC2-VPC en su clúster de Amazon Redshift, debe usar grupos de seguridad de VPC. Le recomendamos que lance el clúster en una plataforma EC2-VPC.

No se puede mover un clúster a una VPC después de haberse lanzado con EC2-Classic. Sin embargo, puede restaurar una instantánea EC2-Classic en un clúster EC2-VPC con la consola de Amazon Redshift. Para obtener más información, consulte [Restauración de un clúster desde una instantánea](#) (p. 258).

- Si utiliza la plataforma EC2-Classic en su clúster de Amazon Redshift, debe usar grupos de seguridad de Amazon Redshift.

En cualquiera de los casos, se añaden reglas al grupo de seguridad para otorgar acceso de entrada explícito a un rango específico de direcciones IP/CIDR o a un grupo de seguridad de Amazon Elastic Compute Cloud (Amazon EC2), si el cliente SQL se ejecuta en una instancia de Amazon EC2. Para obtener más información, consulte [Grupos de seguridad de clúster de Amazon Redshift](#) (p. 390).

Además de las reglas de acceso de entrada, crea usuarios de base de datos para brindar credenciales que se autentique para la base de datos dentro del mismo clúster. Para obtener más información, consulte [Databases](#) (p. 4) en este tema.

Encryption

Al aprovisionar el clúster, tiene la opción de cifrarlo para obtener seguridad adicional. Cuando habilita el cifrado de, Amazon Redshift almacena todos los datos en tablas creadas por el usuario en un formato cifrado. Puede usar AWS Key Management Service (AWS KMS) para administrar claves de cifrado de Amazon Redshift.

El cifrado es una propiedad inmutable del clúster. La única forma de cambiar de un clúster cifrado a uno no cifrado es descargar los datos y volverlos a cargar en un clúster nuevo. El cifrado se aplica al clúster y a todos los backups. Cuando los datos se restauran desde una snapshot cifrada, el nuevo clúster también se cifra.

Para obtener más información acerca del cifrado, las claves y los módulos de seguridad de hardware, consulte [Cifrado de base de datos de Amazon](#) (p. 286).

Conexiones SSL

Puede usar un Secure Sockets Layer (SSL, Cifrado de capa de conexión segura) para cifrar la conexión entre el cliente SQL y el clúster. Para obtener más información, consulte [Configuración de las opciones de seguridad para las conexiones](#) (p. 151).

Monitoreo de clústeres

Hay distintas características relacionadas con la monitorización en Amazon Redshift. Puede utilizar el registro de auditoría de bases de datos para generar registros de actividad, configurar eventos y suscripciones a notificaciones para realizar un seguimiento de información de interés. Utilice las métricas de Amazon Redshift y Amazon CloudWatch para obtener más información acerca del estado y el rendimiento de sus clústeres y bases de datos.

Registro de auditoría de bases de datos

Puede usar la característica de registro de auditoría de bases de datos para realizar un seguimiento de información relacionada con los intentos de autenticación, las conexiones, las desconexiones, los cambios en las definiciones de usuario de la base de datos y las consultas ejecutadas en esta última. Esta

información es útil en términos de seguridad y solución de problemas en Amazon Redshift. Los logs se almacenan en buckets de Amazon S3. Para obtener más información, consulte [Registro de auditoría de bases de datos](#) (p. 373).

Eventos y notificaciones

Amazon Redshift realiza un seguimiento de eventos y retiene información relacionada con ellos durante varias semanas en su AWS account. brinda información como la fecha Amazon Redshift la que se produjo cada evento, una descripción de él, su origen (por ejemplo, un clúster, un grupo de parámetros o una snapshot) y el ID de origen. Puede crear suscripciones a notificaciones de eventos de Amazon Redshift que especifican un conjunto de filtros de eventos. Cuando un evento coincide con los criterios de filtro, Amazon Redshift usa Amazon Simple Notification Service para informarle activamente de que se ha producido el evento. Para obtener más información acerca de eventos y notificaciones, consulte [Eventos de Amazon Redshift](#) (p. 471).

Performance

Amazon Redshift ofrece métricas y datos de rendimiento para que pueda registrar la salud y el rendimiento de sus clústeres y bases de datos. Amazon Redshift utiliza métricas de Amazon CloudWatch para monitorear los aspectos físicos del clúster, como la utilización de la CPU, la latencia y el rendimiento. Amazon Redshift también proporciona datos de rendimiento de consulta y carga para ayudarle a supervisar la actividad de la base de datos en el clúster. Para obtener más información acerca de las métricas y la monitorización del rendimiento, consulte [Supervisión del rendimiento del clúster de Amazon Redshift](#) (p. 421).

Databases

Cuando aprovisiona un clúster, Amazon Redshift crea una base de datos. Esta es la base de datos que utiliza para cargar datos y ejecutar consultas en sus datos. Puede crear bases de datos adicionales según necesidad mediante la ejecución de un comando SQL. Para obtener más información acerca de la creación de bases de datos adicionales, consulte [Paso 1: Creación de una base de datos](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Al aprovisionar un clúster, especifica un usuario maestro que tiene acceso a todas las bases de datos creadas dentro del clúster. Ese usuario maestro es un super usuario, el único con acceso inicial a la base de datos, aunque él mismo puede crear usuarios y super usuarios adicionales. Para obtener más información, consulte [Super usuarios y Usuarios de](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Amazon Redshift utiliza grupos de parámetros para definir el comportamiento de todas las bases de datos de un clúster, como estilo de presentación de fecha y precisión de punto flotante. Si no especifica un grupo de parámetros al crear aprovisionar el clúster, Amazon Redshift le asocia un grupo de parámetros predeterminado. Para obtener más información, consulte [Grupos de parámetros de Amazon Redshift](#) (p. 210).

Para obtener más información acerca de las bases de datos de Amazon Redshift, consulte la [Guía para desarrolladores de bases de datos Amazon Redshift](#).

Clúster de Amazon Redshift

En las siguientes secciones, puede obtener información sobre los aspectos básicos para crear un data warehouse mediante el lanzamiento de un conjunto de nodos de computación, llamado Amazon Redshiftclúster.

Temas

- [Descripción general de los clústeres de Amazon Redshift \(p. 5\)](#)
- [Usar EC2-VPC al crear el clúster \(p. 9\)](#)
- [Información general sobre los tipos de nodo RA3 \(p. 10\)](#)
- [Actualización a tipos de nodo RA3 \(p. 12\)](#)
- [Actualización de tipos de nodo DC1 a tipos de nodo DC2 \(p. 14\)](#)
- [Actualización de un clúster DS2 en EC2-Classic a EC2-VPC \(p. 15\)](#)
- [Consideraciones sobre regiones y zonas de disponibilidad \(p. 15\)](#)
- [Mantenimiento de clústeres \(p. 16\)](#)
- [Alarma predeterminada de espacio en disco \(p. 21\)](#)
- [Estado del clúster \(p. 22\)](#)
- [Información general sobre cómo administrar los clústeres de Amazon Redshift \(p. 23\)](#)
- [Trabajo con AQUA \(Advanced Query Accelerator\) \(p. 33\)](#)
- [Administración de los límites de uso en Amazon Redshift \(p. 37\)](#)
- [Gestión de la reubicación de clústeres en Amazon Redshift \(p. 38\)](#)
- [Trabajar con terminales de VPC gestionados por Redshift en Amazon Redshift \(p. 41\)](#)
- [Administración de clústeres a través de la consola \(p. 44\)](#)
- [Administración de clústeres a través de laAWS CLI/API de Amazon Redshift \(p. 72\)](#)
- [Administración de clústeres con la herramienta deAWS SDK for Java \(p. 72\)](#)
- [Administración de clústeres en una VPC \(p. 75\)](#)
- [Historial de versiones del clúster \(p. 87\)](#)

Descripción general de los clústeres de Amazon Redshift

Un almacén de datos de Amazon Redshift es una colección de recursos de computación denominadosNodos, que se organizan en un grupo llamadoclúster. Cada clúster ejecuta un motor de Amazon Redshift y contiene una o más bases de datos.

Note

En este momento, está disponible la versión 1.0 del motor de Amazon Redshift. Sin embargo, como el motor está actualizado, es posible que haya varias versiones de motores de Amazon Redshift disponibles para su selección.

Clusters y nodos en Amazon Redshift

Un clúster de Amazon Redshift está formado por nodos. Cada clúster tiene un nodo principal y uno o más nodos de computación. El nodo principal recibe consultas de las aplicaciones cliente, las analiza y desarrolla planes de ejecución de las consultas. Luego, el nodo principal coordina una ejecución en paralelo de esos planes con los nodos de computación y añade los resultados intermedios de dichos nodos. Finalmente, devuelve los resultados a las aplicaciones cliente.

Los nodos de computación procesan los planes de ejecución de consultas y transmiten datos entre ellos para atender a esas consultas. Los resultados intermedios envían al nodo principal para agregación antes de que vuelvan a las aplicaciones cliente. Para obtener más información acerca de los nodos principales y los nodos de computación, consulte [Arquitectura del sistema de almacenamiento de datos](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Note

Al crear un clúster en la consola de Amazon Redshift (<https://console.aws.amazon.com/redshift/>), puede obtener una recomendación de la configuración de su clúster en función del tamaño de sus datos y las características de consulta de. Para utilizar esta calculadora de tallas, busque [Ayúdeme a elegir](#) en la consola de AWS Regiones que admiten tipos de nodo RA3. Para obtener más información, consulte [Creación de un clúster](#) (p. 47) .

Al lanzar un clúster, una de las opciones que debe especificar es el tipo de nodo. El tipo de nodo determina la capacidad de la CPU, la RAM, el almacenamiento y el tipo de unidad de almacenamiento de cada nodo.

Amazon Redshift ofrece diferentes tipos de nodos para acomodar sus cargas de trabajo y recomendamos elegir RA3 o DC2 en función del rendimiento necesario, el tamaño de los datos y el crecimiento previsto de los datos.

Los nodos RA3 con almacenamiento administrado le permiten optimizar su almacenamiento de datos mediante el escalado y pago de las capacidades de cómputo y almacenamiento administrado de forma independiente. Con RA3, elige la cantidad de nodos que necesita en función de requisitos de rendimiento y solo paga por el almacenamiento administrado que utilice. Dimensione su clúster de RA3 en función de la cantidad de datos que procesa diariamente. Puede lanzar clústeres que usen los tipos de nodos RA3 en una nube virtual privada (VPC). No puede lanzar clústeres RA3 en EC2-Classik. Para obtener más información, consulte [Creación de un clúster en una VPC](#) (p. 77) .

El almacenamiento administrado de Amazon Redshift utiliza amplias unidades de estado sólido de alto rendimiento en cada nodo RA3 para lograr un almacenamiento local ágil y Amazon S3 para lograr un almacenamiento duradero a largo plazo. Si los datos de un nodo aumentan y exceden el tamaño de las amplias unidades de estado sólido locales, el almacenamiento administrado de Amazon Redshift descarga dichos datos a Amazon S3. Paga la misma tarifa reducida para el almacenamiento administrado de Amazon Redshift, con independencia de si los datos residen en unidades de estado sólido de alto rendimiento o en Amazon S3. Para las cargas de trabajo que requieren un almacenamiento cada vez mayor, el almacenamiento administrado permite escalar automáticamente la capacidad de almacenamiento del almacenamiento de datos sin agregar ni pagar nodos adicionales.

Los nodos DC2 permiten tener almacenamientos de datos con uso intensivo de cómputo con almacenamiento SSD local incluido. Debe elegir la cantidad de nodos que necesita en función del tamaño de los datos y los requisitos de rendimiento. Los nodos DC2 almacenan sus datos localmente para obtener un alto rendimiento y, a medida que el tamaño de los datos aumenta, puede agregar más nodos informáticos a fin de incrementar la capacidad de almacenamiento del clúster. Para conjuntos de datos de menos de 1 TB (sin comprimir), recomendamos los tipos de nodos DC2 para lograr el mejor rendimiento al menor precio. Si espera que sus datos crezcan, recomendamos usar nodos RA3 para que pueda dimensionar el cómputo y el almacenamiento de forma independiente para lograr el mejor precio y rendimiento. Puede lanzar clústeres que usen los tipos de nodos DC2 en una nube virtual privada (VPC). No puede lanzar clústeres DC2 en modo EC2-Classik. Para obtener más información, consulte [Creación de un clúster en una VPC](#) (p. 77) .

Los nodos DS2 le permiten crear grandes almacenamientos de datos con unidades de disco duro (HDD), pero recomendamos usar nodos RA3. Si utiliza nodos DS2, consulte [Actualización a tipos de nodo RA3](#) (p. 12) para obtener instrucciones de actualización. Si utiliza ocho o más nodos de ds2.xlarge o cualquier cantidad de nodos ds2.8xlarge, pueden actualizar a RA3 y obtener el doble de almacenamiento y un mejor rendimiento por el mismo costo bajo demanda.

Hay disponibles tipos de nodos de diferentes tamaños. El tamaño y la cantidad de nodos determinan el almacenamiento total de un clúster. Para obtener más información, consulte [Detalles acerca de los tipos de nodos](#) (p. 7) .

Algunos tipos de nodos admiten un único nodo (nodo único) o dos o más nodos (nodo múltiple). El número mínimo de nodos para clústeres de algunos tipos de nodos es de dos nodos. En un clúster de nodo único, se comparte ese nodo para la funcionalidad principal y para la de computación. No se recomiendan clústeres de nodo único para ejecutar cargas de trabajo de producción. En un clúster de nodos múltiples, el nodo principal es independiente de los nodos de computación. El nodo principal es del mismo tipo de nodo que los nodos de computación. Solo paga por nodos de computación.

Amazon Redshift aplica cuotas a los recursos de cada AWS en cada AWS Región. Actualmente limita la cantidad de recursos que una cuenta puede crear para un tipo de recurso determinado, como los nodos o las instantáneas, dentro de una AWS Región. Para obtener más información acerca de las cuotas predeterminadas que se aplican a los recursos de Amazon Redshift, visite [Límites de Amazon Redshift](#) en la Referencia general de Amazon Web Services. Para solicitar un aumento, envíe un [Formulario de aumento de límite de Amazon Redshift](#).

El costo de su clúster depende de la AWS Región, tipo de nodo, número de nodos y si los nodos están reservados de manera anticipada. Para obtener más información sobre el costo de los nodos, consulte [Precios de Amazon Redshift](#) (Se ha creado el certificado).

Detalles acerca de los tipos de nodos

En las siguientes tablas, se resumen las especificaciones de cada tipo y tamaño de nodo. Los títulos de las tablas tienen estos significados:

- vCPU es la cantidad de CPU virtuales de cada nodo.
- RAM es la cantidad de memoria en gibibytes (GiB) de cada nodo.
- Sectores predeterminados por nodo es el número predeterminado de sectores en los que se particiona un nodo de computación cuando se crea un clúster o se cambia el tamaño con el cambio de tamaño clásico.

El número de sectores por nodo podría cambiar si se cambia el tamaño del clúster mediante el cambio de tamaño elástico. Sin embargo, el número total de sectores en todos los nodos de computación del clúster sigue siendo el mismo después del cambio de tamaño elástico.

Al crear un clúster con la operación de restauración desde instantánea, el número de sectores del clúster resultante podría cambiar respecto al clúster original si cambia el tipo de nodo.

- Almacenamiento es la capacidad y el tipo almacenamiento de cada nodo.
- Rango de nodos es el número mínimo y máximo de nodos que admite Amazon Redshift para el tipo y tamaño de nodo de.

Note

Puede tener restricciones para utilizar menos nodos según la cuota que se aplica a su cuenta de AWS en la región de AWS seleccionada. Para solicitar un aumento, envíe un [Formulario de aumento de límite de Amazon Redshift](#).

- Capacidad total es la capacidad total de almacenamiento del clúster si implementa el número máximo de nodos especificado en el rango de nodos.

Tipos de nodo RA3

Tamaño del nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Cuota de almacenamiento administrado por nodo	Rango de nodos con Crear clúster	Capacidad total de almacenamiento administrado	
ra3.xlplus	4	32	2	32 TB ¹	2—16 ²	1024 TB ^{2,4}	
ra3.4xlarge	12	96	4	128 TB ¹	2—32 ³	8192 TB ^{3,4}	

Tamaño del nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Cuota de almacenamiento administrado por nodo	Rango de nodos con Crear clúster	Capacidad total de almacenamiento administrado	
ra3.16xlarge	48	384	16	128 TB ¹	2—128	16.384 TB ⁴	

¹Cuota de almacenamiento para el almacenamiento gestionado de Amazon Redshift.

²Puede crear un clúster con el tipo de nodo ra3.xlplus que tenga hasta 16 nodos. Puede cambiar su tamaño con el ajuste elástico a un máximo de 32 nodos.

³Puede crear clúster con el tipo de nodo ra3.4xlarge o ra3.16xlarge con hasta 16 nodos. Puede cambiar su tamaño con un cambio de tamaño elástico a un máximo de 64 nodos.

⁴La cuota total de almacenamiento administrado es el número máximo de nodos por la cuota de almacenamiento administrado por nodo.

Tipos de nodos de almacenamiento de alta densidad

Tamaño del nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Almacenamiento por nodo	Rango de nodos	Capacidad total	
ds2.xlarge	4	31	2	HDD de 2 TB	1—32	64 TB	
ds2.8xlarge	36	244	16	HDD de 16 TB	2—128	2 PB	

Tipos de nodos de computación de alta densidad

Tamaño del nodo	vCPU	RAM (GiB)	Sectores predeterminados por nodo	Almacenamiento por nodo	Rango de nodos	Capacidad total	
dc2.large	2	15	2	SSD NVMe de 160 GB	1—32	5.12 TB	
dc2.8xlarge	32	244	16	SSD NVMe de 2,56 TB	2—128	326 TB	
dc1.large ¹	2	15	2	SSD de 160 GB	1—32	5.12 TB	
dc1.8xlarge ¹	32	244	32	SSD de 2,56 TB	2—128	326 TB	

¹ Recomendamos los tipos de nodos DC2 frente a los tipos de nodos DC1. Para obtener más información sobre cómo actualizar, consulte [Actualización de tipos de nodo DC1 a tipos de nodo DC2 \(p. 14\)](#).

Nombres anteriores de los tipos de nodos

En versiones anteriores de Amazon Redshift, determinados tipos de nodos tenían nombres diferentes. Puede utilizar los nombres anteriores en la API de Amazon Redshift y en AWS CLI. Sin embargo,

recomendamos que actualice cualquier script que haga referencia a esos nombres para usar los nombres actuales en su lugar. A continuación, se detallan los nombres actuales y anteriores.

Nombre actual	Nombres anteriores
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

Determinar cuál es la cantidad de nodos

Como Amazon Redshift distribuye y ejecuta consultas en paralelo en todos los nodos de computación de un clúster, puede aumentar el rendimiento de consultas añadiendo nodos a su clúster. Cuando ejecuta un clúster con al menos dos nodos de computación, los datos de cada nodo se reflejan en discos de otro nodo para reducir el riesgo de pérdida de datos.

Puede monitorear el rendimiento de las consultas en la consola de Amazon Redshift y con métricas de Amazon CloudWatch. También puede agregar o eliminar nodos según sea necesario para lograr el equilibrio entre precio y rendimiento de su clúster. Cuando solicita un nodo adicional, Amazon Redshift se encarga de todos los detalles de implementación, equilibrio de cargas y mantenimiento de datos. Para obtener más información acerca del rendimiento de un clúster, consulte [Supervisión del rendimiento del clúster de Amazon Redshift \(p. 421\)](#).

Los nodos reservados son adecuados para cargas de trabajo de producción de estado estable y aportan descuentos significativos en comparación con los precios bajo demanda. Puede comprar nodos reservados después de ejecutar experimentos y pruebas de conceptos para validar la configuración de producción. Para obtener más información, consulte [Compra de nodos reservados de Amazon Redshift \(p. 271\)](#).

Cuando se pausa un clúster, suspende la facturación bajo demanda durante el tiempo en que se detiene el clúster. Durante este tiempo de pausa, solo paga por el almacenamiento de copia de seguridad. De este modo, puede olvidarse de planificar y adquirir capacidad para el almacenamiento de datos antes de necesitarla, lo que le permite administrar de manera rentable entornos de desarrollo o pruebas.

Para obtener información acerca de los precios de los nodos bajo demanda y reservados, consulte [Precios de Amazon Redshift](#).

Usar EC2-VPC al crear el clúster

Los clústeres de Amazon Redshift se ejecutan en instancias de Amazon EC2 que están configuradas para el tipo y tamaño de nodo de Amazon Redshift que haya seleccionado. Cree su clúster con EC2-VPC. Si sigue utilizando EC2-Classic, le recomendamos que use EC2-VPC para mejorar el rendimiento y la seguridad. Para obtener más información acerca de estas plataformas de redes, consulte [Plataformas admitidas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux. SusAWSLa configuración de la cuenta determina si EC2-VPC o EC2-Classic están disponibles para usted.

Note

Para evitar problemas de conexión entre las herramientas cliente de SQL y la base de datos de Amazon Redshift, le recomendamos que realice alguna de estas dos operaciones. Puede configurar una regla de entrada que permita a los hosts negociar el tamaño del paquete. También puede deshabilitar las tramas gigantes de TCP/IP estableciendo la unidad máxima de transmisión

(MTU) en 1500 en la interfaz de red (NIC) de sus instancias de Amazon EC2. Para obtener más información acerca de estos métodos, consulte [Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster \(p. 173\)](#).

EC2-VPC

Cuando utiliza EC2-VPC, su clúster se ejecuta en una Virtual Private Cloud (VPC), que está aislada lógicamente de su AWS account. Si aprovisiona su clúster en EC2-VPC, controla el acceso a su clúster asociando uno o más grupos de seguridad de la VPC con el clúster. Para obtener más información, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Para crear un clúster en una VPC, primero debe crear un grupo de subred de clúster de Amazon Redshift proporcionando información de subred a su VPC; luego, al lanzar el clúster, debe proporcionar el grupo de subred. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#).

Para obtener más información acerca de Amazon Virtual Private Cloud (Amazon VPC), consulte la [Página de detalles del producto de Amazon VPC](#).

EC2-Classic

En EC2-Classic, el clúster se ejecuta en una sola red plana que comparte con otros AWS clientes. Si aprovisiona su clúster en EC2-Classic, controla el acceso a su clúster asociando uno o más grupos de seguridad de clúster de Amazon Redshift con el clúster. Para obtener más información, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#).

Lance un clúster

Su AWS puede lanzar instancias de EC2-VPC y EC2-Classic, o solo EC2-VPC, región por región. Para determinar qué plataforma de red admite su cuenta y, a continuación, lanzar un clúster, haga lo siguiente:

1. Decida en qué región de AWS desea implementar un clúster. Para obtener una lista de AWS en las regiones en las que está disponible Amazon Redshift, consulte [Puntos de enlace de Amazon Redshift](#) en la Referencia general de Amazon Web Services.
2. Averigüe qué plataformas de Amazon EC2 admite su cuenta en la AWS Región. Puede encontrar esta información en la consola de Amazon EC2. Para obtener instrucciones paso a paso, consulte [Plataformas admitidas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.
3. Si su cuenta es compatible con ambas plataformas, le recomendamos EC2-VPC. Si su cuenta solo es compatible con EC2-VPC, debe implementar su clúster en la VPC.
4. Inicie su clúster de Amazon Redshift. Puede crear un clúster mediante la consola de Amazon Redshift o mediante la API de Amazon Redshift, AWS CLI, o bibliotecas SDK. Para obtener más información acerca de estas opciones y enlaces a documentación relacionada, consulte [¿Qué es Amazon Redshift \(p. 1\)](#).

Información general sobre los tipos de nodo RA3

Se recomienda actualizar las cargas de trabajo existentes que se ejecutan en clústeres de tipo de nodo DS2 a tipos de nodo RA3 para aprovechar el rendimiento mejorado y obtener más capacidad de almacenamiento. Los nodos RA3 proporcionan las siguientes ventajas:

- Son flexibles para aumentar su capacidad de cómputo sin aumentar sus costos de almacenamiento. Además, escalan su almacenamiento sin aprovisionar en exceso la capacidad de cómputo.
- Utilizan SSD de alto rendimiento para los datos calientes y Amazon S3 para datos fríos. Por lo tanto, proporcionan facilidad de uso, almacenamiento rentable y alto rendimiento de consultas.

- Utilizan redes de alto ancho de banda construidas en AWS para reducir aún más el tiempo necesario para la descarga y recuperación de los datos de Amazon S3.

Considere la posibilidad de seleccionar tipos de nodo RA3 en estos casos:

- Si necesita flexibilidad para escalar y pagar el cálculo por separado del almacenamiento.
- Consulta una fracción de los datos totales.
- El volumen de datos está creciendo rápidamente o se espera que crezca rápidamente.
- Desea flexibilidad para ajustar el tamaño del clúster en función únicamente de las necesidades de rendimiento.

Para utilizar tipos de nodo RA3, su región de AWS debe admitir RA3. Para obtener más información, consulte [Disponibilidad del tipo de nodo RA3 en AWS Regiones](#) (p. 12) .

Important

Los tipos de nodo ra3.xplus solo se pueden utilizar con la versión del clúster 1.0.21262 o posterior. Puede ver la versión de un clúster existente con la consola de Amazon Redshift. Para obtener más información, consulte [Determinación de la versión de mantenimiento del clúster](#) (p. 20) .

Asegúrese de utilizar la nueva consola de Amazon Redshift cuando trabaje con tipos de nodo RA3. La consola original no soporta todas las operaciones RA3.

Además, para utilizar tipos de nodos RA3 con operaciones de Amazon Redshift que utilizan la pista de mantenimiento, el valor de la pista de mantenimiento debe establecer en una versión de clúster que admita RA3. Para obtener más información sobre las pistas de mantenimiento, consulte [Elección de pistas de mantenimiento del clúster](#) (p. 17).

Uso de almacenamiento gestionado por Amazon Redshift

Con el almacenamiento administrado de Amazon Redshift, puede almacenar y procesar todos sus datos en Amazon Redshift mientras obtiene más flexibilidad para escalar la capacidad de cálculo y de almacenamiento por separado. Siga adquiriendo datos con el comando COPY o INSERT. Para optimizar el rendimiento y administrar la colocación automática de datos en los niveles de almacenamiento, Amazon Redshift aprovecha las optimizaciones como la temperatura del bloque de datos, la antigüedad del bloque de datos y los patrones de cargas de trabajo. Cuando es necesario, Amazon Redshift escala el almacenamiento automáticamente a Amazon S3 sin necesidad de ninguna acción manual.

Para obtener información sobre los costos de almacenamiento, consulte [Precios de Amazon Redshift](#).

Administración de tipos de nodo RA3

Para aprovechar la separación del proceso de computación del almacenamiento, puede crear o actualizar el clúster con el tipo de nodo RA3. Para utilizar los tipos de nodo RA3, cree sus clústeres en una nube virtual privada (EC2-VPC).

Para cambiar el número de nodos del clúster de Amazon Redshift con un tipo de nodo RA3, realice una de las siguientes acciones:

- Agregue o elimine nodos con la operación de cambio de tamaño elástico. En algunas situaciones, la eliminación de nodos de un clúster RA3 no se permite con el cambio de tamaño elástico. Por ejemplo, cuando una actualización de recuento de nodos 2:1 coloca el número de sectores por nodo en 32. Para obtener más información, consulte [Cambio de tamaño de clústeres](#) (p. 23) . Si el cambio de tamaño elástico no está disponible, use el cambio de tamaño clásico.

- Agregue o quite nodos con la operación clásica de cambio de tamaño. Elija esta opción cuando cambie el tamaño a una configuración que no esté disponible mediante el cambio de tamaño elástico. El cambio de tamaño elástico es más rápido que el cambio de tamaño clásico. Para obtener más información, consulte [Cambio de tamaño de clústeres \(p. 23\)](#).

Disponibilidad del tipo de nodo RA3 enAWSRegiones

Los tipos de nodo RA3 solo están disponibles en la siguienteAWSRegiones:

- Región EE.UU. Este (Norte de Virginia) (us-east-1)
- Región EE.UU. Este (Ohio) (us-east-2)
- Región EE.UU. Oeste (Norte de California) (us-west-1)
- Región EE.UU. Oeste (Oregón) (us-west-2)
- Región Asia Pacífico (Hong Kong) (ap-east-1)
- Región Asia Pacífico (Mumbai) (ap-south-1)
- Región Asia Pacífico (Seúl) (ap-northeast-2)
- Región de Asia Pacífico (Singapur) (ap-southeast-1)
- Región de Asia Pacífico (Sídney) (ap-southeast-2)
- Región de Asia Pacífico (Tokio) (ap-northeast-1)
- Región Canadá (Central): ca-central-1
- Región de Europa (Fráncfort) (eu-central-1)
- Región de China (Pekín) (cn-north-1)
- Región de China (Ningxia) (cn-northwest-1)
- Región de Europa (Irlanda) (eu-west-1)
- Región de Europa (Londres) (eu-west-2)
- Región de Europa (París) (eu-west-3)
- Región de Europa (Estocolmo) (eu-north-1)
- América del Sur (São Paulo) (sa-east-1)
- AWSGovCloud (EE.UU. Este) (us-gov-east-1): solo están disponibles los tipos de nodos ra3.4xlarge y ra3.16xlarge.
- AWSGovCloud (Estados Unidos-Oeste) (us-gov-west-1): solo están disponibles los tipos de nodos ra3.4xlarge y ra3.16xlarge.

Actualización a tipos de nodo RA3

Para actualizar el tipo de nodo existente a RA3, tiene las siguientes opciones para cambiar el tipo de nodo:

- Restaurar desde una instantánea: Amazon Redshift utiliza la instantánea más reciente de su clúster DS2 o DC2 y la restaura para crear un nuevo clúster RA3. Tan pronto como se complete la creación del clúster (normalmente en cuestión de minutos), los nodos RA3 estarán listos para ejecutar toda la carga de trabajo de producción. Dado que la computación está separada del almacenamiento, los datos calientes se llevan a la caché local a velocidades rápidas gracias a un gran ancho de banda de red. Si restaura a partir de la última instantánea DS2 o DC2, RA3 conserva la información de bloques calientes de la carga de trabajo de DS2 o DC2 y rellena su caché local con los bloques más calientes. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 243\)](#).

Para mantener el mismo punto de enlace para las aplicaciones y los usuarios, puede cambiar el nombre del nuevo clúster RA3 por el mismo nombre que el clúster DS2 o DC2 original.

Para cambiar el nombre del clúster, modifique el clúster en la consola de Amazon Redshift o `ModifyCluster` Operación API. Para obtener más información, consulte [Cambio de nombre de los clústeres \(p. 32\)](#) o `ModifyCluster` Operación de la API en la Referencia del API de Amazon Redshift.

- Cambio de tamaño elástico: cambie el tamaño del clúster mediante el cambio de tamaño elástico. Cuando utiliza el ajuste elástico para cambiar el tipo de nodo, Amazon Redshift crea automáticamente una instantánea, crea un nuevo clúster, elimina el antiguo clúster y cambia el nombre del nuevo clúster. La operación de cambio de tamaño elástico puede ejecutarse bajo demanda o puede programarse para ejecutarse en un momento futuro. Puede actualizar rápidamente sus clústeres de tipo de nodo DS2 o DC2 existentes a RA3 con el cambio de tamaño elástico. Para obtener más información, consulte [Elastic resize \(Cambio de tamaño elástico\) \(p. 24\)](#).

En la siguiente tabla se muestran recomendaciones al actualizar a tipos de nodos RA3.

Tipo de nodo existente	Rango del número existente de nodos	Nuevo tipo de nodo recomendado	Acción de actualización	
ds2.xlarge	1—7	ra3.xlplus	Cree 2 nodos de ra3.xlplus por cada 3 nodos de ds2.xlarge.	
ds2.xlarge	8—128	ra3.4xlarge	Cree 1 nodo de ra3.4xlarge por cada 4 nodos de ds2.xlarge.	
ds2.8xlarge	2—15	ra3.4xlarge	Cree 2 nodos de ra3.4xlarge por cada 1 nodo de ds2.8xlarge.	
ds2.8xlarge	16—128	ra3.16xlarge	Cree 1 nodo de ra3.16xlarge por cada 2 nodos de ds2.8xlarge.	
dc2.8xlarge	2—15	ra3.4xlarge	Cree 2 nodos de ra3.4xlarge para cada 1 nodo de dc2.8xlarge ¹ .	
dc2.8xlarge	16—128	ra3.16xlarge	Cree 1 nodo de ra3.16xlarge por cada 2 nodos de dc2.8xlarge ¹ .	
dc2.large	1—4	ninguno	Mantenga el clúster dc2.large existente.	
dc2.large	4—15	ra3.xlplus	Cree 3 nodos de ra3.xlplus por cada 8 nodos de dc2.large ¹ .	
dc2.large	16—128	ra3.4xlarge	Cree 1 nodo de ra3.4xlarge por	

Tipo de nodo existente	Rango del número existente de nodos	Nuevo tipo de nodo recomendado	Acción de actualización	
			cada 8 nodos de dc2.large ¹ .	

¹Es posible que se necesiten nodos adicionales en función de los requisitos de carga de trabajo. Agregar o quitar nodos en función de los requisitos de computación del rendimiento de consulta requerido.

El número mínimo de nodos para clústeres RA3 es de 2 nodos. Tenga esto en cuenta al crear un clúster RA3.

Si ya ha adquirido nodos reservados DS2, póngase en contacto conAWSPara obtener ayuda para convertir los nodos reservados DS2 en nodos reservados RA3. Para ponerse en contacto conAWSPara obtener más información, consulte[Instancias de Amazon Redshift RA3 con almacenamiento administrado](#).

Actualización de tipos de nodo DC1 a tipos de nodo DC2

Para aprovechar las mejoras de rendimiento, puede actualizar sus clústeres DC1 a tipos de nodo DC2.

Los clústeres que usen los tipos de nodos DC2 deben lanzarse en una nube virtual privada (EC2-VPC).

Si el clúster DC1 no está en una VPC:

1. Cree una instantánea de su clúster DC1. Para obtener más información, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).
2. Cree una VPC y, a continuación, cree un clúster DC2 en la VPC. Para obtener más información, consulte [Administración de clústeres en una VPC \(p. 75\)](#).
3. Restaure la instantánea en el nuevo clúster DC2 en la VPC. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 243\)](#).

Si el clúster DC1 ya está en una VPC, elija uno de los métodos siguientes:

- Cambie el tamaño del clúster DC1 y cambie el tipo de nodo a DC2 como parte de la operación. El clúster no está disponible durante un período de tiempo durante la operación de cambio de tamaño. Para obtener más información, consulte [Cambio de tamaño de los clústeres de Amazon Redshift \(p. 23\)](#).
- Cree una instantánea del clúster DC1 y, a continuación, restaure la instantánea en un clúster DC2 en la VPC. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 243\)](#).

Tenga en cuenta lo siguiente al actualizar de tipos de nodos DC1 a DC2.

- Es posible que los clústeres DC1 que están 100% llenos no se actualicen a un número equivalente de nodos DC2. Si necesita más espacio en disco, puede.
 - Cambiar el tamaño a una configuración con más espacio en disco disponible.
 - Limpie los datos innecesarios mediante el truncamiento de tablas o la eliminación de filas.
- Los clústeres de DC2 no admiten redes de EC2-Classic. Si su clúster de DC1 no se está ejecutando en una VPC, cree una para su migración de DC2. Para obtener más información, consulte [Administración de clústeres en una VPC \(p. 75\)](#).

- Si cambia el tamaño del clúster, podría ponerse en modo de solo lectura durante el periodo que dure la operación. Para obtener más información, consulte [Cambio de tamaño de los clústeres de Amazon Redshift \(p. 23\)](#).
- Si ha adquirido nodos reservados DC1, puede actualizar sus nodos reservados DC1 a nodos DC2 durante el resto de su oferta. Para obtener más información sobre cómo cambiar la reserva con la AWS CLI, consulte [Actualizar nodos reservados con AWS CLI \(p. 278\)](#).
- Si utiliza restaurar para actualizar de dc1.large a dc2.large y cambia el número de nodos, la instantánea debe haberse creado en la versión del clúster 1.0.10013 o posterior.
- Si utiliza restaurar para actualizar de dc1.8xlarge a dc2.8xlarge, la instantánea debe haberse creado en la versión del clúster 1.0.10013 o posterior.
- Si utiliza el cambio de tamaño elástico para actualizar de DC1 a DC2 y cambia el número de nodos, el clúster debe estar en la versión 1.0.10013 o posterior del clúster.
- Si una instantánea del clúster dc1.8xlarge que se va a actualizar es de un clúster anterior a la versión 1.0.10013, restaure primero la instantánea desde el clúster dc1.8xlarge a un nuevo clúster dc1.8xlarge con el mismo número de nodos. A continuación, utilice uno de los siguientes métodos para actualizar el nuevo dc1.8xlarge:
 - Utilice una instantánea del nuevo clúster restaurado para actualizar a dc2.8xlarge.
 - Utilice elastic resize para actualizar el nuevo clúster restaurado a dc2.8xlarge.

Actualización de un clúster DS2 en EC2-Classic a EC2-VPC

Los clústeres de Amazon Redshift se ejecutan en instancias de Amazon EC2 configuradas para el tipo y el tamaño de nodo de Amazon Redshift que elija. Para mejorar el rendimiento y la seguridad de le recomendamos que actualice el clúster en EC2-Classic para lanzar en una VPC con EC2-VPC.

Para actualizar el clúster DS2 en EC2-Classic a EC2-VPC

1. Cree una instantánea de su clúster DS2. Para obtener más información, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).
2. Cree una VPC y, a continuación, cree un clúster DS2 en la VPC. Para obtener más información, consulte [Administración de clústeres en una VPC \(p. 75\)](#).
3. Restaure la instantánea en el nuevo clúster DS2 en la VPC. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 243\)](#).

Consideraciones sobre regiones y zonas de disponibilidad

Amazon Redshift está disponible en varios AWS Regiones de De forma predeterminada, Amazon Redshift aprovisiona su clúster en una Availability Zone (AZ) seleccionada de manera aleatoria dentro de la AWS Región que elija. Todos los nodos del clúster se aprovisionan en la misma zona de disponibilidad.

Opcionalmente, puede solicitar una zona de disponibilidad específica si Amazon Redshift está disponible en dicha zona. Por ejemplo, si ya dispone de una instancia de Amazon EC2 que se ejecuta en una zona de disponibilidad, es posible que desee crear el clúster de Amazon Redshift en la misma zona para reducir la latencia. Por otro lado, es posible que desee elegir otra zona de disponibilidad para obtener una mayor disponibilidad. Es posible que Amazon Redshift no esté disponible en todas las zonas de disponibilidad de una AWS Región.

Para obtener una lista de AWS Regiones en las que puede aprovisionar un clúster de Amazon Redshift, consulte [Puntos de enlace de Amazon Redshift](#) en la Referencia general de Amazon Web Services.

Mantenimiento de clústeres

Amazon Redshift realiza periódicamente tareas de mantenimiento para aplicar actualizaciones a su clúster. Durante estas actualizaciones, su clúster de Amazon Redshift no está disponible para las operaciones habituales. Existen varias formas de controlar cómo realizamos el mantenimiento de su clúster. Por ejemplo, puede controlar cuando implementamos actualizaciones en sus clústeres. También puede elegir si su clúster ejecuta la versión más reciente o la versión anterior a la versión más reciente. Finalmente, tiene la opción de posponer las actualizaciones de mantenimiento que no son obligatorias.

Temas

- [Períodos de mantenimiento \(p. 16\)](#)
- [Posponer el mantenimiento \(p. 17\)](#)
- [Elección de pistas de mantenimiento del clúster \(p. 17\)](#)
- [Administración de versiones del clúster \(p. 18\)](#)
- [Reversión de la versión del clúster \(p. 19\)](#)
- [Determinación de la versión de mantenimiento del clúster \(p. 20\)](#)

Períodos de mantenimiento

Amazon Redshift asigna una ventana de mantenimiento de 30 minutos al azar dentro de un bloque de 8 horas por AWS Región, que ocurre aleatoriamente un día de la semana (de lunes a domingo, inclusive).

Periodos de mantenimiento predeterminados

En la siguiente lista, se muestran los bloques de tiempo para cada AWS Región desde donde se asignan los periodos predeterminados de mantenimiento:

- Región EE.UU. Este (Virginia): 03:00 — 11:00 UTC
- Región: EE.UU. Este (Ohio) 03:00 — 11:00 UTC
- Región: EE. UU. Oeste (Norte de California) 06:00 — 14:00 UTC
- Región de EE. UU. Oeste (Oregón): 06:00 — 14:00 UTC
- Región de África (Ciudad del Cabo): 20:00 — 04:00 UTC
- Región Asia Pacífico (Hong Kong): 13:00 — 21:00 UTC
- Región Asia Pacífico (Mumbai): 16:30 — 00:30 UTC
- Región Asia Pacífico (Osaka) 13:00 — 21:00 UTC
- Región Asia Pacífico (Seúl): 13:00 — 21:00 UTC
- Región Asia Pacífico (Singapur) 14:00 — 22:00
- Región Asia Pacífico (Sídney) 12:00 — 20:00 UTC
- Región Asia Pacífico (Tokio) 13:00 — 21:00 UTC
- Región Canadá (Central) 03:00 — 11:00 UTC
- Región: China (Pekín) 13:00 — 21:00 UTC
- Región: China (Ningxia) 13:00 — 21:00 UTC
- Región de Europa (Fráncfort): 06:00 — 14:00 UTC
- Región de Europa (Irlanda): 22:00 — 06:00 UTC

- Región de Europa (Londres): 22:00 — 06:00 UTC
- Región Europa (Milán): 21:00 — 05:00 UTC
- Región: Europa (París) 23:00 — 07:00 UTC
- Región de Europa (Estocolmo): 23:00 — 07:00 UTC
- Región: 13:00 — 21:00 UTC
- Región América del Sur (São Paulo): 19:00 — 03:00 UTC

Si hay un evento de mantenimiento programado para una semana determinada, comienza dentro del período de mantenimiento de 30 minutos asignado. Mientras Amazon Redshift realiza las tareas de mantenimiento, se terminan todas las consultas o cualquier otra operación que haya en progreso. La mayoría de las tareas de mantenimiento se completan dentro del período de mantenimiento de 30 minutos, pero es posible que algunas tareas sigan ejecutándose después de que termine el período. Si no es necesario realizar tareas de mantenimiento durante el período de mantenimiento programado, su clúster continúa funcionando de manera habitual hasta el próximo período de mantenimiento programado.

Puede cambiar el período de mantenimiento programado si modifica el clúster, ya sea mediante programación o por medio de la consola de Amazon Redshift. El período debe ser de al menos 30 minutos y no debe superar las 24 horas. Para obtener más información, consulte [Administración de clústeres a través de la consola \(p. 44\)](#).

Posponer el mantenimiento

Si necesita volver a programar el período de mantenimiento de su clúster, tiene la opción de posponer el mantenimiento hasta 45 días. Por ejemplo, si el periodo de mantenimiento del clúster está establecido el miércoles de 8:30 a 9:00 UTC y necesite tener acceso al clúster justo a esa hora, puede posponer el mantenimiento. No se realizará ningún mantenimiento en el clúster cuando haya solicitado una postergación, a menos que sea necesario actualizar el hardware.

Si necesitamos actualizar el hardware o realizar alguna otra actualización obligatoria durante el período de postergación, le notificaremos y realizaremos los cambios necesarios. Su clúster no está disponible durante estas actualizaciones.

Si pospone el mantenimiento del clúster, es obligatorio que el período de mantenimiento comience justo después del periodo de postergación. No se puede posponer.

Note

No se puede posponer el mantenimiento una vez que haya comenzado.

Para obtener más información, consulte [Modificación de un clúster \(p. 59\)](#).

Elección de pistas de mantenimiento del clúster

Cuando Amazon Redshift lanza una nueva versión del clúster, este se actualiza durante su periodo de mantenimiento. Puede controlar si el clúster se actualiza a la versión aprobada más reciente o a la versión anterior.

La pista de mantenimiento controla qué versión del clúster se aplica durante un periodo de mantenimiento. Cuando Amazon Redshift lanza una nueva versión del clúster, esa nueva versión se asigna a la actual, y la versión anterior se asigna a la Registros de seguimiento Pista. Para establecer la pista de mantenimiento para el clúster, especifique uno de los siguientes valores.

- actual: usar la versión del clúster aprobada más reciente.
- Registros de seguimiento: usar la versión del clúster anterior a la versión actual.
- Vista previa: usar la versión del clúster que contiene nuevas funciones disponibles para previsualización.

Por ejemplo, supongamos que el clúster está ejecutando actualmente la versión 1.0.2762 y la versión actual de Amazon Redshift es 1.0.3072. Si establece el valor de pista de mantenimiento en Current (Actual), el clúster se actualiza a la versión 1.0.3072 (la siguiente versión aprobada) durante el siguiente período de mantenimiento. Si establece el valor de la pista de mantenimiento en Trailing (Anterior), el clúster no se actualizará hasta que haya una nueva versión posterior a la versión 1.0.3072.

Pistas de previsualización

Puede que no siempre haya una pista de previsualización disponible. Cuando elija una pista de previsualización, también deberá seleccionar un nombre de pista. Las pistas de previsualización y sus recursos relacionados son temporales, tienen limitaciones funcionales y es posible que no contengan todas las funciones de Amazon Redshift de disponibles en otras pistas. Cuando trabaje con pistas de previsualización:

- Utilice la nueva consola de Amazon Redshift cuando trabaje con pistas de previsualización. Por ejemplo, al crear un clúster para utilizarlo con las características de vista previa.
- No puede cambiar un clúster de una pista de previsualización a otra.
- No puede cambiar un clúster a una pista de previsualización desde una pista actual o anterior.
- No se puede restaurar desde una instantánea creada a partir de una pista de previsualización diferente.
- Solo puede usar la pista de previsualización cuando cree un nuevo clúster o al restaurar desde una instantánea.
- No puede restaurar desde una instantánea creada a partir de una pista de previsualización diferente o con una versión de mantenimiento del clúster posterior a la versión del clúster de la pista de previsualización. Por ejemplo, cuando se restaura un clúster a una pista de previsualización, solo se puede usar una instantánea creada a partir de una versión de mantenimiento del clúster anterior a la de la pista de previsualización.

Cambio entre pistas de mantenimiento

El cambio de pistas para un clúster es, por lo general, una decisión que se toma una única vez. Debe tener cuidado al cambiar pistas. Si cambia la pista de mantenimiento de Trailing (Anterior) a Current (Actual), actualizaremos el clúster a la versión de la pista Current (Actual) durante el siguiente periodo de mantenimiento. No obstante, si cambia la pista de mantenimiento del clúster a Trailing (Anterior), no actualizaremos el clúster hasta que haya una nueva versión después de la versión de la pista Current (Actual).

Pistas de mantenimiento y restauración

Una instantánea hereda la pista de mantenimiento del clúster de origen. Si cambia la pista de mantenimiento del clúster de origen después de tomar una instantánea, la instantánea y el clúster de origen estarán en pistas diferentes. Si realiza una restauración desde la instantánea, el nuevo clúster estará en la pista de mantenimiento que había heredado del clúster de origen. Puede cambiar la pista de mantenimiento cuando se complete la operación de restauración. Cambiar el tamaño de un clúster no afecta a la pista de mantenimiento del clúster.

Para obtener más información, consulte, [Establecimiento de la pista de mantenimiento de un clúster \(p. 60\)](#).

Administración de versiones del clúster

Una pista de mantenimiento es una serie de versiones. Puede decidir si su clúster está en la pista Current (Actual) o en la pista Trailing (Anterior). Si pone su clúster en la pista Current (Actual), siempre se actualizará a la versión de clúster más reciente durante el período de mantenimiento. Si pone su clúster en la pista Trailing (Anterior), siempre ejecutará la versión de clúster que se publicó inmediatamente anterior a la versión más reciente.

La **Estado de la versión** En la lista de clústeres de la consola de Amazon Redshift indica si alguno de los clústeres está disponible para actualizar.

Reversión de la versión del clúster

Si el clúster está actualizado con la última versión, puede optar por revertirlo a la versión anterior.

Para obtener información detallada acerca de las características y mejoras incluidas con cada versión del clúster, consulte [Historial de versiones del clúster](#) (p. 87).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

Nueva consola

Para revertir a una versión anterior del clúster

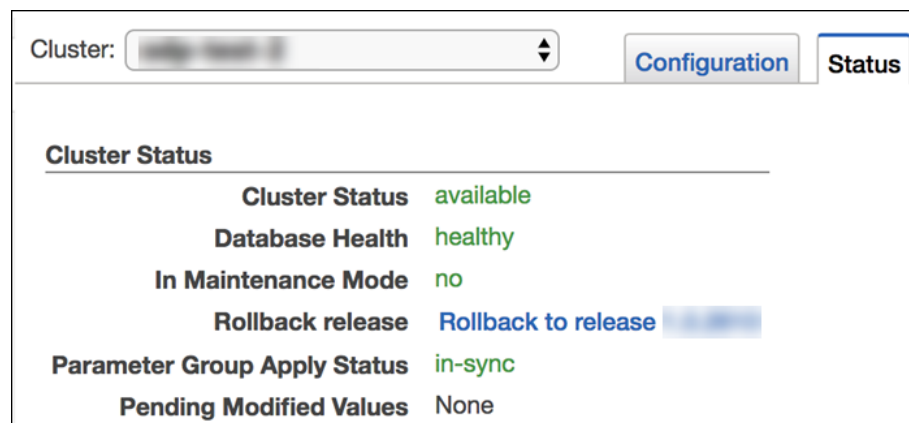
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Seleccione el clúster que quiere revertir.
4. En Actions (Acciones), seleccione Roll back cluster version (Revertir versión del clúster). Aparecerá la página Roll back cluster version (Revertir versión del clúster).
5. Si hay una versión disponible para revertir, siga las instrucciones de la página.
6. Seleccione Roll back now (Revertir ahora).

Consola original

Para revertir a una versión anterior del clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Elija el clúster que desea revertir y haga clic en la pestaña Status (Estado).

Si hay una versión disponible a la que puede revertir, aparecerá en la pestaña de estado en la página de detalles.



Cluster:

[Configuration](#) **Status**

Cluster Status

Cluster Status	available
Database Health	healthy
In Maintenance Mode	no
Rollback release	Rollback to release
Parameter Group Apply Status	in-sync
Pending Modified Values	None

4. Seleccione Rollback to release [Revertir a la versión] (número de versión).

Determinación de la versión de mantenimiento del clúster

Puede determinar la versión de motor de Amazon Redshift y de base de datos de con la consola de Amazon Redshift.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para encontrar la versión de un clúster

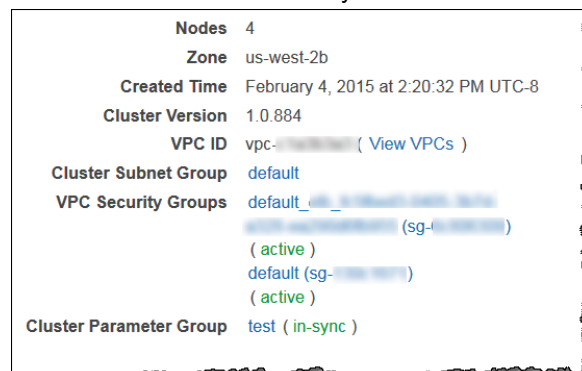
1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluirRendimiento del clúster,Supervisión de consultas,Bases de datos,Comparticiones de datos,Schedules,Mantenimiento, yPropiedadesPestañas.
3. Elija el iconoMantenimientopara ver más detalles.
4. En la sección Maintenance (Mantenimiento), busque Current cluster versión (Versión actual del clúster).

Note

Aunque la consola muestra esta información en un único campo, la API de Amazon Redshift de lo hace en dos parámetros:ClusterVersionyClusterRevisionNumber. Para obtener más información, consulte[Cluster \(Clúster\)](#)en laReferencia del API de Amazon Redshift.

Consola original

Puede determinar las versiones de motor y de base de datos de Amazon Redshift de para su clúster en laVersión del clústeren la consola. Las dos primeras secciones del número son la versión del clúster y la última sección es el número de revisión específica de la base de datos del clúster. En el siguiente ejemplo, la versión del clúster es la 1.0 y el número de revisión de la base de datos es 884.



Note

Aunque la consola muestra esta información en un único campo, la API de Amazon Redshift de lo hace en dos parámetros: `ClusterVersion` y `ClusterRevisionNumber`. Para obtener más información, consulte [Cluster \(Clúster\)](#) en la Referencia del API de Amazon Redshift.

Para especificar si se debe actualizar automáticamente el motor de Amazon Redshift en su clúster cuando haya una nueva versión del motor disponible, utilice la configuración Permitir actualización de la versión. Esta opción de no afecta a las actualizaciones de versiones de base de datos de, que se aplican durante la ventana de mantenimiento que haya especificado para el clúster. Las actualizaciones del motor de Amazon Redshift son Actualizaciones de la versión principal, y las actualizaciones de la base de datos de Amazon Redshift son Actualizaciones de versiones secundarias. Solo puede deshabilitar la opción de actualización automática de versiones principales. Para obtener más información acerca de los períodos de mantenimiento de las actualizaciones secundarias de versiones, consulte [Períodos de mantenimiento](#) (p. 16).

Alarma predeterminada de espacio en disco

Cuando crea un clúster de Amazon Redshift, opcionalmente, puede configurar una alarma de Amazon CloudWatch para monitorear el porcentaje promedio del espacio de disco utilizado en todos los nodos del clúster. Nos referiremos a esta alarma como la alarma predeterminada de espacio en disco.

El objetivo de la alarma predeterminada de espacio en disco es ayudarle a monitorear la capacidad de almacenamiento de su clúster. Puede configurar esta alarma en función de las necesidades de su data warehouse. Por ejemplo, puede usar la advertencia como un indicador de que tal vez tenga que ajustar el tamaño del clúster. Puede cambiar el tamaño a un tipo de nodo diferente o añadir nodos, o quizás comprar nodos reservados para una futura ampliación.

La alarma predeterminada de espacio en disco se activa cuando el uso del disco alcanza o supera un porcentaje específico una determinada cantidad de veces y con una duración específica. De forma predeterminada, esta alarma se activa cuando se alcanza el porcentaje que haya especificado y cuando permanece, o supera, en ese porcentaje durante cinco minutos o más tiempo. Puede editar los valores predeterminados después de lanzar su clúster.

Cuando se activa la alarma de CloudWatch, Amazon Simple Notification Service (Amazon SNS) envía una notificación a los destinatarios especificados para avisarlos de que se ha alcanzado el porcentaje indicado en el umbral. Amazon SNS utiliza un tema para especificar los destinatarios y el mensaje que se envía en las notificaciones. Puede utilizar un tema de Amazon SNS de existente o, de lo contrario, se crea un tema en función de la configuración que haya especificado cuando lanzó el clúster. Puede editar el tema de esta alarma después de lanzar el clúster. Para obtener más información acerca de la creación de temas de Amazon SNS, consulte [Introducción al servicio de notificaciones simples de Amazon](#).

Después de lanzar el clúster, puede ver y editar la alarma desde la ventana Estado del clúster, bajo Alarmas de CloudWatch. El nombre es `percentage-disk-space-used-default-<cadena>`. Puede abrir la alarma para ver el tema de Amazon SNS con el que está asociada y editar la configuración de la alarma. Si no seleccionó un tema de Amazon SNS de existente, el tema creado para usted se llamará `<Clustername>-alarmas predeterminadas (<destinatario>)`; por ejemplo, `ejemploalarmas predeterminadas de luster-predeterminadas (notify@example.com)`.

Para obtener más información acerca de cómo configurar y editar la alarma predeterminada de espacio en disco, consulte [Creación de un clúster](#) (p. 47) y [Crear o editar una alarma de espacio en disco](#) (p. 70).

Note

Si elimina el clúster, no se eliminará la alarma asociada con el clúster, pero tampoco se activará. Si ya no necesita la alarma, puede eliminarla desde la consola de CloudWatch.

Estado del clúster

El estado del clúster muestra el estado actual del clúster. En la siguiente tabla, se proporciona una descripción de cada estado del clúster.

Estado	Descripción
available	El clúster se está ejecutando y está disponible.
available, prep-for-resize	Se está preparando el clúster para un cambio de tamaño elástico. El clúster está en ejecución y disponible para consultas de lectura y escritura, aunque las operaciones de clúster, como crear instantáneas, no están disponibles.
available, resize-cleanup	Una operación de cambio de tamaño elástico está completando la transferencia de datos a los nuevos nodos del clúster. El clúster está en ejecución y disponible para consultas de lectura y escritura, aunque las operaciones de clúster, como crear instantáneas, no están disponibles.
cancelling-resize	Se está cancelando la operación de cambio de tamaño.
creating	Amazon Redshift está creando el clúster. Para obtener más información, consulte Creación de un clúster (p. 47) .
deleting	Amazon Redshift está eliminando el clúster. Para obtener más información, consulte Eliminación de un clúster (p. 61) .
final-snapshot	Amazon Redshift está realizando una instantánea final del clúster antes de eliminarlo. Para obtener más información, consulte Eliminación de un clúster (p. 61) .
hardware-failure	Se detectó un error de hardware en el clúster. Si tiene un clúster de nodo único, el nodo no puede reemplazarse. Para recuperar su clúster, restaure una snapshot. Para obtener más información, consulte Instantáneas de Amazon Redshift (p. 238) .
incompatible-hsm	Amazon Redshift no puede conectarse al módulo de seguridad de hardware (HSM). Compruebe la configuración del HSM entre el clúster y el HSM. Para obtener más información, consulte Cifrado para Amazon Redshift mediante módulos de seguridad de hardware (p. 288) .
incompatible-network	Hay un problema con la configuración de red subyacente. Asegúrese de que la VPC en la que lanzó el clúster exista y de que está bien configurada. Para obtener más información, consulte Administración de clústeres en una VPC (p. 75) .
incompatible-parameters	Hay un problema con uno o más valores de parámetros en el grupo de parámetros asociados y no se pueden aplicar los valores del parámetro. Modifique el grupo de parámetros y actualice todo valor que no sea válido. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift (p. 210) .
incompatible-restore	Hubo un problema al restaurar el clúster desde la snapshot. Vuelva a restaurar el clúster con una snapshot diferente. Para obtener más información, consulte Instantáneas de Amazon Redshift (p. 238) .
modifying	Amazon Redshift está aplicando cambios en el clúster. Para obtener más información, consulte Modificación de un clúster (p. 59) .

Estado	Descripción
paused	El clúster está en pausa. Para obtener más información, consulte Pausa y reanudación de clústeres (p. 31) .
rebooting	Amazon Redshift está reiniciando el clúster. Para obtener más información, consulte Reinicio de un clúster (p. 63) .
renaming	Amazon Redshift está aplicando un nombre nuevo en el clúster. Para obtener más información, consulte Cambio de nombre de los clústeres (p. 32) .
resizing	Amazon Redshift está cambiando el tamaño del clúster. Para obtener más información, consulte Redimensionamiento de un clúster (p. 64) .
rotating-keys	Amazon Redshift está rotando las claves de cifrado del clúster. Para obtener más información, consulte Rotación de claves de cifrado en Amazon Redshift (p. 289) .
storage-full	El clúster alcanzó su capacidad de almacenamiento. Cambie el tamaño del clúster para añadir nodos o elija un tamaño de nodo diferente. Para obtener más información, consulte Redimensionamiento de un clúster (p. 64) .
updating-hsm	Amazon Redshift está actualizando la configuración de HSM.

Información general sobre cómo administrar los clústeres de Amazon Redshift

Después de haber creado el clúster, hay varias operaciones que puede realizar en él. Las operaciones incluyen el cambio de tamaño, la pausa, la reanudación, el cambio de nombre y la eliminación.

Cambio de tamaño de los clústeres de Amazon Redshift

A medida que la capacidad y el rendimiento del almacenamiento de datos necesitan cambiar o aumentar, puede cambiar el tamaño del clúster para hacer el mejor uso de las opciones informáticas y de almacenamiento que proporciona Amazon Redshift.

Puede usar el cambio de tamaño elástico para escalar el clúster cambiando el tipo y el número de nodos. Recomendamos utilizar el cambio de tamaño elástico, que normalmente se completa en minutos. Si la configuración del nuevo nodo no está disponible mediante el cambio de tamaño elástico, puede utilizar el cambio de tamaño clásico. El cambio de tamaño clásico tarda más tiempo en completarse, ya que implica el aprovisionamiento de un nuevo clúster y la copia de bloques de datos en él. Por el contrario, elastic resize redistribuye sectores de datos, lo que requiere menos recursos.

Para cambiar el tamaño del clúster, utilice uno de los métodos siguientes:

- Elastic resize (Cambio de tamaño elástico)— Utilícelo para cambiar el tipo de nodo, el número de nodos o ambos. El cambio de tamaño de Elastic funciona rápidamente cambiando o agregando nodos al clúster existente. Si cambia sólo el número de nodos, las consultas se detienen temporalmente y las conexiones se mantienen abiertas, si es posible. Normalmente, el cambio de tamaño elástico tarda entre 10 y 15 minutos. Durante la operación de cambio de tamaño, el clúster es de solo lectura.

Recomendamos utilizar el cambio de tamaño elástico siempre que sea posible, ya que se completa mucho más rápidamente que el cambio de tamaño clásico.

- **Classic resize (Cambio de tamaño clásico)**— Utilícelo para cambiar el tipo de nodo, el número de nodos o ambos. El cambio de tamaño clásico aprovisiona un nuevo clúster y copia los datos del clúster origen al clúster nuevo. Elija esta opción solo cuando cambie el tamaño a una configuración que no esté disponible mediante el cambio de tamaño elástico, ya que tarda mucho más en completarse. Un ejemplo de cuándo usarlo es cuando cambia el tamaño a o desde un clúster de nodo único. Durante la operación de cambio de tamaño, el clúster es de solo lectura. El cambio de tamaño clásico puede tardar varias horas a varios días, o más, dependiendo de la cantidad de datos que se van a transferir y de la diferencia en el tamaño del clúster y los recursos informáticos.

Si la configuración garantiza realizar un cambio de tamaño clásico, puede minimizar el impacto en la producción haciendo una copia del clúster existente y, posteriormente, redimensionando la copia. [Instantánea, restauración y cambio de tamaño \(p. 28\)](#) describe los pasos.

Puede cambiar el tamaño (tanto cambio de tamaño elástico como clásico) del su clúster siguiendo una programación. Cuando utilice la nueva consola de Amazon Redshift, puede configurar una programación para cambiar el tamaño del clúster. Para obtener más información, consulte [Redimensionamiento de un clúster \(p. 64\)](#). También puede utilizar la AWS CLI para programar un Amazon Redshift de tamaño. Para obtener más información, consulte [crear-action](#) en la AWS CLI Referencia de los comandos de la [CreateScheduledAction](#) en la Referencia de la API de Amazon Redshift.

Temas

- [Elastic resize \(Cambio de tamaño elástico\) \(p. 24\)](#)
- [Classic resize \(Cambio de tamaño clásico\) \(p. 27\)](#)
- [Instantánea, restauración y cambio de tamaño \(p. 28\)](#)
- [Detalles del cambio de tamaño de un clúster \(p. 29\)](#)

Elastic resize (Cambio de tamaño elástico)

El cambio de tamaño elástico es el método más rápido de cambiar el tamaño de un clúster. Puede utilizar el ajuste elástico para agregar o quitar nodos y cambiar los tipos de nodos de un clúster existente.

Cuando el tamaño de un clúster se modifica utilizando el ajuste elástico con el mismo tipo de nodo, los datos se redistribuyen automáticamente por los nuevos nodos. Como no crea un nuevo clúster en este escenario, la operación de cambio de tamaño elástico se completa con rapidez, normalmente en unos pocos minutos. Es posible que observe un ligero incremento en el tiempo de ejecución para algunas consultas mientras se redistribuyen los datos en segundo plano. Una operación de cambio de tamaño elástico se produce en las siguientes etapas:

1. El cambio de tamaño elástico toma una instantánea del clúster.

La instantánea que crea el cambio de tamaño elástico incluye [tablas sin copia de seguridad \(p. 242\)](#). Si el clúster no tiene una instantánea reciente porque deshabilitó las instantáneas automatizadas, la operación de copia de seguridad tardará más tiempo. Para minimizar el tiempo antes de que dé comienzo la operación de cambio de tamaño, le recomendamos habilitar la creación automatizada de instantáneas o crear una instantánea manual antes de comenzar un cambio de tamaño elástico. Cuando inicia un cambio de tamaño elástico y hay una operación de instantánea actualmente en curso, el cambio de tamaño elástico podría devolver un error si la operación de instantánea no se completa en unos minutos. Para obtener más información, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

2. El clúster no estará disponible temporalmente mientras el cambio de tamaño elástico migra los metadatos del clúster.

Esta etapa es muy breve, solo unos minutos como máximo. Amazon Redshift mantiene las conexiones de la sesión y las consultas permanecen en cola. Algunas sesiones y consultas podrían agotar el tiempo de espera.

3. Se restablecen las conexiones de la sesión y se reanudan las consultas.

- El cambio de tamaño elástico redistribuye los datos a los sectores de nodos en segundo plano.

El clúster está disponible para operaciones de lectura y escritura, aunque es posible que algunas consultas tarden más tiempo en ejecutarse.

Cuando se modifica el tamaño de un clúster utilizando el ajuste elástico para cambiar el tipo de nodo, se crea una instantánea. De forma automática, se aprovisionará un nuevo clúster con los datos más recientes de la instantánea. No se podrá escribir en el clúster durante algún tiempo cuando los datos se transfieran al nuevo clúster. Sí se podrá leer. El nuevo clúster se rellena en segundo plano. Una vez completado el nuevo clúster, las consultas deben alcanzar un rendimiento óptimo. Cuando el proceso de cambio de tamaño esté a punto de finalizar, Amazon Redshift actualizará el punto de enlace del nuevo clúster y finalizarán todas las conexiones con el clúster original.

Una vez completado el cambio de tamaño, Amazon Redshift envía una notificación de evento. Podrá conectarse al clúster de destino y reanudar la ejecución de las consultas de lectura y de escritura.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para monitorizar el progreso de una operación de cambio de tamaño mediante la consola de Amazon Redshift, elija CLÚSTERES DELuego elija el clúster que va a cambiar de tamaño para ver los detalles.

Consola original

Para monitorizar el progreso de una operación de cambio de tamaño elástico mediante la consola de Amazon Redshift, elija laEstadoEn la página de detalles del clúster.

The screenshot shows the Amazon Redshift console interface for a cluster named 'resize-example'. The 'Status' tab is selected, showing the following information:

- Cluster Status:** resizing
- Database Health:** healthy
- In Maintenance Mode:** no
- Parameter Group Apply Status:** in-sync
- Pending Modified Values:** None
- Resize Target:**
 - Target Node Type: dc2.large
 - Target Number of Nodes: 8
- Resize Status:**
 - Resize Status: in progress
 - Resize Progress: 0% (Determining amount of data to be transferred...)
 - Average Rate of Transfer: Data currently unavailable
 - Elapsed Time: Data currently unavailable
 - Remaining Time: Data currently unavailable

Below the status information, the 'Recent Events' section shows a log entry for the elastic resize operation:

Date	Time	Event	Severity	Source type	Categories
Nov 9	12:28 PM	Elastic resize for Amazon Redshift cluster 'resize-example' started at 2018-11-09 20:28 UTC. We will hold the database connections during resize. Some queries and connections may be terminated or timed out during this operation.	info	cluster	management

No puede usar el cambio de tamaño elástico en clústeres de nodo único.

Para ejecutar un cambio de tamaño elástico en un clúster que está transfiriendo datos desde una instantánea compartida, debe haber al menos una copia de seguridad disponible para el clúster. Puede ver las copias de seguridad en la lista de instantáneas de la consola de Amazon Redshift, `describe-cluster-snapshots` CLI, o el comando `DescribeClusterSnapshots` Operación de la API de.

El cambio de tamaño elástico no ordena tablas ni recupera espacio en disco, por lo que no es un sustituto de una operación de limpieza. Un cambio de tamaño clásico copia tablas a un nuevo clúster, por lo que reduce la necesidad de efectuar una limpieza. Para obtener más información, consulte [Limpieza de tablas](#).

El cambio de tamaño elástico tiene las siguientes limitaciones:

- El cambio de tamaño elástico solo está disponible para clústeres que usan la plataforma EC2-VPC. Para obtener más información, consulte [Usar EC2-VPC al crear el clúster \(p. 9\)](#).
- Asegúrese de que la configuración del nuevo nodo tenga suficiente almacenamiento para los datos existentes. Incluso cuando se añaden nodos, es posible que la nueva configuración no disponga de suficiente almacenamiento por la forma en que se han redistribuido los datos.
- Las configuraciones posibles del número y el tipo de nodo a las que puede cambiar el tamaño se determinan por el número de nodos del clúster original y el tipo de nodo de destino del clúster con el tamaño cambiado. Para determinar las posibles configuraciones disponibles, puede utilizar la consola de. También puede utilizar `describe-node-configuration-options` AWS CLI Comando de la con `laaction-type resize-cluster` Opción de. Para obtener más información sobre cómo cambiar el tamaño mediante la consola de Amazon Redshift, consulte [Redimensionamiento de un clúster \(p. 64\)](#).

El siguiente comando CLI de ejemplo describe las opciones de configuración disponibles. En este ejemplo, el clúster denominado `mycluster` es un clúster `dc2.large` de 8 nodos.

```
aws redshift describe-node-configuration-options --cluster-identifier mycluster --region eu-west-1 --action-type resize-cluster
```

Este comando devuelve una lista de opciones con recomendaciones sobre los tipos de nodos, el número de nodos y el uso de disco de cada opción. Las configuraciones devueltas pueden variar en función del clúster de entrada específico. Puede elegir una de las configuraciones devueltas cuando especifique las opciones de `laresize-cluster` Command CLI.

- El cambio de tamaño de Elastic tiene límites en los nodos que se pueden agregar a un clúster. Por ejemplo, un clúster `dc2` admite el cambio de tamaño elástico hasta duplicar el número de nodos. Para ilustrar, puede agregar un nodo a un clúster `dc2.8xlarge` de 4 nodos para convertirlo en un clúster de 5 nodos, o agregar más nodos hasta que alcance 8.

Con algunos tipos de nodos `ra3`, puede aumentar el número de nodos hasta cuatro veces el recuento existente. Específicamente, supongamos que su clúster consta de nodos `ra3.4xlarge` o `ra3.16xlarge`. A continuación, puede utilizar `elastic resize` para aumentar el número de nodos en un clúster de 8 nodos a 32. O puede elegir un valor por debajo del límite. Si su clúster tiene nodos `ra3.xlplus`, el límite es doble.

Todos los tipos de nodos `ra3` admiten una disminución en el número de nodos a una cuarta parte del recuento existente. Por ejemplo, puede reducir el tamaño de un clúster con nodos `ra3.4xlarge` de 12 a 3, o a un número por encima del mínimo.

En la siguiente tabla se enumeran los límites de crecimiento y reducción para cada tipo de nodo que admite el cambio de tamaño elástico.

Tipo de nodo	Límite de crecimiento	Límite de reducción
<code>ra3.16xlarge</code>	4x (de 4 a 16 nodos, por ejemplo)	A una cuarta parte del número (de 16 a 4 nodos, por ejemplo)

Tipo de nodo	Límite de crecimiento	Límite de reducción
ra3.4xlarge	4x	A una cuarta parte del número
ra3.xlplus	2x (de 4 a 8 nodos, por ejemplo)	A una cuarta parte del número
dc2.8xlarge	2x	A la mitad del número (de 16 a 8 nodos, por ejemplo)
dc2.large	2x	A la mitad del número
ds2.8xlarge	2x	A la mitad del número
ds2.xlarge	2x	A la mitad del número

Classic resize (Cambio de tamaño clásico)

Con la operación de cambio de tamaño clásico, los datos se copian en paralelo desde el o los nodos de computación del clúster de origen hacia el o los nodos de computación del clúster de destino. El tiempo que toma el cambio de tamaño depende de la cantidad de datos y el número de nodos del clúster más pequeño. Puede tardar desde unas cuantas horas hasta varios días o más.

La duración de un cambio de tamaño clásico varía según diversos factores, incluyendo:

- La carga de trabajo en el clúster de origen.
- El número y tamaño de las tablas que se transfieren.
- Cómo se distribuyen los datos de manera uniforme entre los nodos de computación y los sectores.
- La configuración del nodo en los clústeres de origen y destino.

Cuando comienza la operación de cambio de tamaño, Amazon Redshift pone el clúster existente en el modo de solo lectura hasta que finalice el cambio de tamaño. Durante este tiempo, solo puede ejecutar consultas que lean datos de la base de datos. No puede ejecutar ninguna consulta que escriba en la base de datos, incluidas las consultas de lectura y escritura. Para obtener más información, consulte [Operaciones de lectura y escritura y de escritura](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Note

Para cambiar el tamaño con un impacto de producción mínimo, puede seguir los pasos que se muestran en la siguiente sección, [Instantánea, restauración y cambio de tamaño \(p. 28\)](#). Puede usar estos pasos para crear una copia del clúster, cambiar el tamaño de la copia y luego cambiar el punto de enlace de conexión al clúster con el nuevo tamaño una vez que se complete el cambio de tamaño.

Tanto la opción del cambio de tamaño clásico como la de utilizar instantáneas y restaurar copian las tablas y los datos de usuario al clúster nuevo; no retienen ni los datos ni las tablas del sistema. Tanto con el cambio de tamaño clásico como la opción de crear una instantánea y restaurar, si habilitó el registro de auditoría en el clúster de origen, podrá seguir obteniendo acceso a los registros en Amazon S3. Con estos dos enfoques, seguirá teniendo acceso a los registros incluso si elimina el clúster de origen. Puede omitir o eliminar estos registros según lo especifiquen las políticas de datos. El cambio de tamaño elástico retiene las tablas de registro del sistema.

Una vez que Amazon Redshift pone el clúster de origen en el modo de solo lectura, aprovisiona un nuevo clúster, el clúster destino. Para ello, utiliza la información especificada para el tipo de nodo, tipo de clúster y número de nodos. Luego, Amazon Redshift copia los datos del clúster origen al clúster destino. Cuando esta operación se completa, todas las conexiones pasan a utilizar el clúster de destino. Si tiene alguna consulta en proceso en el momento que ocurra el cambio, la conexión se perderá y deberá reiniciar la

consulta en el clúster de destino. Puede ver el progreso del cambio de tamaño en la consola de Amazon Redshift.

Amazon Redshift no ordena las tablas durante la operación de cambio de tamaño, por lo que se mantiene el orden existente. Cuando cambia el tamaño de un clúster, Amazon Redshift distribuye las tablas de la base de datos a los nuevos nodos en función de sus estilos de distribución y ejecuta un comando ANALYZE para actualizar las estadísticas. Las filas que estén marcadas para eliminarse no se transfieren, por lo que solo deberá ejecutar un comando VACUUM en el caso que necesite reordenar las tablas. Para obtener más información, consulte [Limpieza de tablas](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Para cancelar una operación de cambio de tamaño clásico antes de que se complete, elija **Cancelar cambio de tamaño** en los detalles del clúster de la consola de Amazon Redshift. La cantidad de tiempo que toma cancelar un cambio de tamaño depende de la fase en que cancela la operación de cambio de tamaño. El clúster no está disponible hasta que se complete la operación de cancelación del cambio de tamaño. Si la operación de cambio de tamaño está en la fase final, no podrá cancelar la operación.

Instantánea, restauración y cambio de tamaño

Como se describió en la sección anterior, el tiempo que toma cambiar el tamaño de un clúster con la operación de cambio de tamaño clásico depende en gran medida de la cantidad de datos que haya en el clúster.

[Elastic resize \(Cambio de tamaño elástico\)](#) (p. 24) es el método más rápido de cambiar el tamaño de un clúster de Amazon Redshift. Si el cambio de tamaño elástico no es una opción y necesita acceso de escritura casi constante al clúster, utilice las operaciones de instantánea y restauración con el cambio de tamaño clásico descritas en la siguiente sección. Este enfoque requiere que cualquier dato que se escriba en el clúster de origen después de que se tomó la instantánea deba copiarse manualmente al clúster de destino después del cambio. Según el tiempo que tome la copia, es posible que deba repetir esto varias veces hasta que obtenga los mismos datos en ambos clústeres. A continuación, puede realizar el cambio al clúster de destino. Este proceso puede tener un impacto negativo en las consultas existentes hasta que el conjunto completo de datos esté disponible en el clúster de destino. Sin embargo, sí reduce la cantidad de tiempo en el que no puede escribir a la base de datos.

Para el método de instantánea, restauración y cambio de tamaño se utiliza el siguiente proceso:

1. Tome una instantánea del clúster existente. El clúster existente es el de origen.
2. Anote la hora a la que se realizó la instantánea. Esto sirve para que más adelante pueda identificar el punto temporal en el que tendrá que volver a ejecutar los procesos de extracción, transformación y carga (ETL) para cargar cualquier dato posterior a la instantánea en la base de datos de destino.
3. Restaure la instantánea en un clúster nuevo. Este clúster nuevo es el de destino. Compruebe que existan los datos de ejemplo en el clúster de destino.
4. Cambie el tamaño del clúster de destino. Elija el nuevo tipo de nodo, el número de nodos y otras configuraciones para el clúster de destino.
5. Revise las cargas de los procesos ETL que ocurrieron después de que tomó la instantánea del clúster de origen. Asegúrese de volver a cargar los mismos datos en el mismo orden en el clúster de destino. Si tiene cargas de datos en curso, repita este proceso varias veces hasta que los datos sean los mismos en el clúster de origen como en el de destino.
6. Detenga todas las consultas en ejecución en el clúster de origen. Para ello, puede reiniciar el clúster o puede registrarse como superusuario y utilizar los comandos [PG_CANCEL_BACKEND](#) y [PG_TERMINATE_BACKEND](#). El reinicio del clúster es la forma más sencilla de asegurar que el clúster no esté disponible.
7. Cambie el clúster de origen. Por ejemplo, cambie el nombre de `examplecluster` a `examplecluster-source`.
8. Cambie el nombre del clúster de destino para utilizar el nombre del clúster de origen antes del cambio de nombre. Por ejemplo, cambie el nombre del clúster de destino anterior a `examplecluster`. A partir

de este punto, cualquier aplicación que utilice el punto de enlace que contiene `examplecluster` se conecta al clúster de destino.

9. Elimine el clúster de origen después de cambiar al clúster de destino y compruebe que todos los procesos funcionen según lo previsto.

También puede cambiar el nombre de los clústeres de origen y de destino antes de volver a cargar los datos en el clúster de destino. Este enfoque funciona si no tiene el requisito de que alguno de los sistemas e informes dependientes se actualicen con los del clúster de destino. En este caso, el paso 6 se mueve al final del proceso descrito anteriormente.

El proceso de cambio de nombre solo se requiere si desea que las aplicaciones sigan utilizando el mismo punto de enlace para conectarse al clúster. Si no necesita esto, en su lugar puede actualizar cualquier aplicación que se conecte al clúster para utilizar el punto de enlace del clúster de destino sin cambiar el nombre del clúster.

Existen algunos beneficios en reutilizar el nombre de un clúster. Primero, no necesita actualizar las cadenas de conexión de aplicaciones ya que el punto de enlace no cambia, aunque cambia el clúster subyacente. Segundo, los elementos relacionados, como las alarmas de Amazon CloudWatch y las notificaciones de Amazon Simple Notification Service (Amazon SNS), están asociados al nombre del clúster. Esta asociación significa que puede seguir utilizando las mismas alarmas y notificaciones que configuró para el clúster. Este uso continuo es principalmente un problema en los entornos de producción, donde se desea tener la flexibilidad para cambiar el tamaño del clúster sin tener que volver a configurar los elementos relacionados, como alarmas y notificaciones.

Detalles del cambio de tamaño de un clúster

Si después del aprovisionamiento inicial de su clúster cambian las necesidades de almacenamiento y de rendimiento, puede cambiar el tamaño del clúster. Puede escalar o reducir las instancias del clúster al añadir o quitar nodos. Además, puede aumentar o reducir la escala del clúster al especificar un tipo de nodo diferente.

Por ejemplo, puede añadir más nodos, cambiar el tipo de nodos, pasar de un clúster de nodo único a uno de nodos múltiples o pasar de un clúster de nodos múltiples a uno de nodo único. Sin embargo, debe asegurarse de que el clúster resultante tenga el tamaño suficiente para almacenar los datos que tiene actualmente, de lo contrario el cambio de tamaño no funcionará. Al utilizar la API, tiene que especificar el tipo, el tamaño y la cantidad de nodos, aunque solo cambie una de las propiedades.

A continuación, se describe el proceso de cambio de tamaño:

1. Cuando inicia el proceso de cambio de tamaño, Amazon Redshift envía una notificación de evento que reconoce la solicitud de cambio de tamaño y comienza a aprovisionar el nuevo clúster (destino).
2. Cuando se aprovisiona al nuevo clúster (destino), Amazon Redshift envía una notificación de evento para indicar que se inició el cambio de tamaño (origen) existente en modo de solo lectura. El proceso de reinicio termina todas las conexiones existentes hacia el clúster. Se restauran todas las transacciones sin confirmar (incluso COPY). Mientras el clúster está en modo de solo lectura, puede ejecutar consultas de lectura, pero no de escritura.
3. Amazon Redshift comienza a copiar los datos del clúster origen al clúster destino.
4. Cuando el proceso de cambio de tamaño esté a punto de finalizar, Amazon Redshift actualizará el punto de enlace del clúster destino y finalizarán todas las conexiones al clúster origen.
5. Una vez completado el cambio de tamaño, Amazon Redshift envía una notificación de evento para indicar que el cambio de tamaño se completó. Puede conectarse al clúster destino y reanudar la ejecución de las consultas de lectura y de escritura.

Cuando cambia el tamaño del clúster, este seguirá en modo de solo lectura hasta que se complete el cambio de tamaño. Puede ver el progreso del cambio de tamaño en la consola de Amazon Redshift. El

tiempo que toma cambiar el tamaño de un clúster depende de la cantidad de datos que haya en cada nodo. Por lo general, el proceso de cambio de tamaño tarda entre un par de horas hasta un día, si bien los clústeres que tienen mayor cantidad de datos pueden tardar aún más tiempo. Esto se debe a que los datos se copian en paralelo desde cada nodo del clúster origen hacia los nodos del clúster destino. Para obtener más información sobre el cambio de tamaño de los clústeres, consulte [Redimensionamiento de un clúster](#) (p. 64).

Amazon Redshift no ordena las tablas durante la operación de cambio de tamaño. Cuando cambia el tamaño de un clúster, Amazon Redshift distribuye las tablas de la base de datos a los nuevos nodos de computación en función de sus estilos de distribución y ejecuta la función ANALYZE para actualizar las estadísticas. Las filas que estén marcadas para eliminarse no se transfieren, por lo que deberá ejecutar un comando VACUUM solo si necesita reordenar las tablas. Para obtener más información, consulte [Limpieza de tablas](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Si su clúster es público y está en una VPC, después del cambio de tamaño, conservará la misma dirección IP elástica (EIP) para el nodo principal. Si su clúster es privado y está en una VPC, después del cambio de tamaño conserva la misma dirección IP privada para el nodo principal. Si su clúster no está en una VPC, se asigna una nueva dirección IP pública para el nodo principal como parte de la operación de cambio de tamaño.

Para obtener la dirección IP del nodo principal para un clúster, utilice la utilidad dig, tal como se muestra a continuación:

```
dig mycluster.abcd1234.us-west-2.redshift.amazonaws.com
```

La dirección IP del nodo principal está al final de la sección ANSWER SECTION en los resultados, tal como se muestra a continuación:

```
; <<>> DiG 9.10.1-P1 <<>> [redacted]
com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 55520
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDI
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags::; udp: 1280
;; QUESTION SECTION:
;[redacted]
;; ANSWER SECTION:
[redacted] 6
[redacted]
[redacted] 4239 IN
.. AUTHORITY SECTION.
```

Pausa y reanudación de clústeres

Si tiene un clúster que solo tiene que estar disponible en momentos específicos, puede pausar el clúster y reanudarlo posteriormente. Mientras el clúster está en pausa, la facturación bajo demanda se suspende. Solo el almacenamiento del clúster incurre en cargos. Para obtener más información sobre los precios, consulte la [Página Precios de Amazon Redshift](#).

Cuando pausa un clúster, Amazon Redshift crea una snapshot, comienza a terminar consultas y pone el clúster en estado de pausa. Si elimina un clúster en pausa sin solicitar una instantánea final, no podrá restaurar el clúster. No puede cancelar o deshacer una pausa o reanudar una operación después de que se haya iniciado.

Puede pausar y reanudar un clúster en la nueva consola de Amazon Redshift (no en la consola original), con la AWS CLI o con las operaciones de la API de Amazon Redshift.

Puede programar acciones para pausar y reanudar un clúster. Cuando utiliza la nueva consola de Amazon Redshift para crear una programación periódica para pausar y reanudar, se crean dos acciones programadas para el intervalo de fechas que elija. Los nombres de las acciones programadas tienen el sufijo `-pause` y `-resume`. La longitud total del nombre debe ajustarse al tamaño máximo de un nombre de acción programada.

No puede pausar los siguientes tipos de clústeres:

- Clústeres clásicos de EC2.
- Los clústeres que no están activos, por ejemplo, un clúster que se está modificando actualmente.
- Clústeres de módulo de seguridad de hardware (HSM)
- Clústeres que tienen instantáneas automatizadas deshabilitadas.

Cuando decida pausar un clúster, tenga en cuenta lo siguiente:

- Las conexiones o consultas al clúster no están disponibles.
- No puede ver la información de supervisión de consultas de un clúster pausado en la consola de Amazon Redshift.
- No se puede modificar un clúster en pausa. Las acciones programadas en el clúster no se realizan. Estas incluyen la creación de instantáneas, el cambio de tamaño de los clústeres y las operaciones de mantenimiento de clústeres.
- Las métricas de hardware no se crean. Actualiza las alarmas de CloudWatch si tiene alarmas establecidas en las métricas que faltan.
- No puede copiar las instantáneas automatizadas más recientes de un clúster en pausa en instantáneas manuales.
- Mientras un clúster está en pausa, no se puede reanudar hasta que se complete la operación de pausa.
- Cuando pausa un clúster, la facturación se suspende. Sin embargo, la operación de pausa normalmente se completa en 15 minutos, en función del tamaño del clúster.
- Los registros de auditoría se archivan y no se restauran al reanudar.

Cuando reanude un clúster, tenga en cuenta lo siguiente:

- La versión del clúster reanudado se actualiza a la versión de mantenimiento en función de la ventana de mantenimiento del clúster.
- Si elimina la subred asociada a un clúster en pausa, es posible que tenga una red incompatible. En este caso, restaure el clúster a partir de la última instantánea.
- Si elimina una dirección IP elástica mientras el clúster está en pausa, se solicita una nueva dirección IP elástica.

- Si Amazon Redshift no puede reanudar el clúster con su elastic network interface anterior, Amazon Redshift intenta asignar una nueva.
- Cuando se reanuda un clúster, las direcciones IP de los nodos pueden cambiar. Es posible que tenga que actualizar la configuración de la VPC para admitir estas nuevas direcciones IP para características como COPY desde Secure Shell (SSH) o COPY desde Amazon EMR.
- Si intenta reanudar un clúster que no está en pausa, la operación de reanudación devuelve un error. Si la operación de reanudación forma parte de una acción programada, modifique o elimine la acción programada para evitar errores futuros.
- En función del tamaño del clúster, puede tardar varios minutos en reanudar un clúster antes de que se puedan procesar las consultas. Además, el rendimiento de la consulta puede verse afectado durante algún período de tiempo mientras el clúster se vuelve a hidratar después de que se complete la reanudación.

Cambio de nombre de los clústeres

Puede cambiar el nombre de un clúster si desea que el clúster utilice un nombre diferente. Como el punto de enlace del clúster incluye el nombre del clúster (lo que también se conoce como identificador del clúster), el punto de enlace cambia y pasa a utilizar el nombre nuevo una vez que termina el cambio de nombre. Por ejemplo, si tiene un clúster denominado `examplecluster` y le cambia el nombre por `newcluster`, el punto de enlace pasa a utilizar el identificador `newcluster`. Se debe actualizar cualquier aplicación que se conecte al clúster con el nuevo punto de enlace.

Puede cambiar el nombre de un clúster si desea cambiar el clúster con el que se conectan sus aplicaciones sin tener que cambiar el punto de enlace en esas aplicaciones. En este caso, primero debe cambiar el nombre del clúster original y, luego, cambiar el del segundo clúster para volver a utilizar el nombre del clúster original antes del cambio. Es necesario hacer esto porque el identificador de clúster debe ser único dentro de su cuenta y región, por lo que el clúster original y el segundo clúster no pueden tener el mismo nombre. Si no desea cambiar las propiedades de conexión de ninguna de las aplicaciones dependientes, puede hacerlo restaurando el clúster desde una instantánea.

Note

Si elimina el clúster original, tendrá que eliminar todas las snapshots no deseadas del clúster.

Cuando cambia el nombre de un clúster, el estado del clúster cambia a `renaming` hasta que termina el proceso. El nombre del DNS anterior que utilizaba el clúster se elimina de inmediato, si bien puede quedar almacenado en caché por varios minutos. El nuevo nombre del DNS del clúster que fue renombrado se efectiviza, aproximadamente, a los 10 minutos. El clúster renombrado estará disponible una vez que se efectiviza el nombre nuevo. Se reiniciará el clúster y se perderá cualquier conexión establecida con el clúster. Después que se completa el proceso, el punto de enlace pasará a utilizar el nombre nuevo. Por este motivo, debe detener la ejecución de consultas antes de comenzar con el cambio de nombre y las debe reiniciar una vez que termina con el cambio.

Las snapshots del clúster quedan almacenadas y todas las snapshots asociadas con el clúster quedan asociadas con ese clúster después de que se le cambia el nombre. Por ejemplo, suponga que tiene un clúster que sirve a su base de datos de producción y que ese clúster tiene varias instantáneas. Si cambia el nombre del clúster y, a continuación, lo reemplaza en el entorno de producción por una instantánea, el clúster que renombró sigue teniendo esas instantáneas asociadas a él.

Las alarmas de Amazon CloudWatch y las notificaciones de eventos de Amazon Simple Notification Service (Amazon SNS) están asociadas al nombre del clúster. Si cambia el nombre del clúster, deberá actualizar estos otros elementos asociados como corresponda. Puede actualizar las alarmas de CloudWatch en la consola de CloudWatch y puede actualizar las notificaciones de eventos de Amazon SNS en la consola de Amazon Redshift en la `EventosPanel` de. La carga y los datos de consulta del clúster muestran los datos antes y después del cambio de nombre. Sin embargo, los datos de rendimiento se reinician una vez que termina el proceso de cambio de nombre.

Para obtener más información, consulte [Modificación de un clúster](#) (p. 59).

Cierre y eliminación de clústeres

Puede cerrar su clúster sin desea que deje de funcionar y generar cargos. Cuando lo cierra, puede crear una snapshot final. Si crea una snapshot final, Amazon Redshift creará una snapshot manual de su clúster antes de cerrarlo. Luego, puede restaurar la snapshot si desea reanudar la ejecución del clúster y la consulta de datos.

Si ya no necesita su clúster ni los datos de este, puede cerrarlo sin crear una snapshot final. En este caso, el clúster y los datos se eliminan de manera permanente. Para obtener más información acerca del cierre y la eliminación de clústeres, consulte [Eliminación de un clúster](#) (p. 61).

Independientemente de que cierre su clúster con una snapshot manual final o no, todas las snapshots automatizadas asociadas con el clúster se eliminarán después de que se cierre el clúster. Se conservará toda snapshot manual asociada con el clúster. Cualquier instantánea manual que se conserve, incluida la instantánea final opcional, tendrá la tarifa de almacenamiento de Amazon Simple Storage Service si no hay ningún otro clúster funcionando en el momento en que se cierre el clúster o si se supera la capacidad de almacenamiento gratuito disponible que se proporciona para ejecutar los clústeres de Amazon Redshift. Para obtener más información sobre los cargos de almacenamiento de las instantáneas, consulte la [Página Precios de Amazon Redshift](#).

Trabajo con AQUA (Advanced Query Accelerator)

AQUA (Advanced Query Accelerator) es un acelerador de consultas de análisis para Amazon Redshift que utiliza hardware de diseño personalizado para acelerar las consultas que analizan grandes conjuntos de datos.

AQUA es una adición rentable al almacenamiento administrado por Amazon RedShift que está optimizado para obtener acceso seguro, transaccional y multiinquilino y consultas analíticas de alto rendimiento. Utiliza elementos de almacenamiento de estado sólido de memoria rápida no volátil (NVMe) de alta velocidad y aceleración basada en Nitro para la compresión y el cifrado. Utiliza aceleración basada en una matriz de computación programable en campo (FPGA) para empujar la mayor cantidad posible de computación en la capa de almacenamiento. Estos componentes están conectados entre sí de una manera única, lo que permite escanear datos sin utilizar una CPU tradicional. Al mismo tiempo, estos componentes permiten agregar resultados intermedios en la memoria de alta velocidad. AQUA es una caché de datos y mantiene conexiones de alta velocidad al almacenamiento administrado por Redshift.

No es necesario cambiar las bases de datos o aplicaciones para utilizar AQUA. Amazon Redshift identifica las partes de análisis de las consultas que pueden beneficiarse de la aceleración y las envía a AQUA para su procesamiento. AQUA optimiza automáticamente el rendimiento de las consultas en subconjuntos de datos que requieren análisis extensos, filtros y agregación. Con este enfoque, puede usar AQUA para ejecutar consultas que analizan, filtran y agregan datasets grandes. AQUA sobresale en las consultas que requieren análisis intensivos de procesamiento, filtros y agregación, como las que contienen predicados LIKE y SIMILAR TO.

AQUA admite la autenticación, el cifrado, el aislamiento y el cumplimiento normativo para mantener sus datos en reposo y los datos en tránsito seguros. Para obtener más información acerca de la seguridad de datos y AQUA, consulte lo siguiente:

- [Protección de datos en Amazon Redshift](#) (p. 284)
- [Cifrado en reposo](#) (p. 285)
- [Cifrado en tránsito](#) (p. 301)

Para obtener más información acerca de AQUA, consulte [¿Cuándo utiliza Amazon Redshift AQUA para ejecutar consultas?](#) (p. 35)

AQUA está disponible en clústeres con tipos de nodos `ra3.16xlarge` y `ra3.4xlarge`.

Aqua está disponible con la versión 1.0.24421 o posteriores en la siguiente AWS Regiones de:

- Región de EE.UU. Este (Norte de Virginia) (`us-east-1`)
- Región de EE.UU. Este (Ohio) (`us-east-2`)
- Región de EE.UU. Oeste (Oregón) (`us-west-2`)
- Región de Asia Pacífico (Singapur) (`ap-southeast-1`)
- Región de Asia Pacífico (Sídney) (`ap-southeast-2`)
- Región de Asia Pacífico (Tokio) (`ap-northeast-1`)
- Región de Europa (Fráncfort) (`eu-central-1`)
- Región de Europa (Irlanda) (`eu-west-1`)

Puede activar y gestionar clústeres de AQUA para Amazon Redshift en la consola de Amazon Redshift, con la AWS CLI o con las operaciones de la API de Amazon Redshift. Puede hacerlo cuando cree un clúster, restaure un clúster desde una instantánea o modifique un clúster existente. Cuando active un clúster existente, asegúrese de reiniciar el clúster para que el cambio surta efecto.

Para activar AQUA en la consola de Amazon Redshift, vaya al clúster y elija Configuración de AQUA: para Actions. Para ver una configuración AQUA definida previamente para el clúster, vaya al clúster y consulte la Información general sección, AQUA Información de.

Al configurar AQUA, tiene las siguientes opciones:

- Activar— Usted elige activar AQUA. AQUA solo se puede activar en ciertas AWS Regiones de y para los tipos de nodos `ra3.4xlarge` y `ra3.16xlarge`.
- Desactivación de— Usted elige no activar AQUA.
- Automático— Amazon Redshift determina si se va a utilizar AQUA. Esta es la opción predeterminada. Actualmente, AQUA no se activa con esta opción, pero este comportamiento está sujeto a cambios.

También puede activar AQUA durante la sesión. Para obtener más información, consulte [activate_aqua](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Gestión de AQUA mediante la AWS CLI

Puede utilizar la siguiente AWS CLI para activar y gestionar AQUA. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

- [create-cluster](#)
- [restore-from-cluster-snapshot](#)
- [modificar-aqua-configuración](#)

Gestión de AQUA mediante las operaciones de la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para activar y administrar AQUA. Para obtener más información, consulte la Referencia de la API de Amazon Redshift.

- [CreateCluster](#)
- [RestoreFromClusterSnapshot](#)

- [Modificación de aquaConfiguración](#)

¿Cuándo utiliza Amazon Redshift AQUA para ejecutar consultas?

Para cada consulta que explora una tabla, Amazon Redshift determina si la operación de análisis se envía a AQUA o se ejecuta localmente en el clúster de Amazon Redshift. Las operaciones de escaneo y agregación se envían a AQUA cuando contienen al menos un predicado que contiene una expresión LIKE o SIMILAR TO que admite AQUA. Si se envía una operación de escaneo a AQUA, entonces toda la operación se ejecuta en AQUA (no sólo el procesamiento LIKE o SIMILAR TO).

Por ejemplo, la siguiente consulta incluye los predicados `str1 LIKE 'a%'` y `num1 > 10` que se envían a AQUA.

```
select num2 from tbl where str1 LIKE 'a%' and num1 > 10 GROUP BY num2;
```

En este caso, AQUA escanea la tabla `tbl`, filtra por los predicados, agrupa los resultados por `num2` y devuelve los resultados a Amazon Redshift.

En el siguiente ejemplo, Amazon Redshift determina qué partes de la consulta se ejecutan mejor en AQUA y cuáles se ejecutan localmente en el clúster de Amazon Redshift. En este caso, hay un predicado LIKE en `customer_name` que se utiliza para filtrar las filas devueltas. La operación de análisis se envía a AQUA para ejecutar esa parte de la consulta. Amazon Redshift solo recibe los resultados del análisis, que Amazon Redshift utiliza para realizar una unión localmente y completar la consulta.

```
select c.customer_name, p.prod_name, sum(revenue)
from orders o
  join customers c ON c.id = o.customer_id
  join products p ON p.id = o.product_id
where c.customer_name LIKE '%Amazon%Web%'
order by sum(revenue);
```

Para obtener más información sobre LIKE y SIMILAR TO, consulte [LIKE y SIMILAR](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Consideraciones sobre AQUA

Actualmente AQUA no admite los siguientes tipos de consultas SQL. Las consultas que las incluyen se ejecutan localmente en el clúster de Amazon Redshift.

- Consultas que realizan escrituras, como INSERT, UPDATE, DELETE, CREATE TABLE AS, COPY y DESCARGA. Para obtener más información, consulte [Comandos SQL](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.
- SELECT consultas sin un predicado, por ejemplo el siguiente.

```
select * from tbl1
```

- Funciones definidas por el usuario (UDF) de Python en los análisis, incluidos los análisis de vistas complejas que se definen mediante UDF de Python.
- Consultas que utilizan los siguientes metacaracteres en predicados LIKE y SIMILAR TO:
 - Un literal de expresión regular no constante en una expresión LIKE.
 - Cualquiera de dos alternativas, por ejemplo la siguiente.

```
SIMILAR TO '%(cat|dog)%'
```

- Varias instancias de caracteres comodín de un solo carácter en columnas VARCHAR, por ejemplo, las siguientes.

```
SIMILAR TO 'ab.cd.ef'
```

- Secuencia de escape Unicode, caracteres hexagonales y octal-caracteres en la cadena de coincidencia, por ejemplo el siguiente.

```
SIMILAR TO '%ab\uc382'
```

```
SIMILAR TO '%ab\U0000c382'
```

```
SIMILAR TO '%ab\x88'
```

```
SIMILAR TO '%ab\127'
```

- Metacaracteres de repetición como «*», «+», «?», {m, n} aplicado en un patrón dentro de () y en caracteres multibyte, por ejemplo el siguiente.

```
SIMILAR TO 'abc(def)*'
```

```
SIMILAR TO 'abc#+'
```

- Caracteres multibyte dentro de una expresión de corchete [...], por ejemplo lo siguiente.

```
SIMILAR TO 'abc[#de]'.
```

- Consultas donde [Funciones de cadena](#), como INFERIOR, UPER, IZQUIERDA, DERECHA, se aplican a la salida de un escaneo LIKE o SIMILAR TO Por ejemplo, el siguiente extracto muestra una función LOWER.

```
LOWER(a) LIKE "%cat%"
```

En su lugar, intente reescribir la consulta para utilizar ILIKE insensible a mayúsculas y minúsculas sin LOWER

```
ILIKE "%cat%"
```

Cómo determinar si se utilizó AQUA

El siguiente SQL muestra segmentos de ejecución de consultas desde [SVL_QUERY_SUMMARY](#) que se ejecutó en AQUA.

```
select * from svl_query_summary where label ~ 'Aqua' limit 100;
```

Si tiene acceso de superusuario, también puede unirse a la [STL_QUERY](#) y [STL_QUERYTEXT](#) para ver las sentencias SQL que corresponden a las consultas ejecutadas por AQUA. El plan de explicación generado por la instrucción EXPLAIN no muestra si una consulta utilizó AQUA.

Administración de los límites de uso en Amazon Redshift

Puede definir límites para monitorear y controlar el uso y el costo asociado de algunas características de Amazon Redshift. Puede crear límites de uso diarios, semanales y mensuales, y definir acciones que realizará Amazon Redshift automáticamente si se alcanzan esos límites. Las acciones pueden ser, por ejemplo, incluir un evento en una tabla del sistema para registrar cualquier uso que exceda los límites definidos. Otras posibles acciones pueden ser el envío de alertas con Amazon SNS y Amazon CloudWatch para informar a un administrador y la desactivación de cualquier uso posterior para controlar los costos.

Puede definir límites de uso en cada clúster. Una vez que se ha creado el clúster, puede definir límites de uso para las siguientes características:

- Amazon Redshift Spectrum
- Ajustes de simultaneidad de Amazon Redshift

Los límites de uso están disponibles con la versión 1.0.14677 o posteriores en laAWSRegiones en las que están disponibles Amazon Redshift Spectrum y Amazon Redshift Concurrency Scaling.

Un límite de Redshift Spectrum especifica el umbral de la cantidad total de datos analizados en incrementos de 1 TB. Los límites de escalado de simultaneidad especifican el umbral del total de tiempo invertido en el escalado de simultaneidad en incrementos de 1 minuto. Se puede establecer un límite diario, semanal o mensual (se utiliza el formato UTC para determinar el inicio y el final del período). Si crea un límite en mitad de un período, dicho límite se medirá desde ese punto hasta el final del período. Por ejemplo, si crea un límite mensual el 15 de marzo, el primer período mensual se medirá desde el 15 hasta el 31 de marzo.

Puede definir varios límites de uso para cada característica. Cada límite puede tener una acción diferente. Entre las posibles acciones se incluyen las siguientes:

- Registrar la tabla del sistema— Esta es la acción predeterminada. La información se registra en la tabla `STL_USAGE_CONTROL`. Este registro es útil para poder evaluar el uso pasado y decidir los límites de uso futuros. Para obtener más información sobre el contenido que se registra, consulte [STL_USAGE_CONTROL](#) en laGuía para desarrolladores de bases de datos Amazon Redshift.
- Alerta: Amazon Redshift emite métricas de CloudWatch para el uso disponible y consumido. Puede definir hasta tres límites de uso para cada característica. Si habilita la acción de alerta mediante la consola de Amazon Redshift, se creará automáticamente una alarma de CloudWatch en estas métricas. Si lo desea, puede asociar una suscripción de Amazon SNS a esa alarma. Si utiliza unAWS CLI, si lo desea, asegúrese de crear la alarma CloudWatch manualmente. Cuando se alcance el umbral, los eventos también se registrarán en una tabla del sistema.
- Deshabilitar característica: cuando se alcanza el umbral, Amazon Redshift deshabilita la función hasta que se actualice la cuota para el próximo período de tiempo (diario, semanal o mensual). Solo puede haber un límite en cada característica con la acción de desactivación. Los eventos también se registran en una tabla del sistema. Además, se pueden emitir alertas.

Los límites de uso se mantienen hasta que se elimina la propia definición del límite de uso o el clúster.

Puede definir y administrar los límites de uso con la nueva consola de Amazon Redshift, laAWS CLI o con las operaciones de la API de Amazon Redshift. Para definir un límite en la consola de Amazon Redshift, vaya al clúster y elijaConfigurar el límite de uso: paraActions. Para ver los límites de uso definidos previamente para el clúster, vaya al clúster, elija la opciónMantenimientoPestaña, Límites de uso sección. Para ver el uso disponible y consumido del clúster, desplácese hasta el clúster. Elija el iconoRendimiento del clústerPara ver los gráficos sobre el uso que se ha consumido en una característica.

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar los límites de uso. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

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

Puede utilizar las siguientes operaciones de la API de Amazon Redshift de para administrar los límites de uso. Para obtener más información, consulte laReferencia de la API de Amazon Redshift.

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

Vea el siguiente vídeo para obtener información sobre cómo crear y monitorear límites de uso mediante la consola de Amazon Redshift: [Controles de costes para Amazon Redshift Spectrum y escalado de simultaneidad](#).

Gestión de la reubicación de clústeres en Amazon Redshift

Mediante el uso dereubicaciónen Amazon Redshift, permite que Amazon Redshift mueva un clúster a otra zona de disponibilidad (AZ) sin pérdida de datos ni cambios en las aplicaciones. Con la reubicación, puede continuar las operaciones cuando hay una interrupción del servicio en el clúster con un impacto mínimo.

Cuando la reubicación de clústeres está habilitada, Amazon Redshift puede optar por reubicar clústeres en algunas situaciones. En particular, esto sucede cuando los problemas de la zona de disponibilidad actual impiden el funcionamiento óptimo del clúster o para mejorar la disponibilidad del servicio. También puede invocar la función de reubicación en los casos en que las restricciones de recursos en una zona de disponibilidad determinada interrumpen las operaciones del clúster. Un ejemplo es la capacidad de reanudar o cambiar el tamaño de un clúster. Amazon Redshift ofrece la función de reubicación sin cargo adicional.

Cuando un clúster de Amazon Redshift se reubica en una nueva zona de disponibilidad, el nuevo clúster tiene el mismo extremo que el clúster original. Sus aplicaciones pueden volver a conectarse al endpoint y continuar las operaciones sin modificaciones ni pérdida de datos. Sin embargo, es posible que la reubicación no siempre sea posible debido a las limitaciones de recursos potenciales en una zona de disponibilidad determinada.

La reubicación de clústeres de Amazon Redshift solo se admite para los tipos de instancias RA3, como `ra3.16xlarge`, `ra3.4xlarge` y `ra3.xplus`. Los tipos de instancias RA3 utilizan Redshift Managed Storage (RMS) como capa de almacenamiento duradera. La copia más reciente de los datos de un clúster siempre está disponible en otras zonas de disponibilidad de unAWSRegión . En otras palabras, puede trasladar un clúster de Amazon Redshift a otra zona de disponibilidad sin pérdida de datos.

Cuando habilita el clúster para la reubicación, Amazon Redshift migra el clúster para que esté detrás de un proxy. Esto ayuda a implementar el acceso independiente de la ubicación a los recursos informáticos de un clúster. La migración hace que se reinicie el clúster. Cuando un clúster se reubica en otra zona de disponibilidad, se produce una interrupción mientras el nuevo clúster se vuelve a conectar en la nueva zona de disponibilidad. Sin embargo, no es necesario realizar ningún cambio en las aplicaciones porque el

extremo del clúster permanece sin cambios incluso después de que el clúster se reubica en la nueva zona de disponibilidad.

Si habilita la reubicación y utiliza actualmente la dirección IP del nodo directivo para acceder al clúster, asegúrese de cambiar ese acceso. En lugar de ello, utilice la dirección IP asociada al punto de enlace de nube privada virtual (VPC). Para buscar esta dirección IP del clúster, busque y use el extremo de VPC en el [Redes y seguridad](#) Sección de la página de detalles del clúster. Para obtener más detalles sobre el punto de enlace de VPC, inicie sesión en la consola de Amazon VPC.

También puede utilizar la [AWS Command Line Interface \(AWS CLI\)](#) comando de `describe-vpc-endpoints` Para obtener la elastic network interface asociada al punto de enlace. Puede utilizar `describe-network-interfaces` para obtener la dirección IP asociada. Para obtener más información sobre Amazon Redshift AWS CLI consulte [Comandos disponibles](#) en la [AWS CLI Referencia de comandos](#) de la.

Habilitación de la reubicación

Puede habilitar y gestionar la reubicación de clústeres desde la consola de Amazon Redshift, [AWS CLI](#) y la [API de Amazon Redshift](#).

Para habilitar la reubicación del clúster, defina un grupo de subred que incluya varias zonas de disponibilidad. Si Amazon Redshift identifica más de una zona de disponibilidad accesible, Amazon Redshift elige automáticamente de la lista de zonas de disponibilidad accesibles para reubicar el clúster.

Una vez completada la reubicación, se utiliza el mismo extremo para acceder al clúster. Amazon Redshift elimina los recursos informáticos del clúster original y los devuelve al fondo de recursos.

Limitations

Al utilizar la reubicación de Amazon Redshift, tenga en cuenta las siguientes limitaciones:

- Es posible que la reubicación del clúster no sea posible en todos los escenarios debido a posibles limitaciones de recursos en una zona de disponibilidad determinada. Si esto sucede, Amazon Redshift no cambia el clúster original.
- La reubicación no es compatible con las familias de productos DC1, DC2 o de instancias DS2.
- La reubicación no está disponible para un clúster de Amazon Redshift de acceso público.
- No se puede realizar una reubicación a través de [AWS Regiones](#) de.
- Puede habilitar la reubicación sólo para un clúster que utilice la configuración de puerto predeterminada (5439). De lo contrario, la activación de la reubicación falla.
- Si ha habilitado la reubicación correctamente y posteriormente intenta modificar la configuración predeterminada del puerto, se produce un error en la operación de modificación.

Administración de la reubicación mediante la consola

Puede gestionar la configuración de la reubicación de clústeres mediante la consola de Amazon Redshift.

Habilitación de la reubicación al crear un clúster

Utilice el siguiente procedimiento para habilitar la reubicación al crear un nuevo clúster.

Para habilitar la reubicación de un nuevo clúster

1. Inicie sesión en la [AWS Management Console](#) y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.

2. En el panel de navegación, seleccione **CLÚSTERES DE**.
3. Seleccione **Crear un clúster** Para crear un nuevo clúster. Para obtener más información acerca de cómo crear un clúster, consulte [Crear un clúster de Amazon Redshift](#) in **Inicie sesión en Amazon Redshift**.
4. **UNDER** **Copia de seguridad**, para **Reubicación del clúster**, elija **Habilitar**. La reubicación está deshabilitado de forma predeterminada.
5. **UNDER** **Redes y seguridad**, para **Publicly accessible**, acepte el valor predeterminado **Deshabilitar**. Si elige **Habilitar** Amazon Redshift devuelve un error.
6. Elija **Create cluster**.

Modificación de la reubicación de un clúster existente

Utilice el siguiente procedimiento para cambiar la configuración de reubicación de un clúster existente.

Para modificar la configuración de reubicación de un clúster existente

1. Inicie sesión en la **AWS Management Console** y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione **CLÚSTERES DE**. Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Seleccione el nombre del clúster que desea modificar de la lista. Aparecerá la página de detalles del clúster.
4. Elija el icono **Mantenimiento** y, a continuación, en la pestaña **Detalles Backup** sección, elija **Editar**.
5. **UNDER** **Copia de seguridad**, elija **Habilitar**. La reubicación está deshabilitado de forma predeterminada.
6. Elija el icono **Propiedades** y, a continuación, en la pestaña **Redes y seguridad** asegúrate de elegir **Deshabilitar** para la **Publicly accessible** opción.
7. En el navegador **Redes y seguridad**, asegúrese de elegir **Deshabilitar** para la **Publicly accessible** opción.
8. Elija **Modify Cluster** (Modificar clúster).

Reubicación de un clúster

Utilice el siguiente procedimiento para reubicar manualmente un clúster a otra zona de disponibilidad. Esto resulta especialmente útil cuando desea probar la configuración de red en zonas de disponibilidad secundarias o cuando se encuentra con restricciones de recursos en la zona de disponibilidad actual.

Para reubicar un clúster a otra zona de disponibilidad

1. Inicie sesión en la **AWS Management Console** y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione **CLÚSTERES DE**. Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Seleccione el nombre del clúster que desea mover de la lista. Aparecerá la página de detalles del clúster.
4. Para **Actions**, elija **Reubicar**. La **Reubicar clúster** aparecerá la página.
5. (Opcional) Elija una **Zona de disponibilidad**. Si no elige una zona de disponibilidad, Amazon Redshift elige una para usted.

Amazon Redshift inicia la reubicación y muestra el clúster como reubicación. Una vez finalizada la reubicación, el estado del clúster cambia a disponible.

Gestión de la reubicación mediante la CLI de Amazon Redshift

Puede administrar la configuración de la reubicación de clústeres mediante la herramienta AWS Interfaz de línea de comandos (CLI).

Con el **AWS CLI**, el siguiente comando de ejemplo crea un clúster de Amazon Redshift denominado **mycluster** que tiene habilitada la reubicación.

```
aws redshift create-cluster --cluster-identifier mycluster --number-of-nodes 2 --master-username adminuser --master-user-password TopSecret1 --node-type ra3.4xlarge --port 5439 --no-publicly-accessible --availability-zone-relocation
```

Si su clúster actual está utilizando un puerto diferente, debe modificarlo para usar 5439 antes de modificarlo para habilitar la reubicación. El siguiente comando de ejemplo modifica el puerto en caso de que el clúster no use 5439.

```
aws redshift modify-cluster --cluster-identifier mycluster --port 5439
```

El siguiente comando de ejemplo habilita el parámetro `availability-zone-relocation` en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone-relocation
```

El siguiente comando de ejemplo deshabilita el parámetro `availability-zone-relocation` en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --no-availability-zone-relocation
```

El siguiente comando de ejemplo invoca la reubicación en el clúster de Amazon Redshift.

```
aws redshift modify-cluster --cluster-identifier mycluster --availability-zone us-east-1b
```

Trabajar con terminales de VPC gestionados por Redshift en Amazon Redshift

De forma predeterminada, un clúster de Amazon Redshift está aprovisionado en una nube virtual privada (VPC). Se puede acceder a ella desde otra VPC o subred cuando se permite el acceso público o se configura una puerta de enlace a Internet, un dispositivo NAT o un **AWS Direct Connect** Conexión para enrutar el tráfico al clúster de. O puede acceder a un clúster configurando un endpoint VPC administrado por RedShift (equipado con **AWS PrivateLink**).

Configurar un extremo de VPC administrado por RedShift como una conexión privada entre una VPC que contiene un clúster y una VPC que ejecuta una herramienta cliente. Si el clúster está en otra cuenta, el propietario de la cuenta (otorgante) debe conceder acceso a la cuenta (otorgante) que desea establecer una conexión. Con este enfoque, puede acceder al almacén de datos sin usar direcciones IP públicas ni enrutar el tráfico a través de Internet.

En los siguientes escenarios se describen razones comunes para permitir el acceso a un clúster mediante un extremo VPC administrado por RedShift:

- AWS La cuenta A quiere permitir una VPC en AWS B para tener acceso a un clúster.
- AWS La cuenta A quiere permitir una VPC que también está en AWS cuenta A para tener acceso a un clúster.
- AWS La cuenta A quiere permitir una subred diferente en la VPC del clúster dentro de AWS cuenta A para tener acceso a un clúster.

El flujo de trabajo general para configurar un extremo VPC administrado por RedShift para acceder a un clúster en otra cuenta es el siguiente:

1. La cuenta de propietario del clúster concede autorización de acceso a otra cuenta y especifica la propiedad AWS ID de cuenta e identificador de VPC (o todas las VPC) del beneficiario.
2. Se notifica a la cuenta del beneficiario que tiene permiso para crear un extremo VPC administrado por RedShift.
3. La cuenta del beneficiario crea un endpoint VPC administrado por RedShift.
4. La cuenta del beneficiario ahora puede acceder al clúster de la cuenta de propietario mediante el extremo de VPC administrado por RedShift.

Puede gestionar este proceso con la consola de Amazon Redshift, el AWS CLI o la API de Amazon Redshift.

Consideraciones al usar endpoints VPC administrados por RedShift

Cuando utilice los puntos de enlace de VPC administrados por Redshift, tenga en cuenta lo siguiente:

- Asegúrese de que el clúster al que se accede es un tipo de nodo RA3.
- Asegúrese de que el clúster de acceso tiene activada la reubicación del clúster. Para obtener información acerca de los requisitos para activar la reubicación de clústeres, consulte [Gestión de la reubicación de clústeres en Amazon Redshift \(p. 38\)](#).
- Asegúrese de que el clúster de acceso esté disponible a través del puerto 5439.
- Puede modificar los grupos de seguridad de VPC asociados a un extremo de VPC administrado por RedShift existente. Para modificar otros parámetros de, elimine el punto de enlace de VPC administrado por RedShift y cree uno nuevo.
- El número de endpoints VPC administrados por RedShift que puede crear está limitado a la cuota de endpoints de VPC.
- Los endpoints VPC administrados por RedShift no son accesibles desde Internet. Sólo se puede acceder a un extremo de VPC administrado por RedShift dentro de la VPC en la que se aprovisiona el endpoint o en cualquier VPC con la VPC donde se aprovisiona el endpoint según lo permitan las tablas de rutas y los grupos de seguridad.
- No puede utilizar la consola de Amazon VPC para administrar los puntos de enlace de VPC administrados por RedShift.

Para obtener información sobre cuotas y restricciones de nomenclatura, consulte [Cuotas y límites de Amazon Redshift \(p. 494\)](#).

Para obtener información sobre precios, consulte [precios de AWS PrivateLink](#).

Administración de puntos finales de VPC gestionados por RedShift mediante la consola de Amazon Redshift

Puede configurar el uso de extremos de VPC gestionados por RedShift mediante la consola de Amazon Redshift.

Concesión de acceso a un clúster

Si la VPC a la que desea acceder a su clúster está en otroAWS, asegúrate de autorizarla desde la cuenta del propietario (del otorgante).

Para permitir una VPC en otroAWS para tener acceso a su clúster

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación de, seleccioneCLÚSTERES DE.
3. Para el clúster al que desea permitir acceso, consulte los detalles del clúster seleccionando el nombre del clúster. Elija el iconoPropiedadesdel clúster.

LaCuentas concedidasmuestra las cuentas y las VPC correspondientes que tienen acceso al clúster.

4. SeleccionarConcesión de acceso para mostrar un formulario para introducirInformación del beneficiarioPara añadir una cuenta.
5. ParaAWSID de cuenta de, ingrese el ID de la cuenta a la que está otorgando acceso. Puede conceder acceso a VPC específicas o a todas las VPC de la cuenta especificada.
6. SeleccionarConcesión de accesoPara conceder acceso a.

Creación de un endpoint VPC administrado por RedShift

Si posee un clúster o se le ha concedido acceso a él, puede crear un extremo VPC administrado por RedShift para el clúster.

Para crear un extremo VPC administrado por RedShift

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación de, seleccioneCONFIGURACIONES.

LaConfiguracionesmuestra los extremos de VPC administrados por RedShift que se han creado. Para ver los detalles de un extremo, elija su nombre.

3. SeleccionarCreación de un punto de enlace para mostrar un formulario para introducir información sobre el extremo que desea agregar.
4. Introduzca valores paraEndpoint name (Nombre del punto de enlace),AWSID de cuenta de,Identificador de clúster,Virtual private cloud (VPC) (Nube virtual privada (VPC)),Subnet groupy otras propiedades del endpoint.

El grupo de subredes deSubnet groupdefine las subredes y las direcciones IP en las que Amazon Redshift implementa el endpoint. Amazon Redshift elige una subred que tenga direcciones IP disponibles para la interfaz de red asociada al endpoint.

El grupo de seguridad opcional enGrupo de seguridaddefine los puertos, protocolos y fuentes para el tráfico entrante que está autorizando para el endpoint. Normalmente, permite el acceso al puerto 5439 al grupo de seguridad o al rango CIDR donde se ejecutan las cargas de trabajo.

5. SeleccionarCreación de un punto de enlacePara crear el punto de enlace.

Una vez creado el endpoint, puede acceder al clúster a través de la URL que se muestra enURL del punto de enlaceen la configuración del endpoint VPC administrado por RedShift.

Administración de endpoints VPC administrados por RedShift mediante elAWS CLI

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para trabajar con extremos de VPC administrados por RedShift. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

- [authorize-punto de enlace](#)
- [revoke-endpoint-access](#)
- [crear-endpoint-access](#)
- [modificar-endpoint-access](#)
- [eliminar-endpoint-access](#)
- [describe-endpoint-access](#)
- [describe-endpoint autorización-endpoint](#)

Gestión de endpoints VPC gestionados por Redshift mediante operaciones de la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para trabajar con extremos de VPC gestionados por RedShift. Para obtener más información, consulte laReferencia de la API de Amazon Redshift.

- [AuthorizeEndPointAccess](#)
- [RevokeEndPointAccess](#)
- [CreateEndPointAccess](#)
- [Modificar EndPointAccess](#)
- [DeleteEndPointAccess](#)
- [DescribeEndPointAccess](#)
- [DescribeEndPointAuthorization](#)

Administración de clústeres a través de la consola

Para crear, modificar, redimensionar, eliminar y reiniciar clústeres o hacer una copia de seguridad de ellos, utilice la herramientaClústeresen la consola de Amazon Redshift.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

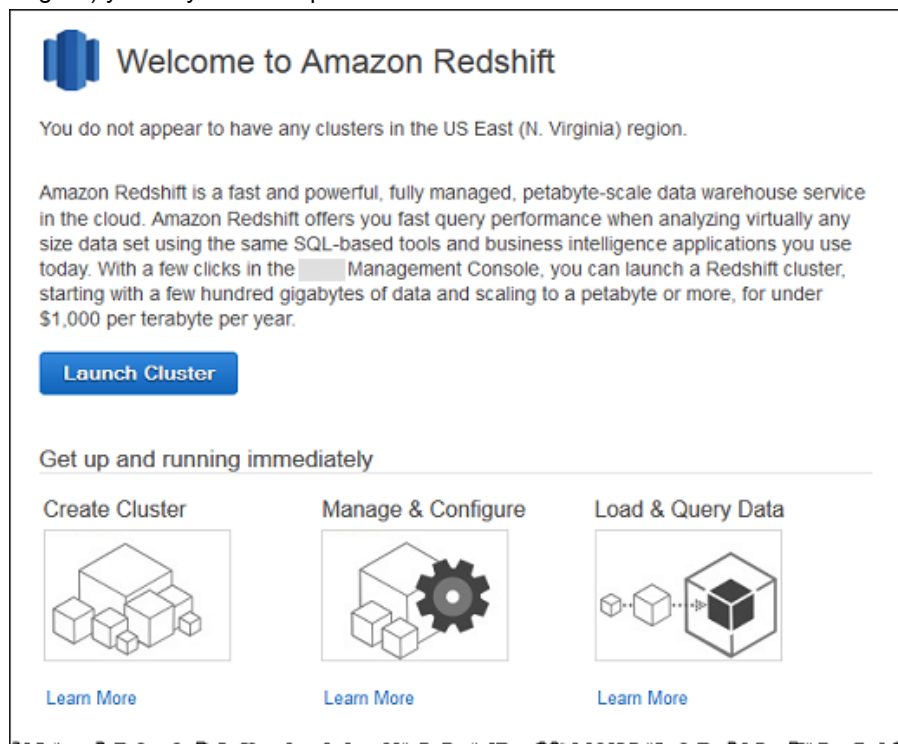
New console

Para ver clústeres

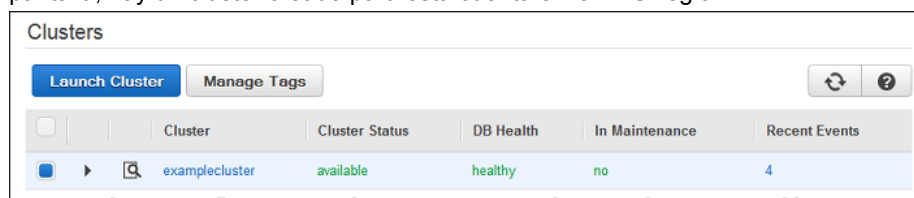
1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas. Si no tiene ningún clúster, seleccione Create cluster (Crear clúster) para crear uno.
3. Seleccione el nombre del clúster en la lista para ver más detalles sobre un clúster.

Consola original

Cuando no tiene ningún clúster en unaAWSRegión y abre el cuadro de diálogoClústeres, tiene la opción de iniciar un clúster. En la siguiente captura de pantalla, laAWSLa región es la región EE. UU. Este (Norte de Virginia) y no hay clústeres para esta cuenta.



Cuando tiene al menos un clúster en unaAWSRegión, laClústeresLa sección muestra un subconjunto de información acerca de todos los clústeres para la cuenta en esaAWSRegión . En la siguiente captura de pantalla, hay un clúster creado para esta cuenta en laAWSRegión .



Puede ampliar el clúster para ver más información acerca de este, como los detalles del punto de enlace, las propiedades del clúster y la base de datos, etiquetas, etc. En la siguiente captura de pantalla, examplecluster se expande para mostrar un resumen con información sobre el clúster.

Clusters

[Launch Cluster](#)
[Manage Tags](#)
[Manage IAM Roles](#)

	Cluster	Cluster Status	DB Health	In Ma
☐	examplecluster	available	healthy	no

Endpoint [examplecluster.cluster-xyz.us-west-1.redshift.amazonaws.com:5439 \(authorized \)](#)

Cluster Properties

Cluster Name	examplecluster
Node Type	dc1.large
Nodes	1
Zone	us-west-1a
Cluster Parameter Group	default.redshift-1.0 (in-sync)
Enhanced VPC Routing	Yes

Cluster Status

Cluster Status	available
Database Health	healthy
In Maintenance Mode	no
Parameter Group Apply Status	in sync
Pending Modified Values	None

Cluster Database Properties

Port	5439
Database Name	dev
Master Username	masteruser
Encrypted	No

Backup, Audit Logging, and Maintenance

Automated Snapshot Retention Period	35 days
Cross-Region Snapshots Enabled	No
Audit Logging Enabled	No
Maintenance Window	00:00-01:00 UTC
Allow Version Upgrade	No

Tags

You have not created any tags. Please add tags using the **Manage Tags** button above.

Temas

- [Creación de un clúster \(p. 47\)](#)
- [Modificación de un clúster \(p. 59\)](#)
- [Eliminación de un clúster \(p. 61\)](#)
- [Reinicio de un clúster \(p. 63\)](#)
- [Redimensionamiento de un clúster \(p. 64\)](#)
- [Actualizar la versión de lanzamiento de un clúster \(p. 66\)](#)
- [Obtención de información acerca de la configuración del clúster \(p. 67\)](#)
- [Obtención de información general acerca del estado del clúster \(p. 67\)](#)
- [Crear una instantánea de un clúster \(p. 69\)](#)
- [Crear o editar una alarma de espacio en disco \(p. 70\)](#)

- [Uso de los datos de rendimiento del clúster \(p. 71\)](#)

Creación de un clúster

Antes de crear un clúster, lea [Descripción general de los clústeres de Amazon Redshift \(p. 5\)](#) y [Clusters y nodos en Amazon Redshift \(p. 5\)](#).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Una forma de aprender más sobre la creación de clústeres es crear un clúster con la consola.

Pasos para crear un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES). Se enumeran los clústeres de su cuenta en la región de AWS actual. Se muestra en la lista un subconjunto de propiedades de cada clúster en columnas.
3. Seleccione Create cluster (Crear clúster) para crearlo.
4. Siga las instrucciones en la página de la consola para introducir las propiedades de la Cluster configuration (Configuración del clúster).

Elija uno de los siguientes métodos para ajustar el tamaño del clúster:

Note

En el siguiente paso se describe una consola de Amazon Redshift que se ejecuta en unAWSRegión compatible con tipos de nodo RA3. Para obtener una lista deAWSLas regiones que admiten tipos de nodo RA3, consulte[Información general sobre los tipos de nodo RA3](#)en laGuía de administración de clúster de Amazon Redshift.

- Si las recetasAWSLa región admite tipos de nodo RA3, elijaProducciónorPrueba gratuita para responder a la pregunta¿Para qué planeas usar este clúster?

Si su organización es elegible, es posible que pueda crear un clúster bajo el programa de prueba gratuita de Amazon Redshift. Para ello, elijaPrueba gratuita para crear una configuración con el tipo de nodo dc2.large. Para obtener más información sobre cómo elegir una versión de prueba gratuita, consulte.[Prueba gratuita de Amazon Redshift](#).

- Si no sabe cuál es el tamaño de su clúster, elijaAyúdeme a elegir. De este modo, se inicia una calculadora de tamaño que le hace preguntas sobre el tamaño y las características de consulta de los datos que planea almacenar en el almacén de datos.

Si conoce el tamaño requerido de su clúster (es decir, el tipo de nodo y el número de nodos), elijaYo elegiré. A continuación, elija la opciónTipo de nodoy número deNodospara ajustar el tamaño del clúster para obtener la prueba de concepto.

5. Siga las instrucciones en la página de la consola para introducir las propiedades de la Cluster configuration (Configuración del clúster).

Note

Si se encuentra detrás de un firewall, el puerto de la base de datos debe ser un puerto abierto que acepta conexiones entrantes.

6. (Opcional) Siga las instrucciones en la página de la consola para introducir las propiedades de Cluster permissions (Permisos del clúster). Proporcione permisos de clúster si su clúster necesita tener acceso a otros AWS, por ejemplo, para cargar datos desde Amazon S3.
7. Seleccione Create cluster (Crear clúster) para crearlo. El clúster tardará varios minutos antes de estar listo para su uso.

Configuraciones adicionales

Cuando cree un clúster, puede especificar propiedades adicionales para personalizarlo. Puede encontrar más información sobre algunas de estas propiedades en la siguiente lista.

Nube virtual privada (VPC)

Elija una VPC que tenga un grupo de subredes. Una vez creado el clúster, el grupo de subred no puede cambiarse.

Grupos de parámetros

Elija un grupo de parámetros para asociarlo al clúster. Si no lo elige, el clúster usará el grupo de parámetros predeterminado.

Cifrado

Elija si desea cifrar todos los datos dentro del clúster y sus instantáneas. Si deja el valor predeterminado, None (Ninguno), no se habilitará el cifrado. Si desea habilitar el cifrado, elija si desea utilizar AWS Key Management Service (AWS KMS) o un módulo de seguridad de hardware (HSM), y establezca la configuración correspondiente. Para obtener más información sobre el cifrado en Amazon Redshift, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

- KMS

Seleccione KMS si desea habilitar el cifrado y utilizar AWS KMS para administrar la clave de cifrado. En Master Key (Clave maestra), seleccione (default) aws/redshift para utilizar una clave maestra de cliente (CMK) predeterminada o para seleccionar otra clave de la cuenta de AWS.

Note

Si desea utilizar una clave de otra cuenta de AWS, seleccione Enter a key ARN (Escribir un ARN de clave) en Master Key (Clave maestra). A continuación, escriba el nombre de recurso de Amazon (ARN) de la clave que va a usar. Debe tener permisos para usar la clave. Para obtener más información sobre el acceso a claves en AWS KMS, consulte [Controlar el acceso a sus llaves](#) en la [AWS Key Management Service Guía para desarrolladores](#).

Para obtener más información acerca del uso de AWS KMS claves de cifrado en Amazon Redshift, consulte [Cifrado de base de datos de Amazon Redshift mediante AWS KMS \(p. 286\)](#).

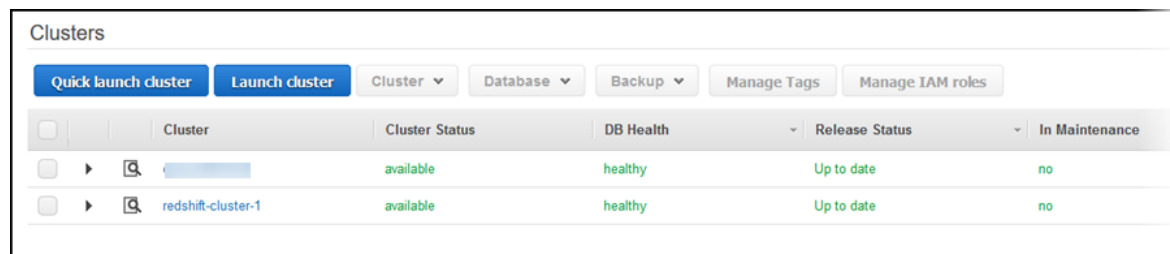
- HSM

Seleccione HSM si desea habilitar el cifrado y utilizar un módulo de seguridad de hardware (HSM) para administrar la clave de cifrado.

Si selecciona HSM, elija valores de HSM Connection (conexión de HSM) y HSM Client Certificate (Certificado de cliente de HSM). Estos valores se necesitan para que Amazon Redshift y el HSM formen una conexión confiable sobre la cual pueda pasar la clave del clúster. La conexión del HSM y el certificado de cliente se deben configurar en Amazon Redshift antes de lanzar un clúster. Para obtener más información acerca de cómo configurar las conexiones del HSM y los certificados de clientes, consulte [Cifrado para Amazon Redshift mediante módulos de seguridad de hardware \(p. 288\)](#).

Aparece una página de confirmación. El clúster tarda varios minutos en crearse. Seleccione Close (Cerrar) para regresar a la lista de clústeres.

5. En la página Clusters (Clústeres), seleccione el clúster que acaba de lanzar y revise la información de Cluster Status (Estado del clúster). Asegúrese de que el Cluster Status (Estado del clúster) se available (disponible) y de que Database Health (Estado de la base de datos) sea healthy (saludable) antes de intentar conectarse a la base de datos.



	Cluster	Cluster Status	DB Health	Release Status	In Maintenance
☐		available	healthy	Up to date	no
☐	redshift-cluster-1	available	healthy	Up to date	no

Creación de un clúster mediante un lanzamiento del clúster

Si ya es un usuario de Amazon Redshift existente de o desea personalizar su clúster, use el siguiente procedimiento para lanzar su clúster. Si es la primera vez que usa Amazon Redshift o solo necesita un clúster básico, consulte [Creación de un clúster mediante el lanzamiento rápido del clúster \(p. 49\)](#).

Para crear un clúster mediante un lanzamiento del clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. Seleccione Launch Cluster (Lanzar Clúster).
3. En la página Cluster Details (Detalles del clúster), especifique los valores de las siguientes opciones y seleccione Continue (Continuar).

Cluster Identifier (Identificador del clúster)

Escriba un nombre único para el clúster.

Los identificadores de clúster deben cumplir las condiciones a continuación:

- Deben contener de 1 a 63 caracteres alfanuméricos o guiones.
- Los caracteres alfanuméricos deben ir en minúscula.
- El primer carácter debe ser una letra.
- No pueden incluir dos guiones consecutivos ni acabar con guion.
- Deben ser únicos para todos los clústeres de una cuenta de AWS.

Database Name (Nombre de base de datos)

Escriba un nombre si desea crear una base de datos con un nombre personalizado (por ejemplo, **mydb**). Este campo es opcional. Si no se especifica un nombre personalizado, se crea una base de datos con el nombre predeterminado dev para el clúster.

Los nombres de base de datos deben cumplir las condiciones siguientes:

- Deben contener de 1 a 64 caracteres alfanuméricos.
- Deben contener letras en minúscula únicamente.
- Un nombre de base de datos no puede ser una palabra reservada. Para obtener más información, consulte [Palabras reservadas](#) en la Guía para desarrolladores de bases de datos.

Database Port (Puerto de base de datos)

Escriba un número de puerto a través del cual planea conectarse desde las aplicaciones cliente a la base de datos. El número de puerto se debe incluir en la cadena de conexión cuando abra conexiones JDBC u ODBC a las bases de datos en el clúster.

El número de puerto debe cumplir las condiciones siguientes:

- Debe contener caracteres numéricos únicamente.
- Debe caer en el rango 1150—65535. El puerto predeterminado es 5439.
- Si está detrás de un firewall, debe especificar un puerto abierto que acepta conexiones entrantes.

Master User Name (Nombre de usuario maestro)

Escriba un nombre de cuenta para el usuario maestro de la base de datos.

Los nombres de usuario maestro deben cumplir las condiciones siguientes:

- Deben contener de 1 a 128 caracteres alfanuméricos.
- El primer carácter debe ser una letra.
- Un nombre de usuario maestro no puede ser una palabra reservada. Para obtener más información, consulte [Palabras reservadas](#) en la Guía para desarrolladores de bases de datos.

Master User Password (Contraseña de usuario maestro) y Confirm Password (Confirmar contraseña)

Escriba una contraseña para la cuenta del usuario maestro y, luego, vuelva a escribir la contraseña para confirmarla.

Puede usar cualquier carácter ASCII con códigos ASCII 33—126, excepto '(comillas sencillas), \"(comillas dobles), \\/o @.

En la siguiente captura de pantalla, `examplecluster` es el identificador de clúster, no se especifica nombre personalizado de base de datos, 5439 es el puerto y `masteruser` es el nombre del usuario maestro.

CLUSTER DETAILS NODE CONFIGURATION ADDITIONAL CONFIGURATION REVIEW

Provide the details of your cluster. Fields marked with * are required.

Cluster Identifier* This is the unique key that identifies a cluster. This parameter is stored as a lowercase string. (e.g. my-dw-instance)

Database Name

Database Port* Optional. A default database named dev is created for the cluster. Optionally, specify a custom database name (e.g. mydb) to create an additional database.

Master User Name* Port number on which the database accepts connections.

Master User Password* Name of master user for your cluster. (e.g.)

Confirm Password* Password must contain 8 to 64 printable ASCII characters excluding: /, ", ', \, and @. It must contain 1 uppercase letter, 1 lowercase letter, and 1 number.

Confirm Master User Password.

- En la página Node Configuration (Configuración del nodo), especifique los valores de las siguientes opciones y seleccione Continue (Continuar).

Node Type

Elija un tipo de nodo. Cuando selecciona un tipo de nodo, la página muestra información que corresponde al tipo de nodo seleccionado, como CPU, Memory (Memoria), Storage (Almacenamiento) e I/O Performance (Rendimiento de E/S).

Cluster Type (Tipo de clúster)

Elija un tipo de clúster. Cuando lo haga, aparece la cantidad máxima de nodos de computación para el tipo de nodo y clúster seleccionado en el cuadro Maximum (Máximo), y el mínimo, en el cuadro Minimum (Mínimo).

Si selecciona Single Node (Un solo nodo), tendrá un nodo que comparte la funcionalidad principal y de computación.

Si selecciona Multi Node (Varios nodos), especifique la cantidad de nodos de computación que desea para el clúster en Number of Compute Nodes (Número de nodos de computación).

En la siguiente captura de pantalla, se ha seleccionado el tipo de nodo dc1.large para un clúster de tipo Multi Node (Varios nodos) que tiene dos nodos de computación.

The screenshot shows the 'Additional Configuration' page in the Amazon Redshift console. It includes the following settings:

- Node Type:** dc1.large (Dropdown menu)
- CPU:** 7 EC2 Compute Units (2 virtual cores) per node
- Memory:** 15 GiB per node
- Storage:** 160GB SSD storage per node
- I/O Performance:** Moderate
- Cluster Type:** Multi Node (Dropdown menu)
- Number of Compute Nodes:** 2 (Input field)
- Maximum:** 32
- Minimum:** 2

At the bottom, there are 'Cancel', 'Previous', and 'Continue' buttons. A 'Continue' button is highlighted in blue.

5. En la página Additional Configuration (Configuración adicional), especifique los valores de las siguientes opciones y haga clic en Continue (Continuar).
- a. En Provide the optional additional configuration details below (Proporcione a continuación otros detalles de configuración opcionales), configure las siguientes opciones:

Cluster Parameter Group (Grupo de parámetros del clúster)

Elija un grupo de parámetros para asociarlo al clúster. Si no lo elige, el clúster usará el grupo de parámetros predeterminado.

Encrypt Database (Cifrar base de datos)

Elija si desea cifrar todos los datos dentro del clúster y sus instantáneas. Si deja el valor predeterminado, None (Ninguno), no se habilitará el cifrado. Si desea habilitar el cifrado, elija si desea utilizar AWS Key Management Service (AWS KMS) o un módulo de seguridad de hardware (HSM), y establezca la configuración correspondiente. Para obtener más información sobre el cifrado en Amazon Redshift, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

- KMS

Seleccione KMS si desea habilitar el cifrado y utilizar AWS KMS para administrar la clave de cifrado. En Master Key (Clave maestra), seleccione (default) aws/redshift para utilizar una clave maestra de cliente (CMK) predeterminada o para seleccionar otra clave de la cuenta de AWS.

Note

Si desea utilizar una clave de otra cuenta de AWS, seleccione Enter a key ARN (Escribir un ARN de clave) en Master Key (Clave maestra). A continuación, escriba el nombre de recurso de Amazon (ARN) de la clave que va a usar. Debe tener permisos para usar la clave. Para obtener más información sobre el acceso a claves en AWS KMS, consulte [Controlar el acceso a sus llaves en la AWS Key Management Service](#) Guía para desarrolladores.

Para obtener más información acerca del uso de AWS KMS claves de cifrado en Amazon Redshift, consulte [Cifrado de base de datos de Amazon Redshift mediante AWS KMS \(p. 286\)](#).

- HSM

Seleccione HSM si desea habilitar el cifrado y utilizar un módulo de seguridad de hardware (HSM) para administrar la clave de cifrado.

Si selecciona HSM, elija valores de HSM Connection (conexión de HSM) y HSM Client Certificate (Certificado de cliente de HSM). Estos valores se necesitan para que Amazon

Redshift y el HSM formen una conexión confiable sobre la cual pueda pasar la clave del clúster. La conexión del HSM y el certificado de cliente se deben configurar en Amazon Redshift antes de lanzar un clúster. Para obtener más información acerca de cómo configurar las conexiones del HSM y los certificados de clientes, consulte [Cifrado para Amazon Redshift mediante módulos de seguridad de hardware](#) (p. 288).

- b. En Configure Networking Options (Configurar opciones de red), configure si desea lanzar el clúster en una nube virtual privada (VPC) o fuera de una VPC. La opción que elija afectará a otras opciones disponibles en esta sección. Amazon Redshift utiliza las plataformas EC2-VPC y EC2-Classic para lanzar clústeres. La cuenta de AWS determina qué plataforma o plataformas tiene a disposición para su clúster. Para obtener más información, consulte [Plataformas admitidas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Choose a VPC (Seleccionar una VPC)

- Para lanzar el clúster en una Virtual Private Cloud (VPC, Nube virtual privada), elija la VPC que desea utilizar. Debe tener al menos un grupo de subredes de de Amazon Redshift configurado para usar una VPC. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift](#) (p. 80).

Configure Networking Options:

Choose a VPC **Default VPC (vpc-01234567)** The identifier of the VPC in which you want to create your cluster

Cluster Subnet Group **default** Selected Cluster Subnet Group may limit the choice of Availability Zones

Publicly Accessible ☒ Yes ☐ No Select Yes if you want the cluster to have a public IP address that can be accessed from the public internet, select No if you want the cluster to have a private IP address that can only be accessed from within the VPC.

Choose a Public IP Address ☐ Yes ☒ No Select Yes if you want to select an elastic IP (EIP) address that you already have configured. Otherwise, select No to have Amazon Redshift create an EIP for your instance.

Enhanced VPC Routing ☒ Yes ☐ No ⚠ Additional VPC configuration might be required. [Learn more.](#)

Availability Zone **No Preference** The EC2 Availability Zone that the cluster will be created in.

- Para lanzar un clúster fuera de una VPC, seleccione Not in VPC (No en la VPC). Esta opción solo está disponible para cuentas de AWS que admiten plataformas EC2-Classic. De lo contrario, deberá lanzar el clúster en una VPC.

Configure Networking Options:

Choose a VPC **Not in VPC** Only VPCs with Cluster Subnet Groups are allowed

Availability Zone **No Preference** The EC2 Availability Zone that the cluster will be created in.

Cluster Subnet Group (Grupo de subredes del clúster)

Seleccione el grupo de subredes de de Amazon Redshift en el cual lanzar el clúster.

Note

Esta opción solo está disponible para clústeres en una VPC.

Publicly Accessible

Seleccione Yes (Sí) para permitir que la conexión con el clúster pueda establecerse fuera de la VPC en la que ha lanzado el clúster. Seleccione No si desea que las conexiones con el clúster solamente puedan hacerse desde dentro de la VPC.

Note

Esta opción solo está disponible para clústeres en una VPC.

Choose a Public IP Address (Seleccionar dirección IP pública)

Si configura Publicly Accessible De a Sí, elija No aquí para que Amazon Redshift proporcione una dirección IP elástica (EIP) para el clúster. Como alternativa, elija Yes (Sí) si desea utilizar una EIP que ha creado y administrado. Si desea que Amazon Redshift cree la EIP, también se encargará de administrarla Amazon Redshift.

Note

Esta opción solo está disponible en los clústeres de una VPC en los que Publicly accessible es Enabled (Habilitado).

Elastic IP

Seleccione la EIP que desee usar para conectarse al clúster desde fuera de la VPC.

Note

La opción está disponible solamente en los clústeres de una VPC en los que las opciones Publicly Accessible (Accesible públicamente) y Choose a Public IP Address (Seleccionar dirección IP pública) están establecidas en Yes (Sí).

Zona de disponibilidad

Seleccionar No Preference (Sin preferencias) Para que Amazon Redshift elija la zona de disponibilidad en la que se crea el clúster. De lo contrario, elija una zona de disponibilidad específica.

Enhanced VPC Routing

Seleccione Yes (Sí) para permitir el direccionamiento mejorado de la VPC. El direccionamiento mejorado de la VPC podría requerir cierta configuración adicional. Para obtener más información, consulte [Enhanced VPC Routing](#) (p. 202).

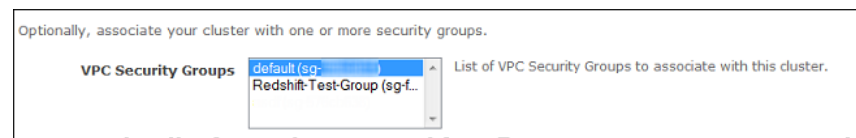
- c. En Optionally, associate your cluster with one or more security groups (Si lo desea, puede asociar el clúster con uno o varios grupos de seguridad), especifique valores para las siguientes opciones:

Grupos de seguridad de la VPC

Elija un grupo o grupos de seguridad de VPC para el clúster. De manera predeterminada, el grupo de seguridad elegido es el grupo de seguridad de VPC predeterminado. Para obtener más información acerca de los grupos de seguridad de VPC, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Note

Esta opción solo está disponible si lanza el clúster en la plataforma EC2-VPC.



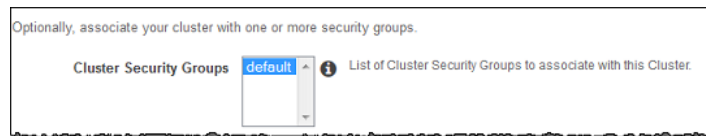
Cluster Security Groups (Grupos de seguridad del clúster)

Elija un grupo o grupos de seguridad de Amazon Redshift para el clúster. De manera predeterminada, el grupo de seguridad elegido es el grupo de seguridad predeterminado.

Para obtener más información acerca de los grupos de seguridad del clúster, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#).

Note

Esta opción solo está disponible si lanza el clúster en la plataforma EC2-Classical.



- d. En Optionally create a basic alarm for this cluster (Si lo desea, puede crear una alarma básica para este clúster), configure las siguientes opciones y seleccione Continue (Continuar):

Create CloudWatch Alarm (Crear alarma de CloudWatch)

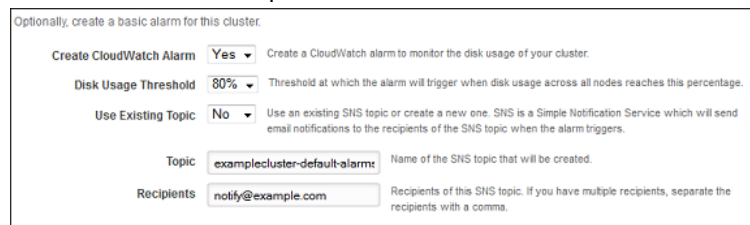
Seleccione Yes (Sí) si desea crear una alarma que monitoree el uso del disco en el clúster y especifique los valores de las opciones correspondientes. Seleccione No si no desea crear una alarma.

Disk Usage Threshold (Umbral de uso del disco)

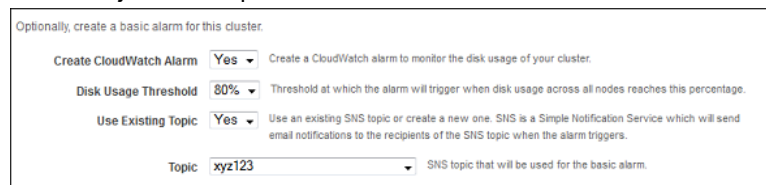
Elija un porcentaje de uso promedio alcanzado o superado del disco en el cual debe desencadenar la alarma.

Use Existing Topic (Usar tema existente)

SeleccionarNoSi desea crear un nuevo tema de Amazon Simple Notification Service (Amazon SNS) para esta alarma. En el cuadro Topic (Tema), modifique el nombre predeterminado, si es necesario. En Recipients (Destinatarios), escriba las direcciones de correo electrónico de todos los destinatarios que deberían recibir la notificación cuando se dispare la alarma.



SeleccionarSíSi desea elegir un tema de Amazon SNS existente para esta alarma y, en laTemaElija el tema que desea utilizar.



- e. En Optionally, select your maintenance track for this cluster (Si lo desea, puede seleccionar una pista de mantenimiento para este clúster), seleccione Current (Actual) o Trailing (Anterior).

Si selecciona Current (Actual), el clúster se actualiza con la versión aprobada más reciente durante el periodo de mantenimiento. Si selecciona Trailing (Anterior), el clúster se actualiza con la versión que se aprobó previamente.

Optionally, select your maintenance track for this cluster.

Maintenance Track

☒ Current ☐ Trailing

Select Current to apply the latest certified maintenance release including features and bug-fixes. Select Trailing to apply the previously certified maintenance release.

6. En la página Review (Revisar), revise los detalles del clúster. Si todo está correcto, seleccione Launch Cluster (Lanzar clúster) para comenzar el proceso de creación. De lo contrario, seleccione Back (Atrás) para realizar los cambios necesarios. A continuación, haga clic en Continue (Continuar) para volver a la página Review (Revisar).

Note

Algunas propiedades del clúster, como los valores de Database Port (Puerto de base de datos) y Master User Name (Nombre de usuario maestro) no se podrán modificar más adelante. Si necesita modificarlos, seleccione Back (Atrás) para hacerlo ahora.

En la siguiente captura de pantalla, se muestra un resumen de distintas opciones elegidas durante el proceso de lanzamiento del clúster.

✓

✓

✓

○

CLUSTER DETAILS NODE CONFIGURATION ADDITIONAL CONFIGURATION REVIEW

You are about to launch a cluster with following the following specifications:

Cluster Properties

These attributes specify the name of your cluster, what type of virtual hardware it will run on, how many nodes it will contain, and the availability zone in which it will be located.

Cluster Identifier: examplecluster

Node Type: dc1.large

Number of Compute Nodes: 1 (leader and compute run on a single node)

Availability Zone: No Preference

Database Configuration

These properties specify the database name, port, will use to connect to the database. The parameter configuration values used by the database.

Database Name: A default datab (dev)

Database Port: 5439

Master User Name: masteruser

Cluster Parameter Group: default.redshift

Security, Access, and Encryption

These settings control whether your cluster will be created in an existing VPC to allow for simpler integration with other Services, and the security groups which define access rules to your cluster.

Virtual Private Cloud: vpc-ed1c0e8f

Cluster Subnet Group:

Publicly Accessible: Yes

Elastic IP: Not used

VPC Security Groups: sg-6c4f540e

Enhanced VPC Routing: Yes

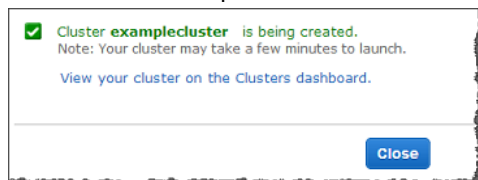
Encrypt Database: No

CloudWatch Alarms

CloudWatch alarms are used to notify if metrics for within a certain threshold. All recipients under the S for your alarm will receive notifications once an ala

Basic alarms will not be created for this cluster.

7. Después de iniciar el proceso de creación, seleccione Close (Cerrar). El clúster tardará varios minutos antes de estar listo para su uso.



Puede monitorizar el estado de la operación en el panel de rendimiento.

Modificación de un clúster

Cuando modifica un clúster, se aplican cambios de inmediato a las siguientes opciones:

- Grupos de seguridad de la VPC
- Publicly accessible (Accesible públicamente)
- Master User Password
- Conexión del HSM
- HSM Client Certificate (Certificado del cliente HSM)
- Mantenimiento detallado
- Snapshot preferences (Preferencias de instantáneas)

Los cambios en las siguientes opciones entran en vigor solamente después de reiniciar el clúster:

- Identificador de clúster

Amazon Redshift reinicia el clúster automáticamente cuando cambia el valor Identificador de clúster.

- Enhanced VPC Routing

Amazon Redshift reinicia el clúster automáticamente cuando cambia Enhanced VPC Routing.

- Grupo de parámetros del clúster

Si disminuye el período de retención automatizado de snapshots, se eliminarán las snapshots automatizadas existentes cuya configuración no se ajusten al nuevo período de retención. Para obtener más información, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Pasos para modificar un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Elija el clúster que se va a modificar.
4. Elija Edit. La Editar clúster Aparece la página.
5. Actualizar propiedades del clúster. Algunas de las propiedades que puede modificar son:
 - Identificador de clúster
 - Retención de instantáneas
 - Reubicación de clústeres

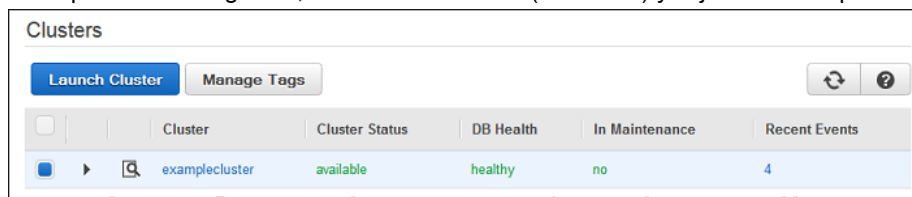
Para editar la configuración de Redes y seguridad, Mantenimiento, y Configuración de las bases, la consola proporciona vínculos a la ficha de detalles del clúster correspondiente.

6. Elija Save changes (Guardar cambios).

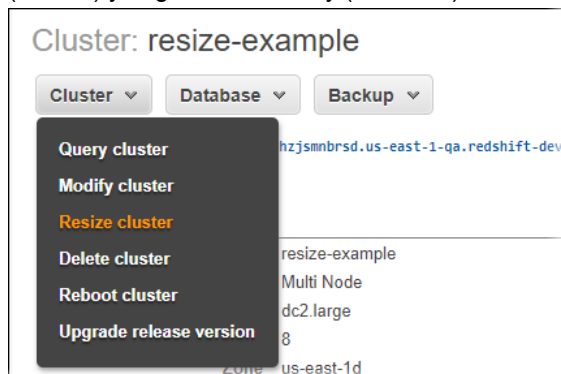
Consola original

Pasos para modificar un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee modificar.



3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, seleccione Cluster (Clúster) y haga clic en Modify (Modificar).



4. En la ventana Modify Cluster (Modificar clúster), cambie el clúster y, luego, elija Modify (Modificar). La ventana resultante muestra las opciones disponibles para modificar un clúster. Incluye pestañas con opciones para actualizar Cluster settings (Configuración del clúster), Maintenance settings (Configuración de mantenimiento) y Snapshot settings (Configuración de instantáneas).

Establecimiento de la pista de mantenimiento de un clúster

Puede establecer la pista de mantenimiento de un clúster con la consola. Para obtener más información, consulte [Elección de pistas de mantenimiento del clúster \(p. 17\)](#).

Para establecer una pista de mantenimiento para un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee modificar.
3. Elija la pestaña Maintenance settings (Configuración de mantenimiento).
4. Seleccione Current (Actual) o Trailing (Anterior).
5. Elija Modify.

Posponer el mantenimiento

Si necesita volver a programar el período de mantenimiento de su clúster, tiene la opción de posponer el mantenimiento hasta 45 días.

Para posponer el periodo de mantenimiento

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee modificar.
3. Elija la pestaña Maintenance settings (Configuración de mantenimiento).
4. Elija Defer maintenance (Posponer mantenimiento) y elija la fecha y la hora a la que posponer el mantenimiento.
5. Elija Modify.

Modify cluster

Cluster settings

Maintenance settings

Maintenance window settings

Maintenance window start: Saturday 07:30 UTC

Defer maintenance ☒ Uncheck to remove the setting

From: 16-11-2018 19:00 UTC

To: 23-11-2018 19:00 UTC

Warning: Modify your defer maintenance time settings to accommodate a mandatory hardware update. [Learn more](#)

We don't apply routine maintenance during the time period that you specify unless we need to replace hardware. We apply routine maintenance during the maintenance window that follows the deferred maintenance period.

Maintenance track settings

Maintenance Track: Current

Cancel Modify

Eliminación de un clúster

Si ya no necesita su clúster, puede eliminarlo. Si planifica aprovisionar un nuevo clúster con los mismos datos y la misma configuración que el que está eliminado, necesitará una instantánea manual. Con una instantánea manual, puede restaurar la instantánea más tarde y continuar utilizando el clúster. Si elimina el clúster, pero no crea una instantánea manual final, se eliminarán los datos del clúster. En ambos casos, las snapshots automatizadas se eliminan luego de que se elimina el clúster, pero las snapshots manuales se conservan hasta que usted las elimine. Es posible que se utilicen tarifas de almacenamiento de Amazon Simple Storage Service para las instantáneas manuales en función la cantidad de almacenamiento que tenga disponible para las instantáneas de Amazon Redshift para sus clústeres. Para obtener más información, consulte [Cierre y eliminación de clústeres \(p. 33\)](#).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

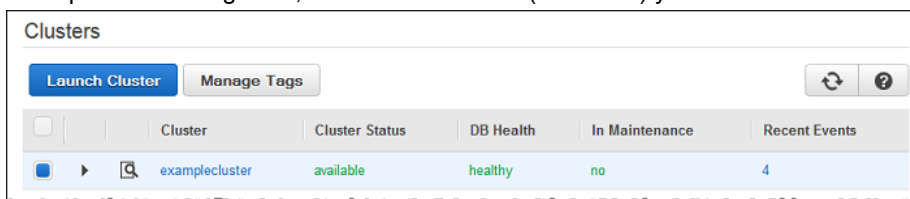
Para eliminar un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Elija el clúster que quiere eliminar.
4. En Actions (Acciones), elija Delete (Eliminar). Se abrirá la página Delete cluster (Eliminar clúster).
5. Seleccione Delete cluster (Eliminar clúster).

Consola original

Para eliminar un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y seleccione el clúster que desee eliminar.



3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, seleccione Cluster (Clúster) y Delete (Eliminar).
4. En el cuadro de diálogo Delete Cluster (Eliminar clúster), realice una de las siguientes acciones:
 - En Create snapshot (Crear instantánea), seleccione Yes (Sí) para eliminar el clúster y tomar una instantánea final. En Snapshot name (Nombre de la instantánea), seleccione un nombre para la instantánea final y haga clic en Delete (Eliminar).

Delete Cluster

If you want to restore your cluster later, you must create a manual snapshot. You can restore the cluster from the snapshot later and resume querying in minutes. You will be charged the Amazon S3 storage rate for a manual snapshot only if you don't have other clusters running, or if you exceed the allocated storage for active clusters.

Cluster

examplecluster

Create snapshot

☒ Yes ☐ No

Snapshot name

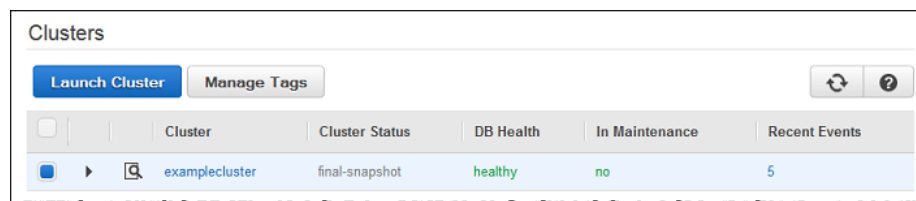
Cancel

Delete

- En Create snapshot (Crear instantánea), seleccione No para eliminar el clúster sin tomar una instantánea final y haga clic en Delete (Eliminar).

Después de iniciar la eliminación del clúster, puede tomar varios minutos para que este se elimine. Puede monitorear el estado en la lista de clúster como se muestra en las siguientes capturas de pantalla. Si solicitó una instantánea final, Cluster Status (estado del clúster) muestra *final-snapshot* antes de *deleting*.

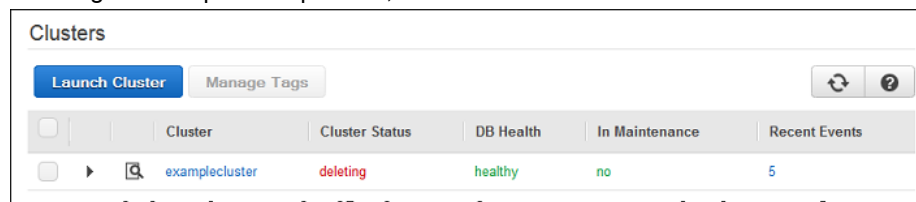
En la siguiente captura de pantalla, se muestra el clúster con un estado de *final-snapshot* antes de eliminarse.



The screenshot shows the 'Clusters' page in the AWS Management Console. At the top, there are buttons for 'Launch Cluster' and 'Manage Tags'. Below is a table with columns: Cluster, Cluster Status, DB Health, In Maintenance, and Recent Events. A single cluster named 'examplecluster' is listed with a status of 'final-snapshot', a health of 'healthy', and 'no' in maintenance. It has 5 recent events.

Cluster	Cluster Status	DB Health	In Maintenance	Recent Events
examplecluster	final-snapshot	healthy	no	5

En la siguiente captura de pantalla, se muestra el clúster con un estado de *deleting*.



The screenshot shows the 'Clusters' page in the AWS Management Console. The table now shows the cluster 'examplecluster' with a status of 'deleting', a health of 'healthy', and 'no' in maintenance. It still has 5 recent events.

Cluster	Cluster Status	DB Health	In Maintenance	Recent Events
examplecluster	deleting	healthy	no	5

Una vez finalizado el proceso, podrá comprobar que el clúster se haya eliminado porque ya no aparece en la lista de clústeres, en la página Clusters (Clústeres).

Reinicio de un clúster

Cuando reinicia un clúster, el estado se establece en *rebooting* y se crea un evento de clúster cuando se completa el reinicio. Se aplican todas las modificaciones pendientes al clúster en este reinicio.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Pasos para reiniciar de un clúster

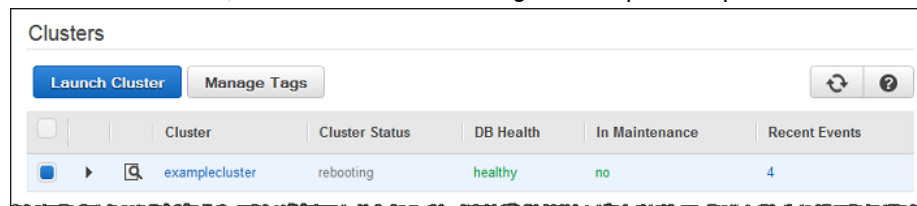
1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Elija el clúster que quiere reiniciar.
4. En Actions (Acciones), elija Reboot cluster (Reiniciar clúster). Se abrirá la página Reboot cluster (Reiniciar clúster).
5. Seleccione Reboot cluster (Reiniciar clúster).

Consola original

Pasos para reiniciar de un clúster

1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee reiniciar.
3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, seleccione Cluster (Clúster) y Reboot (Reiniciar).
4. En la ventana Reboot Clusters (Reiniciar clústeres), confirme que desea reiniciar este clúster y seleccione Reboot (Reiniciar).

El clúster puede demorar varios minutos en estar disponible. Puede monitorear el estado del reinicio en la lista de clúster, como se muestra en la siguiente captura de pantalla.



Redimensionamiento de un clúster

Cuando redimensione un clúster, especifique la cantidad de nodos o el tipo de nodo diferente de la configuración actual del clúster. Mientras el clúster está en proceso de redimensionamiento, no puede ejecutar consultas de escritura de lectura/escritura en el clúster; solo puede ejecutar consultas de solo lectura.

Para obtener más información acerca del redimensionamiento de clústeres, incluido el avance del proceso de redimensionamiento de clústeres utilizando diferentes enfoques, consulte [Cambio de tamaño de los clústeres de Amazon Redshift](#) (p. 23).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

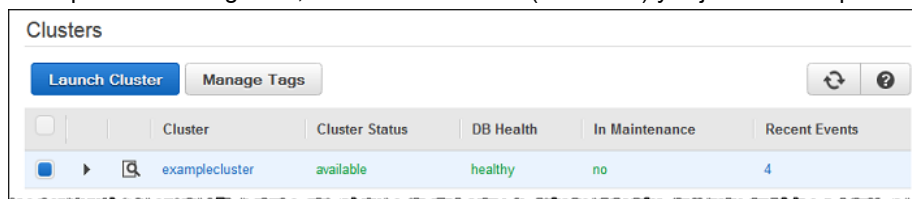
Pasos para redimensionar un clúster

1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Elija el clúster al que quiere cambiar el tamaño.
4. En Actions (Acciones), elija Resize (Cambiar tamaño). Se abrirá la página Resize cluster (Cambiar tamaño del clúster).
5. Siga las instrucciones de la página. Puede cambiar el tamaño del clúster ahora, una vez en un momento específico, o aumentar y disminuir el tamaño del clúster según una programación.
6. En función de sus opciones, elija Resize now (Cambiar tamaño ahora) o Schedule resize (Programar cambio de tamaño).

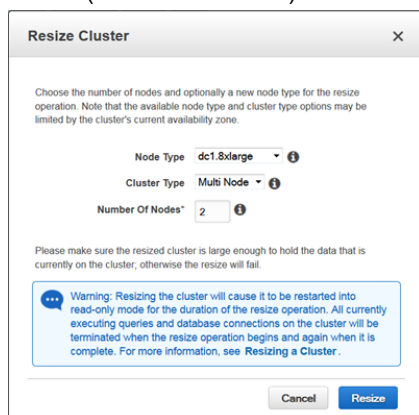
Consola original

Pasos para redimensionar un clúster

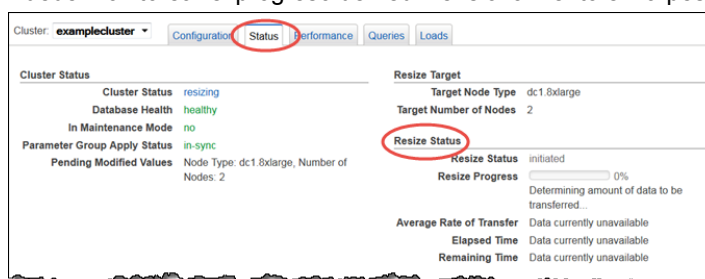
1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee redimensionar.



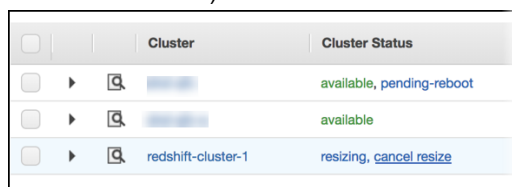
3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, seleccione Cluster (Clúster) y haga clic en Resize (Cambiar tamaño).
4. En la ventana Resize Clusters (Cambiar tamaño de los clústeres), configure los parámetros de redimensionamiento, como Node Type (Tipo de nodo), Cluster Type (Tipo de clúster) y Number of Nodes (Número de nodos). A continuación, haga clic en Resize (Cambiar tamaño).



Puede monitorear el progreso del redimensionamiento en la pestaña Status (Estado).



Para cancelar un cambio de tamaño clásico antes de que se complete, elija cancel resize (cancelar cambio de tamaño) en la lista de clústeres.



Actualizar la versión de lanzamiento de un clúster

Puede actualizar la versión de mantenimiento de un clúster que tiene un valor de Release Status (Estado de la versión) de New release available (Nueva actualización disponible). Puede optar por actualizar la versión de mantenimiento inmediatamente o en el siguiente período de mantenimiento.

Important

Si actualiza inmediatamente, el clúster está sin conexión hasta que finalice la actualización.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para actualizar un clúster a una nueva versión de lanzamiento

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Elija el clúster que quiere actualizar.
4. En Actions (Acciones), seleccione Upgrade cluster version (Actualizar versión del clúster). Aparecerá la página Upgrade cluster version (Actualizar versión del clúster).
5. Siga las instrucciones de la página.
6. Seleccione Upgrade cluster version (Actualizar versión del clúster).

Consola original

Para actualizar su clúster a una nueva versión de lanzamiento

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres) y después elija el clúster que desee actualizar.
3. En la pestaña Clusters (Clústeres), elija Cluster (Clúster) y, después, elija Upgrade release version (Actualizar versión de lanzamiento).
4. En la ventana Upgrade (Actualización), puede ver los números de Current release (Versión actual) y New release (Nueva versión), un enlace a los detalles sobre [Historial de versiones del clúster \(p. 87\)](#) y la Maintenance window schedule (Programación de períodos de mantenimiento). Si elige Yes, Upgrade now (Sí, actualizar ahora), debe confirmar que el clúster está sin conexión durante la actualización. De lo contrario, puede elegir Never mind, upgrade in my maintenance window (No importa, actualizar durante mi período de mantenimiento).

Una vez finalizada la actualización, puede ver el nuevo estado en la columna Release status (Estado de la versión).

Obtención de información acerca de la configuración del clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

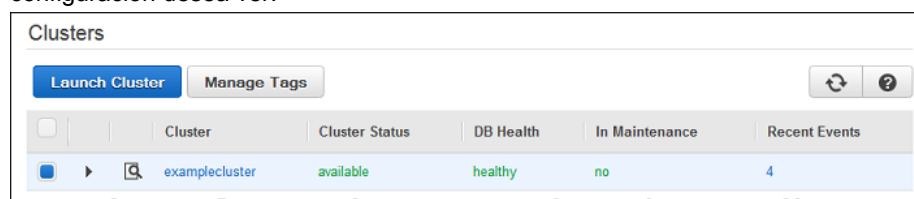
Para mostrar información sobre un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluir Rendimiento del clúster, Supervisión de consultas, Bases de datos, Comparticiones de datos, Schedules, Mantenimiento, y Propiedades Pestañas.
3. Seleccione cada pestaña para ver más información.

Consola original

Pasos para obtener los detalles de configuración del clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster cuya información de configuración desea ver.



3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, revise la información de configuración. Puede ver información acerca de las propiedades del clúster, el estado, la base de datos, la capacidad, el backup, el registro de auditorías, el mantenimiento y la configuración de adquisición de SSH.

Obtención de información general acerca del estado del clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para ver el estado de un clúster

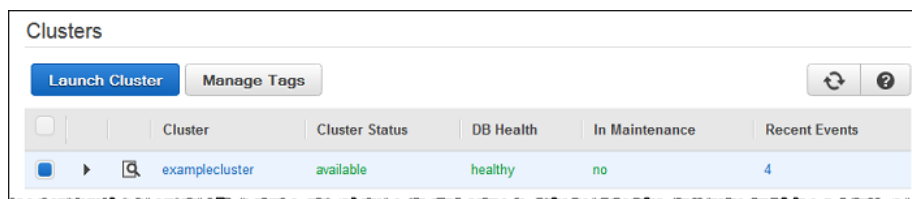
1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Vea el estado del clúster en la columna Status (Estado).

Consola original

La pestaña Status (Estado) del clúster contiene información general sobre el estado de un clúster y un resumen de los eventos relacionados con el clúster. También proporciona una lista de alarmas de Amazon CloudWatch asociadas con el clúster.

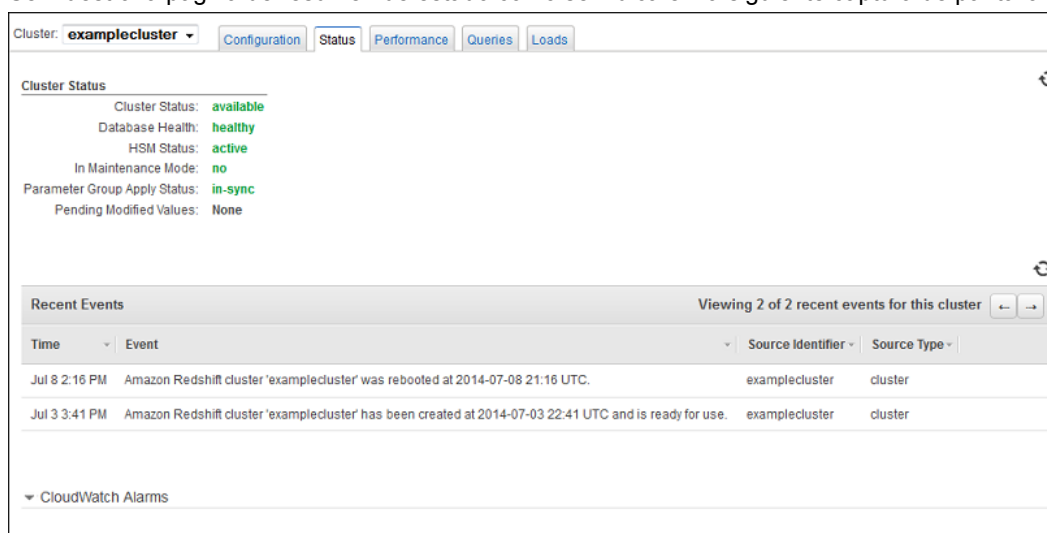
Pasos para obtener información general acerca del estado del clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster cuya información de estado desea ver.



3. Seleccione la pestaña Status (Estado).

Se muestra la página de resumen de estado como se indica en la siguiente captura de pantalla.



Crear una instantánea de un clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una instantánea de un clúster

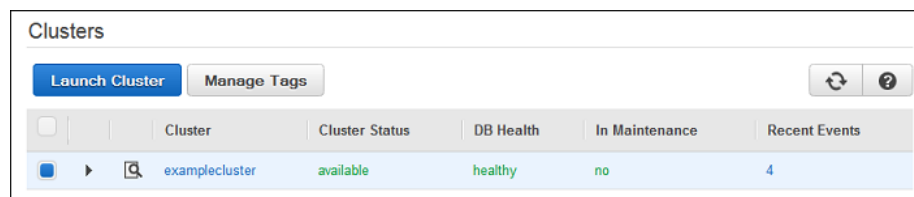
1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES).
3. Seleccione el clúster del que quiere crear una instantánea.
4. En Actions (Acciones), seleccione Create alias (Crear alias). Aparecerá la página Create snapshot (Crear instantánea).
5. Siga las instrucciones de la página.
6. Seleccione Create snapshot (Crear instantánea).

Consola original

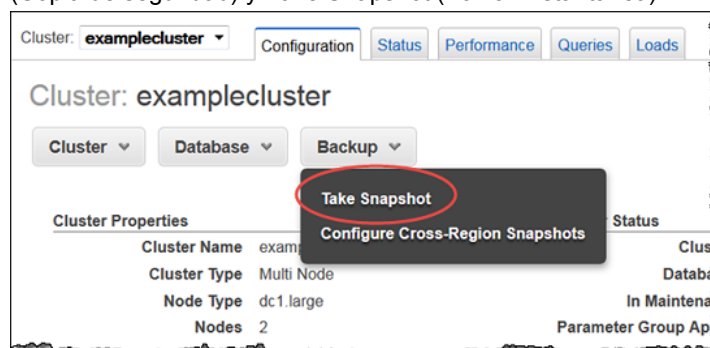
Puede crear una instantánea de su clúster desde la pestaña Configuration (Configuración) del clúster, tal y como se muestra a continuación. También puede crear una instantánea de su clúster desde la parte de instantáneas de la consola de Amazon Redshift. Para obtener más información, consulte [Administración de instantáneas mediante la consola](#) (p. 250).

Para crear una instantánea de un clúster

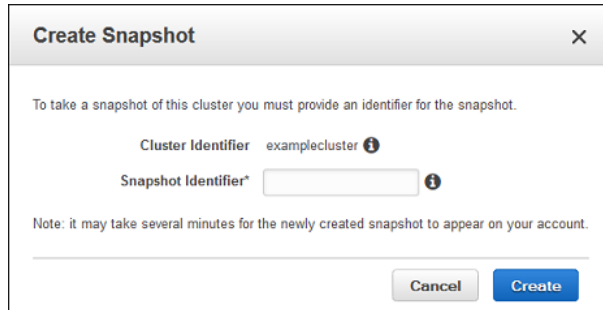
1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster del que desea realizar una instantánea.



3. En la pestaña Configuration (Configuración) de la página de detalles del clúster, seleccione Backup (Copia de seguridad) y Take Snapshot (Tomar instantánea).



4. En el cuadro de diálogo Create Snapshot (Crear instantánea), haga lo siguiente:
 - a. En el cuadro Cluster Identifier (Identificador del clúster), seleccione el clúster del que desea realizar una instantánea.
 - b. En el cuadro Snapshot Identifier (Identificador de instantánea), escriba un nombre para la instantánea.



5. Seleccione Create (Crear).

Para ver los detalles de la instantánea tomada y todas las demás instantáneas de suAWSConsulte la sección de instantáneas de la consola de Amazon Redshift. Para obtener más información, consulte [Administración de instantáneas mediante la consola \(p. 250\)](#).

Crear o editar una alarma de espacio en disco

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una alarma de uso de espacio en disco para un clúster

1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione ALARMS (ALARMAS).
3. En Actions (Acciones), seleccione Create alarm (Crear alarma). Aparecerá la página Create alarm (Crear alarma).
4. Siga las instrucciones de la página.
5. Elija Create alarm (Crear alarma).

Consola original

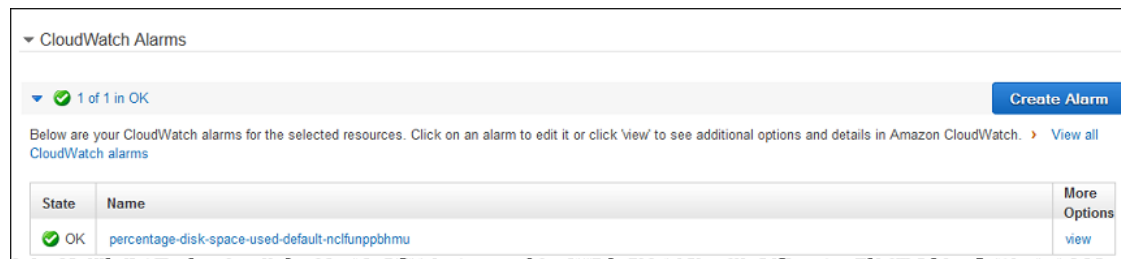
Si creó una alarma predeterminada de espacio en disco cuando creó su clúster de Amazon Redshift, puede editar la alarma. Por ejemplo, es posible que desee cambiar el porcentaje en el que se activa la alarma. O es posible que desee cambiar la configuración de duración.

Pasos para editar la alarma predeterminada de espacio en disco

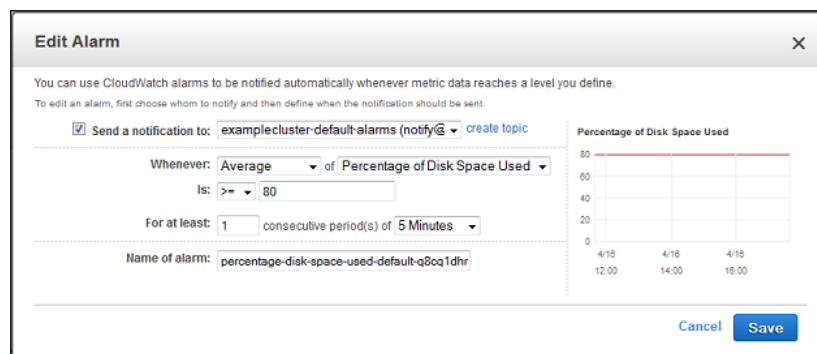
1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.

2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster asociado a la alarma que desea editar.
3. Seleccione la pestaña Status (Estado).
4. En la sección CloudWatch Alarms (Alarmas de CloudWatch), seleccione la alarma que desea editar.

El nombre que se asignó a la alarma de espacio en disco predeterminada que se creó cuando lanzó el clúster es `percentage-disk-space-used-default-cadena`. La **cadena** es generado aleatoriamente por Amazon Redshift.



5. En la ventana Edit Alarm (Editar alarma), edite los valores que desee modificar, como el porcentaje o los minutos.



6. Para cambiar el tema de Amazon SNS al que se asocia la alarma, lleve a cabo alguna de las siguientes operaciones:
 - Si desea elegir otro tema existente, seleccione un tema en la lista Send a notification to (Enviar notificación a).
 - Si desea crear un tema nuevo, elija Create topic (Crear tema) y especifique un nombre de tema nuevo y las direcciones de correo electrónico de los destinatarios.
7. Elija Save (Guardar).

Uso de los datos de rendimiento del clúster

En la nueva consola, puede trabajar con el rendimiento del clúster en la pestaña Cluster performance (Rendimiento del clúster) de la página de detalles del clúster.

En la consola original, puede trabajar con el rendimiento del clúster a través de las pestañas Performance (Rendimiento), Queries (Consultas) y Loads (Cargas). Para obtener más información acerca de cómo trabajar con el rendimiento de un clúster, consulte [Uso de los datos de rendimiento en la consola de Amazon Redshift](#) (p. 430).

Administración de clústeres a través de laAWS CLI/API de Amazon Redshift

Puede utilizar las siguientesAWS CLIpara gestionar clústeres en 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](#)

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar clústeres.

- [CancelResize](#)
- [CreateCluster](#)
- [DeleteCluster](#)
- [DescribeClusters](#)
- [DescribeClusterVersions](#)
- [DescribeNodeConfigurationOptions](#)
- [DescribeResize](#)
- [DescribeOrderableClusterOptions](#)
- [ModifyCluster](#)
- [PauseCluster](#)
- [RebootCluster](#)
- [ResizeCluster](#)
- [ResumeCluster](#)

Administración de clústeres con la herramienta deAWS SDK for Java

En el siguiente ejemplo de código Java se muestran las operaciones de administración de clústeres comunes, incluidas:

- Creación de un clúster.

- Visualización de metadatos sobre un clúster.
- Modificación de las opciones de configuración.

Después de iniciar la solicitud para crear el clúster, debe esperar hasta que el clúster esté en el estado `available` antes de poder modificarlo. En este ejemplo se utiliza un bucle para comprobar periódicamente el estado del clúster con el método `describeClusters`. Cuando el clúster está disponible, la ventana de mantenimiento preferida para el clúster cambia.

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Debe actualizar el código y especificar un identificador de clúster.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[CreateAndModifyCluster demonstrates how to create and modify
// an Amazon Redshift cluster.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateCluster]
// snippet-keyword:[DescribeClusters]
// snippet-keyword:[ModifyCluster]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyCluster.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;

import com.amazonaws.services.redshift.AmazonRedshift;
import com.amazonaws.services.redshift.AmazonRedshiftClientBuilder;
import com.amazonaws.services.redshift.model.*;

public class CreateAndModifyCluster {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "****provide a cluster identifier****";
    public static long sleepTime = 20;

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
        com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
```

```
        createCluster();
        waitForClusterReady();
        describeClusters();
        modifyCluster();
        describeClusters();
    } catch (Exception e) {
        System.err.println("Operation failed: " + e.getMessage());
    }
}

private static void createCluster() {
    CreateClusterRequest request = new CreateClusterRequest()
        .withClusterIdentifier(clusterIdentifier)
        .withMasterUsername("masteruser")
        .withMasterUserPassword("12345678Aa")
        .withNodeType("ds2.xlarge")
        .withNumberOfNodes(2)
        .withClusterSubnetGroupName("subnetgroup1");

    Cluster createResponse = client.createCluster(request);
    System.out.println("Created cluster " + createResponse.getClusterIdentifier());
}

private static void describeClusters() {
    DescribeClustersRequest request = new DescribeClustersRequest()
        .withClusterIdentifier(clusterIdentifier);

    DescribeClustersResult result = client.describeClusters(request);
    printResult(result);
}

private static void modifyCluster() {
    ModifyClusterRequest request = new ModifyClusterRequest()
        .withClusterIdentifier(clusterIdentifier)
        .withPreferredMaintenanceWindow("wed:07:30-wed:08:00");

    client.modifyCluster(request);
    System.out.println("Modified cluster " + clusterIdentifier);
}

private static void printResult(DescribeClustersResult result)
{
    if (result == null)
    {
        System.out.println("Describe clusters result is null.");
        return;
    }

    System.out.println("Cluster property:");
    System.out.format("Preferred Maintenance Window: %s\n",
result.getClusters().get(0).getPreferredMaintenanceWindow());
}

private static void waitForClusterReady() throws InterruptedException {
    Boolean clusterReady = false;
    System.out.println("Waiting for cluster to become available.");
    while (!clusterReady) {
        DescribeClustersResult result = client.describeClusters(new
DescribeClustersRequest()

.withClusterIdentifier(clusterIdentifier));
        String status = (result.getClusters()).get(0).getClusterStatus();
        if (status.equalsIgnoreCase("available")) {
            clusterReady = true;
        }
    }
}
```

```
        }
        else {
            System.out.print(".");
            Thread.sleep(sleepTime*1000);
        }
    }
}
// snippet-end:[redshift.java.CreateAndModifyCluster.complete]
```

Administración de clústeres en una VPC

Temas

- [Overview \(p. 75\)](#)
- [Creación de un clúster en una VPC \(p. 77\)](#)
- [Administración de grupos de seguridad de VPC para un clúster \(p. 79\)](#)
- [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#)

Overview

Amazon Redshift admite las plataformas EC2-VPC y EC2-Classic para lanzar un clúster en una nube privada virtual (VPC) en función del servicio de Amazon VPC. Para obtener más información, consulte [Usar EC2-VPC al crear el clúster \(p. 9\)](#).

Note

Amazon Redshift admite el lanzamiento de clústeres en las VPC de tenencia dedicada. Para obtener más información, consulte [Instancias dedicadas](#) en la Guía del usuario de Amazon VPC.

Cuando aprovisiona un clúster en la VPC, debe realizar lo siguiente:

- Proporcione la información de la VPC.

Cuando solicite a Amazon Redshift que cree un clúster en su VPC, debe proporcionar la información de su VPC mediante la creación de un grupo de subredes de clúster. Esta información incluye el ID de la VPC y una lista de subredes en su VPC. Cuando lance un clúster, debe proporcionar el grupo de subredes de clúster para que Amazon Redshift pueda aprovisionar el clúster en una de las subredes de la VPC. Para obtener más información acerca de la creación de grupos de subredes en Amazon Redshift, consulte [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#). Para obtener más información acerca de la configuración de VPC, consulte [Introducción a Amazon VPC](#) en la Guía de introducción a Amazon VPC.

- Si lo desea, puede configurar las opciones de acceso público.

Si configura su clúster para que sea de acceso público, tiene la opción de seleccionar una dirección IP elástica para utilizarla con la dirección IP externa. Una dirección IP elástica es una dirección IP estática que está asociada a su AWS account. Puede utilizar una dirección IP elástica para conectarse al clúster desde fuera de la VPC. Una dirección IP elástica le ofrece la posibilidad de cambiar su configuración subyacente sin afectar la dirección IP que los clientes utilizan para conectarse a su clúster. Esto puede ser útil para situaciones como la recuperación después de un error.

Si desea utilizar una dirección IP elástica asociada a su propia AWS Debe crearla en Amazon EC2 antes de lanzar el clúster de Amazon Redshift. De lo contrario, no estará disponible durante el proceso de lanzamiento. También puede hacer que Amazon Redshift configure una dirección IP elástica

para utilizarla en la VPC. Sin embargo, la dirección IP elástica asignada se administrará con el servicio de Amazon Redshift y no estará asociada a su AWS account. Para obtener más información, consulte [Direcciones IP elásticas](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

En algunos casos, es posible que tenga un clúster de acceso público en una VPC al que desee conectarse con la dirección IP privada desde la VPC. Si es el caso, establezca los siguientes parámetros de VPC en `true`:

- `DNS resolution`
- `DNS hostnames`

Supongamos que tiene un clúster de acceso público en una VPC pero no establece estos parámetros en `true` en la VPC. En estos casos, las conexiones realizadas desde la VPC se resuelven en la dirección IP elástica del clúster en lugar de la dirección IP privada. Recomendamos que establezca estos parámetros en `true` y utilice la dirección IP privada para un clúster de acceso público cuando se conecte desde la VPC. Para obtener más información, consulte [Uso de DNS con su VPC](#) en la Guía del usuario de Amazon VPC.

Note

Si tiene un clúster de acceso público existente en una VPC, las conexiones realizadas desde la VPC seguirán utilizando la dirección IP elástica para conectarse al clúster hasta que cambie el tamaño del clúster. Esto ocurrirá incluso con los anteriores parámetros establecidos. Los clústeres nuevos seguirán el nuevo comportamiento de uso de la dirección IP privada cuando se conecten al clúster de acceso público desde la misma VPC.

La dirección IP elástica es una dirección IP externa para acceder al clúster fuera de la VPC. No está relacionado con el [Direcciones IP públicas y privadas del nodo del clúster](#) que se muestran en la consola de Amazon Redshift en [Detalles de la conexión](#). Las direcciones IP públicas y privadas del nodo del clúster aparecen sin importar que el clúster sea de acceso público o no. Se utilizan únicamente en determinadas circunstancias para configurar reglas de entrada en el host remoto. Estas circunstancias se producen cuando se cargan datos desde una instancia de Amazon EC2 u otro host remoto utilizando una conexión Secure Shell (SSH). Para obtener más información, consulte [Paso 1: Recuperar la clave pública del clúster y las direcciones IP del nodo del clúster](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

La opción de asociar un clúster a una dirección IP elástica está disponible cuando se crea el clúster o se restaura el clúster desde una instantánea. En algunos casos, es posible que quiera asociar el clúster con una dirección IP elástica o cambiar una dirección IP elástica que está asociada con el clúster. Para asociar una dirección IP elástica después de crear el clúster, primero actualice el clúster para que no sea accesible públicamente, y después haga que sea accesible públicamente y añada una dirección IP elástica en la misma operación.

- Asocie un grupo de seguridad de VPC.

Luego, se concede acceso de entrada mediante un grupo de seguridad de VPC. Este grupo de seguridad de VPC debe permitir el acceso al clúster a través del puerto de la base de datos de modo que pueda conectarse mediante las herramientas de cliente SQL. Puede configurar esto con antelación o añadirle reglas después de lanzar el clúster. Para obtener más información, consulte [Seguridad en su VPC](#) en la Guía del usuario de Amazon VPC. No puede utilizar los grupos de seguridad de clúster de Amazon Redshift para conceder acceso de entrada al clúster.

Para obtener más información acerca del uso de clústeres en una VPC, consulte [Creación de un clúster en una VPC \(p. 77\)](#).

Restauración de una instantánea de un clúster en VPC

Una instantánea de un clúster en VPC solo se puede restaurar en una VPC, no fuera de esta. Puede restaurarla en la misma VPC o en otra VPC de la cuenta. Para obtener más información acerca de las instantáneas, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

Creación de un clúster en una VPC

Los siguientes son los pasos generales sobre cómo puede implementar un clúster en su nube virtual privada (VPC).

New console

Creación de un clúster en una VPC

1. Configure una VPC.

Puede crear el clúster en la VPC predeterminada para la cuenta, si la cuenta tiene una, o en una VPC que haya creado. Para obtener más información, consulte [Usar EC2-VPC al crear el clúster \(p. 9\)](#). Para crear una VPC, consulte [Introducción a Amazon VPC](#) en la Guía del usuario de Amazon VPC. Anote el identificador de la VPC, la subred y la zona de disponibilidad de la subred. Necesitará esta información para lanzar el clúster.

Note

Debe tener por lo menos una subred definida en la VPC para que pueda añadirla al grupo de subredes del clúster en el siguiente paso. Si utiliza el asistente de VPC, se creará una subred para su VPC automáticamente. Para obtener más información acerca de cómo añadir una subred a su VPC, consulte [Agregar una subred a su VPC](#) en la Guía del usuario de Amazon VPC.

2. Cree un grupo de subredes de clúster de Amazon Redshift para especificar qué subred puede utilizar el clúster de Amazon Redshift en la VPC.

Puede crear un grupo de subredes de clúster mediante la consola de Amazon Redshift o mediante programación. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#).

3. Autorice el acceso para conexiones entrantes en un grupo de seguridad de VPC que vaya a asociar con el clúster.

Puede habilitar un cliente fuera de la VPC (en Internet público) para conectarse al clúster. Para ello, va a asociar el clúster con un grupo de seguridad de VPC que otorga acceso entrante al puerto que utilizó cuando lanzó el clúster. Para obtener ejemplos de las reglas de grupos de seguridad, consulte [Reglas del grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

4. Siga los pasos de [Introducción a Amazon Redshift](#) en la [Introducción a Amazon Redshift](#) para crear un clúster. Realice las siguientes modificaciones cuando cree un clúster:
 - Para mostrar la sección Additional configurations (Configuraciones adicionales), deshabilite Use defaults (Usar valores predeterminados).
 - En la sección Network and security (Red y seguridad), especifique la Nube virtual privada (VPC), el Grupo de subredes del clúster y el Grupo de seguridad de VPC que configuró.

Consola original

Creación de un clúster en una VPC

1. Configure una VPC.

Puede crear el clúster en la VPC predeterminada para la cuenta, si la cuenta tiene una, o en una VPC que haya creado. Para obtener más información, consulte [Usar EC2-VPC al crear el clúster \(p. 9\)](#). Para crear una VPC, consulte [Introducción a Amazon VPC](#) en la Guía del usuario de Amazon VPC. Anote el identificador de la VPC, la subred y la zona de disponibilidad de la subred. Necesitará esta información para lanzar el clúster.

Note

Debe tener por lo menos una subred definida en la VPC para que pueda añadirla al grupo de subredes del clúster en el siguiente paso. Si utiliza el asistente de VPC, se creará una subred para su VPC automáticamente. Para obtener más información acerca de cómo agregar una subred a su VPC, consulte [Agregar una subred a su VPC](#) en la Guía del usuario de Amazon VPC.

2. Cree un grupo de subredes de clúster de Amazon Redshift que especifique cuál de las subredes de la VPC puede utilizar el clúster de Amazon Redshift.

Puede crear un grupo de subredes de clúster mediante la consola de Amazon Redshift o mediante programación. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift](#) (p. 80).

3. Autorice el acceso para conexiones entrantes en un grupo de seguridad de VPC que vaya a asociar con el clúster.

Puede habilitar un cliente fuera de la VPC (en Internet público) para conectarse al clúster. Para ello, va a asociar el clúster con un grupo de seguridad de VPC que otorga acceso entrante al puerto que utilizó cuando lanzó el clúster. Para obtener ejemplos de las reglas de grupos de seguridad, consulte [Reglas del grupo de seguridad](#) en la Guía del usuario de Amazon VPC.

4. Lance un clúster en la VPC.

Para lanzar el clúster en la VPC, puede usar el procedimiento que se describe en la sección Introducción. Para obtener más información, consulte [Paso 2: Lance un clúster](#). Cuando siga el asistente, en la opción Configure Network Options (Configurar opciones de red) de la página ADDITIONAL CONFIGURATION, especifique la siguiente información:

- Choose a VPC (Seleccionar una VPC): seleccione la VPC en la lista desplegable.
- Cluster Subnet Group (Grupo de subredes del clúster): seleccione el grupo de subredes del clúster que creó en el paso 2.
- Publicly accessible— SeleccionarHabilitarSi desea que el clúster tenga una dirección IP pública a la que se pueda acceder desde Internet pública.

Note

Al elegirHabilitarSu clúster estará accesible públicamente fuera de la VPC y se verá expuesto a amenazas de seguridad.

SelectDeshabilitarSi desea que el clúster tenga una dirección IP privada a la que solamente se pueda acceder desde la VPC.

- Choose a Public IP Address (Seleccionar dirección IP pública)— SeleccionarSiSi desea seleccionar una dirección IP elástica que ya haya configurado. De lo contrario, seleccioneNoPara que Amazon Redshift cree una dirección IP elástica para su instancia de.
- Elastic IPSeccione una dirección IP elástica para conectarse al clúster desde fuera de la VPC.
- Zona de disponibilidad— SeleccionarNo Preference (Sin preferencias)Para que Amazon Redshift seleccione la zona de disponibilidad en la que se va a crear el clúster de. De lo contrario, seleccione una zona de disponibilidad específica.
- Seleccione el grupo de seguridad de VPC que concede el acceso de dispositivos autorizados al clúster.

La siguiente es una captura de pantalla de ejemplo de la sección Configure Networking Options (Configurar opciones de red) de la página ADDITIONAL CONFIGURATION.

Configure Networking Options:

Choose a VPC **vpc-xxxxxx** The identifier of the VPC in which you want to create your cluster

Cluster Subnet Group **examplesubnet** Selected Cluster Subnet Group may limit the choice of Availability Zones

Publicly Accessible **Yes** Select Yes if you want the cluster to be accessible from the public internet. Select No if you want it to be accessible only from within your private VPC network

Choose a Public IP Address **Yes** Select Yes if you want to select your own public IP address from a list of elastic IP (EIP) addresses that are already configured for your cluster's VPC. Select No if you want Amazon Redshift to provide an EIP for you instead.

Elastic IP **elb-xxxxxx** Select the Elastic IP that you want the cluster to use for its public IP address.

Availability Zone **No Preference** The EC2 Availability Zone that the cluster will be created in.

Ahora ya puede utilizar el clúster. Puede seguir los pasos de introducción para probar el clúster mediante la carga de datos de ejemplo y la prueba de consultas de ejemplo.

Administración de grupos de seguridad de VPC para un clúster

Cuando aprovisiona un clúster de Amazon Redshift, se bloquea por defecto para que nadie pueda obtener acceso a él. Para concederle a otros usuarios acceso de entrada a un clúster de Amazon Redshift, debe asociar el clúster a un grupo de seguridad. Si está en la plataforma de EC2-VPC, puede utilizar un grupo de seguridad de Amazon VPC existente o definir uno nuevo. Luego lo asociará a un clúster como se describe a continuación. Si está en la plataforma EC2-Classic, defina un grupo de seguridad de clúster y asíelo a un clúster. Para obtener más información acerca del uso de grupos de seguridad de clúster en la plataforma EC2-Classic, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#).

Un grupo de seguridad de VPC está formado por un conjunto de reglas que controlan el acceso a una instancia en la VPC, como el clúster. Las reglas individuales establecen el acceso en función de los rangos de direcciones IP o de otros grupos de seguridad de VPC. Cuando asocia un grupo de seguridad de VPC a un clúster, las reglas que están definidas en el grupo de seguridad de VPC controlan el acceso al clúster.

Cada uno de los clústeres que aprovisiona en la plataforma de EC2-VPC tiene uno o varios grupos de seguridad de Amazon VPC asociados a él. Amazon VPC proporciona un grupo de seguridad de VPC llamado «default» que se crea automáticamente junto con la VPC. Cada clúster que se lanza en la VPC se asocia automáticamente al grupo de seguridad de VPC predeterminado si no especifica un grupo de seguridad de VPC diferente cuando crea el clúster. Puede asociar un grupo de seguridad de VPC a un clúster cuando crea el clúster o puede asociarlo más adelante mediante la modificación del clúster. Para obtener más información acerca de la asociación de grupos de seguridad de VPC a un clúster, consulte [Creación de un clúster mediante un lanzamiento del clúster \(p. 50\)](#) y [Pasos para modificar un clúster \(p. 60\)](#).

La tabla siguiente describe las reglas predeterminadas para el grupo de seguridad de VPC predeterminado.

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

Puede cambiar las reglas para el grupo de seguridad de VPC predeterminado según las necesidades del clúster de Amazon Redshift.

Si el grupo de seguridad de VPC predeterminado es suficiente para el usuario, no es necesario que cree más. Sin embargo, de forma opcional, puede crear grupos de seguridad de VPC adicionales para administrar mejor el acceso de entrada al clúster. Por ejemplo, suponga que está ejecutando un servicio en un clúster de Amazon Redshift y tiene varios niveles de servicio diferentes que proporciona a los clientes. Si no desea proporcionar el mismo acceso a todos los niveles de servicio, es posible que desee crear grupos de seguridad de VPC independientes, uno para cada nivel de servicio. Luego puede asociar estos grupos de seguridad de VPC al clúster.

Puede crear hasta 100 grupos de seguridad de VPC para una VPC y asociar un grupo de seguridad de VPC con muchos clústeres. Sin embargo, solo puede asociar hasta cinco grupos de seguridad de VPC con un clúster determinado.

Amazon Redshift aplica los cambios a un grupo de seguridad de VPC de inmediato. Por lo que si asoció un grupo de seguridad de VPC a un clúster, las reglas de acceso de entrada al clúster en el grupo de seguridad de VPC actualizado se aplican de inmediato.

Puede crear y modificar grupos de seguridad de VPC en la <https://console.aws.amazon.com/vpc/>. También puede administrar grupos de seguridad de VPC mediante programación con la AWS CLI, la CLI de Amazon EC2 y la AWS Tools for Windows PowerShell. Para obtener más información acerca de cómo trabajar con grupos de seguridad de VPC, consulte [Grupos de seguridad de su VPC](#) en la Guía del usuario de Amazon VPC.

Grupos de subredes del clúster de Amazon Redshift

Overview

Usted crea un grupo de subred de clúster si aprovisiona el clúster en su Virtual Private Cloud (VPC, Nube privada virtual). Para obtener más información acerca de VPC, consulte la [Amazon VPC](#) Página de detalles del producto.

Su VPC puede tener una o más subredes, un subconjunto de direcciones IP dentro de la VPC, que le permite agrupar recursos según las necesidades de seguridad y operación. Un grupo de subred de clúster le permite especificar un conjunto de subredes en su VPC. Cuando aprovisiona un clúster, proporciona un grupo de subredes y Amazon Redshift crea el clúster en una de las subredes del grupo.

Para obtener más información acerca de la creación de una VPC, visite [Guía del usuario de Amazon VPC](#) Documentación.

Después de crear un grupo de subredes, puede eliminar las subredes que añadió previamente o añadir más subredes. Amazon Redshift ofrece operaciones de API que le permiten crear, modificar o eliminar un grupo de subredes de clúster. También puede usar la consola para realizar estas operaciones.

Administración de grupos de subred de clúster mediante la consola

Puede administrar los grupos de subredes de clúster utilizando la consola de Amazon Redshift. Puede crear un grupo de subredes del clúster, administrar o eliminar uno existente. Todas estas tareas parten de la lista de grupos de subredes de clúster. Para administrar este tipo de grupo, debe seleccionar un grupo de subredes de clúster.

Puede aprovisionar un clúster en una de las subredes que proporciona al grupo de subred. Un grupo de subred de clúster le permite especificar un conjunto de subredes en su virtual private cloud (VPC).

Creación de un grupo de subredes de clúster

Debe tener al menos un grupo de subred de clúster definido para aprovisionar un clúster en una Virtual Private Cloud (VPC, Nube virtual privada).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

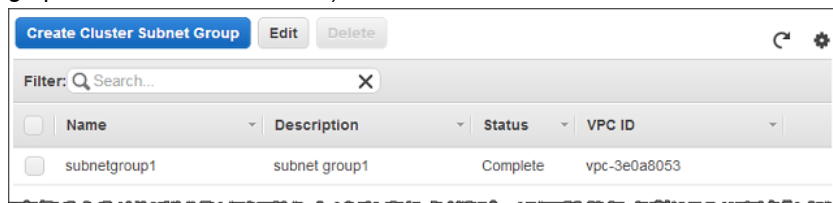
Pasos para crear un grupo de subred de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione CONFIGy, a continuación, seleccione Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Seleccione Create cluster subnet group (Crear grupo de subred de clúster) para mostrar la página de creación.
4. Introduzca información para el grupo de subredes, incluidas las subredes que desea añadir.
5. Elija Create cluster subnet group (Crear grupo de subred de clúster) para crear el grupo con las subredes que eligió.

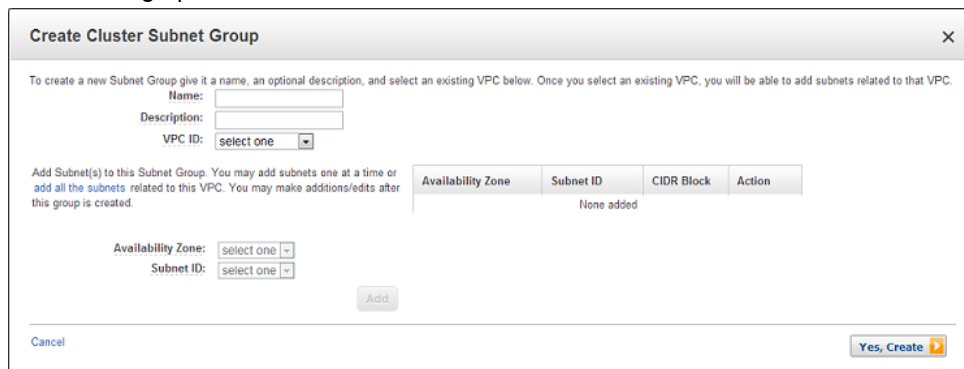
Consola original

Pasos para crear un grupo de subred de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Subnet Groups (Grupos de subredes), haga clic en Create Cluster Subnet Group (Crear grupo de subredes del clúster).



4. En el cuadro de diálogo Create Cluster Subnet Group (Crear grupo de subredes del clúster), añada subredes al grupo.



- a. Especificar los valores de los campos Name (Nombre), Description (Descripción) y VPC ID (ID de VPC) para el grupo de subredes del clúster.
- b. Añadir subredes al grupo mediante una de las acciones siguientes:

- Haga clic en el enlace add all the subnets (añadir todas las subredes).
- Use los cuadros Availability Zone (Zona de disponibilidad) y Subnet ID (ID de subred) para seleccionar una subred específica y haga clic en Add (Añadir).

En el siguiente ejemplo, se muestra un grupo de subred de clúster especificado con un grupo de subredes.

Create Cluster Subnet Group

To create a new Subnet Group give it a name, an optional description, and select an existing VPC below. Once you select an existing VPC, you will be able to add subnets related to that VPC.

Name:

Description:

VPC ID:

Add Subnet(s) to this Subnet Group: You may add subnets one at a time or add all the subnets related to this VPC. You may make additions/edits after this group is created.

Availability Zone	Subnet ID	CIDR Block	Action
us-east-1d	subnet-...	10.0.0.0/24	Remove

Availability Zone:

Subnet ID:

[Add](#)

[Cancel](#) [Yes, Create](#)

5. Elija Yes, Create (Sí, crear).

El nuevo grupo se muestra en la lista de grupos de subredes de clúster.

Modificación de un grupo de subredes de clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Pasos para modificar un grupo de subredes de clúster

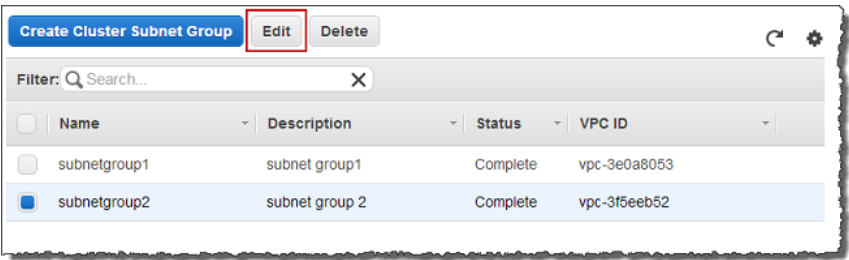
1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione CONFIGy, a continuación, seleccione Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Elija el grupo de subredes que modificar.
4. Para Actions (Acciones), seleccione Modify (Modificar) para mostrar los detalles del grupo de subredes.
5. Actualice la información para el grupo de subredes.
6. Seleccione Save (Guardar) para modificar el grupo.

Consola original

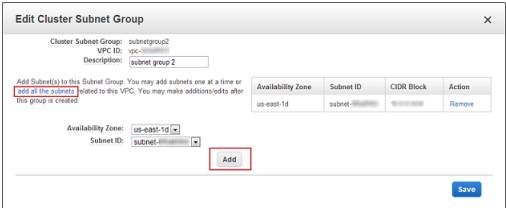
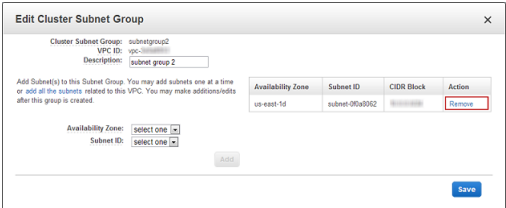
Pasos para modificar un grupo de subredes de clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), en la lista de grupos de subredes del clúster, haga clic en la fila del grupo que desea modificar y después en Edit (Editar).

En el siguiente ejemplo, subnetgroup2 es el grupo de subredes de clúster que queremos modificar.



4. En Cluster Subnet Group Details (Detalles del grupo de subredes del clúster), realice una de las siguientes acciones.

Para	Haga lo siguiente
Añadir una o más subredes al grupo	Seleccione una subred específica usando los cuadros Availability Zone (Zona de disponibilidad) y Subnet ID (ID de subred) o haga clic en add all the subnets (añadir todas las subredes).  Save (Guardar).
Eliminar una subred del grupo	En la lista de subredes que se están utilizando para el grupo, haga clic en Remove (Eliminar) junto a la subred que desee eliminar.  Save (Guardar).

Eliminación de un grupo de subredes de clúster

No puede eliminar un grupo de subredes de clúster que es utilizado por algún clúster.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Pasos para eliminar un grupo de subredes de clúster

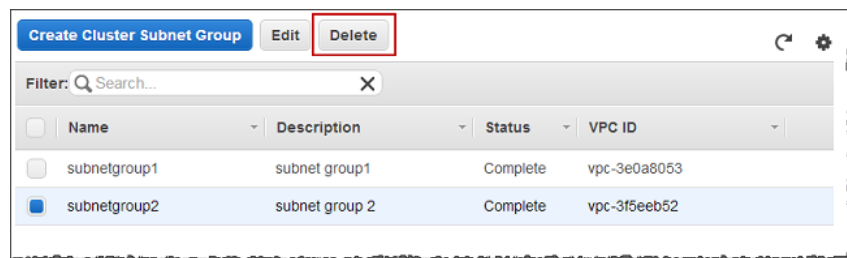
1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione CONFIGy, a continuación, seleccione Subnet groups (Grupos de subredes). Se muestra la lista de grupos de subredes.
3. Elija el grupo de subredes que eliminar, luego seleccione Delete (Eliminar).

Consola original

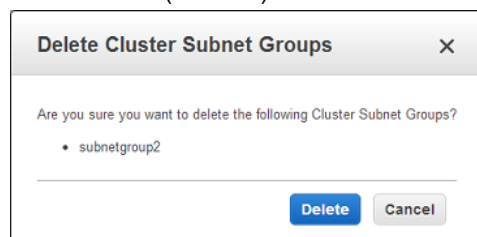
Pasos para eliminar un grupo de subredes de clúster

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Subnet Groups (Grupos de subredes), en la lista de grupos de subredes de clúster, haga clic en la fila del grupo que desee eliminar.

En el siguiente ejemplo, my-subnet-group es el grupo de subredes de clúster que queremos eliminar.



4. En el cuadro de diálogo Delete Cluster Subnet Group (Eliminar grupo de subredes del clúster), haga clic en Delete (Eliminar).



Administración de grupos de subredes del clúster mediante laAWS SDK for Java

En el siguiente ejemplo de código Java se muestran las operaciones de subred de clúster comunes, incluidas:

- Creación de un grupo de subredes de clúster.
- Visualización de metadatos sobre un grupo de subredes de clúster.
- Modificación de un grupo de subredes de clúster.

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Deberá actualizar el código y proporcionar un nombre de grupo de subred de clúster y dos identificadores de subred.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[CreateAndModifyClusterSubnetGroup demonstrates how to create
// and modify an Amazon Redshift subnet group.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterSubnetGroup]
// snippet-keyword:[DescribeClusterSubnetGroups]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyClusterSubnetGroup.complete]
package com.amazonaws.services.redshift;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

import com.amazonaws.services.redshift.model.*;

public class CreateAndModifyClusterSubnetGroup {

    public static AmazonRedshift client;
    public static String clusterSubnetGroupName = "subnet-group-name";
    // You can use the VPC console to find subnet IDs to use.
    public static String subnetId1 = "***provide a subnet ID***";
    public static String subnetId2 = "***provide a subnet ID***";

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            createClusterSubnetGroup();
            describeClusterSubnetGroups();
            modifyClusterSubnetGroup();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createClusterSubnetGroup() {
        CreateClusterSubnetGroupRequest request = new CreateClusterSubnetGroupRequest()
```



```

        .withClusterSubnetGroupName(clusterSubnetGroupName)
        .withDescription("my cluster subnet group")
        .withSubnetIds(subnetId1);
client.createClusterSubnetGroup(request);
System.out.println("Created cluster subnet group: " + clusterSubnetGroupName);
    }

    private static void modifyClusterSubnetGroup() {
        // Get existing subnet list.
        DescribeClusterSubnetGroupsRequest request1 = new
DescribeClusterSubnetGroupsRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName);
        DescribeClusterSubnetGroupsResult result1 =
client.describeClusterSubnetGroups(request1);
        List<String> subnetNames = new ArrayList<String>();
        // We can work with just the first group returned since we requested info about one
group.
        for (Subnet subnet : result1.getClusterSubnetGroups().get(0).getSubnets()) {
            subnetNames.add(subnet.getSubnetIdentifier());
        }
        // Add to existing subnet list.
        subnetNames.add(subnetId2);

        ModifyClusterSubnetGroupRequest request = new ModifyClusterSubnetGroupRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName)
            .withSubnetIds(subnetNames);
        ClusterSubnetGroup result2 = client.modifyClusterSubnetGroup(request);
        System.out.println("\nSubnet group modified.");
        printResultSubnetGroup(result2);
    }

    private static void describeClusterSubnetGroups() {
        DescribeClusterSubnetGroupsRequest request = new
DescribeClusterSubnetGroupsRequest()
            .withClusterSubnetGroupName(clusterSubnetGroupName);

        DescribeClusterSubnetGroupsResult result = client.describeClusterSubnetGroups(request);
        printResultSubnetGroups(result);
    }

    private static void printResultSubnetGroups(DescribeClusterSubnetGroupsResult result)
    {
        if (result == null)
        {
            System.out.println("\nDescribe cluster subnet groups result is null.");
            return;
        }

        for (ClusterSubnetGroup group : result.getClusterSubnetGroups())
        {
            printResultSubnetGroup(group);
        }
    }

    private static void printResultSubnetGroup(ClusterSubnetGroup group) {
        System.out.format("Name: %s, Description: %s\n", group.getClusterSubnetGroupName(),
group.getDescription());
        for (Subnet subnet : group.getSubnets()) {
            System.out.format("    Subnet: %s, %s, %s\n", subnet.getSubnetIdentifier(),
                subnet.getSubnetAvailabilityZone().getName(),
                subnet.getSubnetStatus());
        }
    }
}

```

```
// snippet-end:[redshift.java.CreateAndModifyClusterSubnetGroup.complete]
```

Administración de grupos de subredes del clúster mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar los grupos de subredes de clúster.

- [create-cluster-subnet-group](#)
- [delete-cluster-subnet-group](#)
- [describe-cluster-subnet-groups](#)
- [modify-cluster-subnet-group](#)

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los grupos de subredes de clúster.

- [CreateClusterSubnetGroup](#)
- [DeleteClusterSubnetGroup](#)
- [DescribeClusterSubnetGroups](#)
- [ModifyClusterSubnetGroup](#)

Historial de versiones del clúster

Amazon Redshift publica periódicamente nuevas versiones de clúster que se utilizan para actualizar el clúster.

Important

Para obtener información acerca de las versiones de clúster de Amazon Redshift disponibles y sus características, mejoras y correcciones, consulte [Anuncios del foro de mantenimiento de Amazon Redshift](#) en el foro de discusión de Amazon Redshift.

Consulta a una base de datos

Para realizar consultas en las bases de datos alojadas en su clúster de Amazon Redshift, tiene dos opciones:

- Conéctese a su clúster y ejecute consultas en la AWS Management Console con el editor de consultas.

Si utiliza el editor de consultas en la consola de Amazon Redshift, no tiene que descargar y configurar una aplicación de cliente SQL.

- Conéctese a su clúster a través de una herramienta de cliente SQL, como SQL Workbench/J.

Amazon Redshift es compatible con las herramientas de cliente SQL que se conectan a través de Java Database Connectivity (JDBC) y Open Database Connectivity (ODBC). Para utilizarlas, Amazon Redshift no proporciona ni instala ninguna biblioteca o herramienta de cliente SQL, por lo que debe instalarlas en el equipo cliente o la instancia de Amazon EC2. Puede utilizar la mayoría de las herramientas de cliente SQL compatibles con los controladores JDBC u ODBC.

Temas

- [Consulta de una base de datos mediante el editor de consultas \(p. 88\)](#)
- [Programar una consulta en la consola de Amazon Redshift \(p. 95\)](#)
- [Conexión a un clúster de Amazon Redshift mediante herramientas de cliente SQL \(p. 98\)](#)
- [Uso de la API de datos de Amazon Redshift \(p. 175\)](#)

Consulta de una base de datos mediante el editor de consultas

El editor de consultas es un método sencillo para ejecutar consultas en bases de datos alojadas en su clúster de Amazon Redshift. Después de crear su clúster, puede ejecutar consultas de forma inmediata usando el editor de consultas en la consola de Amazon Redshift.

En febrero de 2021, se implementó un editor de consultas actualizado y se modificaron los permisos de autorización para usar el editor de consultas. El nuevo editor de consultas utiliza la API de datos de Amazon Redshift para ejecutar consultas. `LaAmazonRedshiftQueryEditor`, que es una `AWS-administradasAWS Identity and Access Management(IAM)`, se actualizó para incluir los permisos necesarios. Si tiene una política de IAM personalizada, asegúrese de actualizarla. Usar `AmazonRedshiftQueryEditor` Como guía. Los cambios en `AmazonRedshiftQueryEditor` son:

- El permiso para administrar los resultados de la instrucción del editor de consultas requiere el usuario propietario de la instrucción.
- Se ha agregado permiso para usar el Secrets Manager para conectarse a una base de datos.

Para obtener más información, consulte [Permisos necesarios para usar el editor de consultas de consola Amazon Redshift \(p. 313\)](#).

Cuando se conecta al clúster desde el nuevo editor de consultas, puede utilizar uno de los dos métodos de autenticación, como se describe en [Conexión con el editor de consultas \(p. 90\)](#).

El editor de consultas antiguo está disponible en la consola de Amazon Redshift durante un tiempo limitado. Puede cambiar a él y volver a la página de la consola del editor de consultas. Con el editor de consultas antiguo, utilice los permisos existentes. Para obtener más información, consulte [Conectar con el editor de consultas antiguo \(p. 91\)](#).

Con el editor de consultas, puede realizar lo siguiente:

- Ejecutar consultas con instrucciones SQL.
- Descargar conjuntos de resultados de hasta 100 MB en un archivo de valores separados por comas (CSV).
- Guardar consultas para su reutilización. No puede guardar consultas en las regiones de Europa (París), Asia Pacífico (Osaka), Asia Pacífico (Hong Kong) o Oriente Medio (Bahréin).
- Ver los detalles de tiempo de ejecución de consultas para tablas definidas por los usuarios.
- Programe consultas para que se ejecuten en un momento futuro.
- Ver un historial de consultas que creó en el editor de consultas.
- Ejecute consultas en clústeres usando Enhanced VPC Routing.

Consideraciones sobre el editor de consultas

Debe tener en cuenta lo siguiente acerca del trabajo con consultas cuando utilice el editor de consultas:

- La duración máxima de una consulta es de 24 horas.
- El tamaño máximo del resultado de la consulta es de 100 MB. Si una llamada devuelve más de 100 MB de datos de respuesta, se terminará la llamada.
- El tiempo máximo de retención para los resultados de la consulta es de 24 horas.
- El tamaño máximo de instrucción de consulta es de 100 KB.
- El clúster debe estar en una nube virtual privada (VPC) basada en el servicio de Amazon VPC.
- No puede usar transacciones en el editor de consultas. Para obtener más información acerca de las transacciones, consulte [BEGIN](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Puede guardar una consulta con un tamaño máximo de 3.000 caracteres.

Habilitar el acceso al editor de consultas

Para obtener acceso al editor de consultas, necesita permiso. Para habilitar el acceso, Asocie el `AmazonRedshiftQueryEditor` a `AmazonRedshiftReadOnlyAccess` de IAM. Para obtener permisos de IAM para el usuario de IAM que utiliza para acceder al clúster. Puede usar la consola de IAM (<https://console.aws.amazon.com/iam/>) para adjuntar directivas de IAM.

Si ya ha creado un usuario de IAM para obtener acceso a Amazon Redshift, puede asociar el `AmazonRedshiftQueryEditor` a `AmazonRedshiftReadOnlyAccess` de IAM a ese usuario. Si aún no ha creado un usuario de IAM, cree uno y asocie la política al usuario de IAM.

La política administrada `AmazonRedshiftQueryEditor` permite la acción `redshift:GetClusterCredentials`, que de forma predeterminada concede a un usuario de base de datos acceso de superusuario a la base de datos. Para restringir el acceso, puede realizar una de las siguientes acciones:

- Crear una política personalizada que permita llamar `aredshift:GetClusterCredentials` y restrinja el recurso a un valor dado para `DbUser`.
- Agregue una directiva al usuario que deniegue el permiso `aredshift:GetClusterCredentials`, a continuación, requiere que los usuarios del editor de consultas inicien sesión con credenciales temporales. Por ejemplo, una política de denegación podría ser similar a la siguiente política.

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

```
"Action": "redshift:GetClusterCredentials",  
"Resource": "*" }  
}
```

Para obtener más información, consulte [Crear un rol o usuario de IAM con permisos para llamar a GetClusterCredentials \(p. 327\)](#).

Si se le concede acceso al editor de consultas de Amazon Redshift adjuntando el AWS-política administrada `AmazonRedshiftQueryEditor`, entonces puedes enumerar todos los secretos. Sin embargo, puede crear y recuperar sólo secretos etiquetados con la clave `RedshiftQueryOwnership` el valor `{aws:userid}`. Si crea la clave desde el editor de consultas de Amazon Redshift, la clave se etiquetará automáticamente. Para utilizar un secreto que no se creó con el editor de consultas de Amazon Redshift, confirme que el secreto está etiquetado con la clave `RedshiftQueryOwnership` un valor de su identificador de usuario único de IAM, por ejemplo `AIDACKCEVSQ6C2EXAMPLE`.

Para asociar las políticas de IAM necesarias al editor de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en <https://console.aws.amazon.com/iam/>.
2. Elija Users (Usuarios).
3. Seleccione el usuario que necesita obtener acceso al editor de consultas.
4. Elija Add permissions.
5. Elija Attach existing policies directly.
6. Para Policy names (Nombres de políticas), elija `AmazonRedshiftQueryEditor` y `AmazonRedshiftReadOnlyAccess`.
7. Seleccione Next (Siguiente): Consulte.
8. Elija Add permissions.

Conexión con el editor de consultas

Cuando se conecta a un clúster con el editor de consultas, puede usar uno de los siguientes métodos de autenticación. Cada método requiere una combinación diferente de entrada de la consola de Amazon Redshift.

AWS Secrets Manager

Con este método, proporcione un valor secreto para `secreto-arn` que se almacena en AWS Secrets Manager. Este secreto contiene credenciales para conectarse a la base de datos.

Credenciales temporales

Con este método, proporcione `subase de datos` y `Usuario de base de datos` Valores.

Almacenamiento de credenciales de base de datos en AWS Secrets Manager

Cuando llame al editor de consultas, puede pasar credenciales para el clúster usando un secreto en AWS Secrets Manager. Para pasar credenciales mediante este método, especifique el nombre o el Nombre de recurso de Amazon (ARN) del secreto.

Para obtener más información sobre los permisos mínimos, consulte [Creación y administración de secretos con AWS Secrets Manager](#) en la AWS Secrets Manager Guía del usuario.

Para almacenar sus credenciales en secreto para un clúster de Amazon Redshift

1. Usar AWS Secrets Manager Para crear un secreto que contenga credenciales para el clúster de. Cuando elige Almacenar un nuevo secreto, elija Credenciales para el clúster Redshift. Almacenar un valor para User name (Nombre de usuario): (el usuario de la base de datos), Contraseña, y Clúster de base de datos (identificador de clúster) en su secreto.

Para obtener instrucciones, consulte [Creación de un secreto básico](#) en la AWS Secrets Manager Guía del usuario.

2. Utilice la consola de AWS Secrets Manager para ver los detalles del secreto que ha creado, o ejecute el comando de la AWS CLI `aws secretsmanager describe-secret`.

Conectar con el editor de consultas antiguo

Los siguientes tipos de nodos de clúster son compatibles con el editor de consultas anterior:

- dc1.8xlarge
- dc2.large
- dc2.8xlarge
- ds2.8xlarge
- ra3.xplus
- ra3.4xlarge
- ra3.16xlarge

Debe ser consciente de las consideraciones siguientes al usar el editor de consultas antiguo en la consola de Amazon Redshift:

- Hasta 50 usuarios pueden conectarse al mismo tiempo a un clúster con el editor de consultas.
- El número máximo de usuarios que se conectan a un clúster incluye aquellos que se conectan a través del editor de consultas.
- Hasta 50 slots de consultas de Workload Management (WLM, Administración de cargas de trabajo) pueden estar activos al mismo tiempo. Para obtener más información sobre slots de consultas, consulte [Implementación de Workload Management](#).
- El editor de consultas solamente ejecuta consultas cortas que se pueden completar en menos de diez minutos.
- Los conjuntos de resultados de las consultas se paginan en 100 filas por página.
- No puede utilizar el editor de consultas con Enhanced VPC Routing. Para obtener más información, consulte [Enhanced VPC Routing](#) (p. 202).
- No puede usar transacciones en el editor de consultas. Para obtener más información acerca de las transacciones, consulte [BEGIN](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.
- Puede guardar una consulta con un tamaño máximo de 3.000 caracteres.

Para poder acceder al editor de consultas antiguo, necesita permiso. Para habilitar el acceso, Asocie el `AWSRedshiftQueryEditorAmazonRedshiftReadOnlyAccess` a la política administrada `AmazonRedshiftQueryEditor` para el usuario de IAM que utiliza para acceder al clúster.

Si ya ha creado un usuario de IAM para obtener acceso a Amazon Redshift, puede asociar el `AmazonRedshiftQueryEditorAmazonRedshiftReadOnlyAccess` a ese usuario. Si aún no ha creado un usuario de IAM, cree uno y asocie las políticas al usuario de IAM.

La política administrada `AmazonRedshiftQueryEditor` permite la acción `redshift:GetClusterCredentials`, que de forma predeterminada concede a un usuario de base de datos acceso de superusuario a la base de datos. Para restringir el acceso, puede realizar una de las siguientes acciones:

- Crear una política personalizada que permita llamar a `redshift:GetClusterCredentials` y restrinja el recurso a un valor dado para `DbUser`.
- Agregue una directiva al usuario que deniegue el permiso para `redshift:GetClusterCredentials`, a continuación, requiere que los usuarios del editor de consultas inicien sesión con credenciales temporales. Por ejemplo, una política de denegación podría ser similar a la siguiente política.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Deny",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "*"
  }
}
```

Para obtener más información, consulte [Crear un rol o usuario de IAM con permisos para llamar a `GetClusterCredentials` \(p. 327\)](#).

Cuando se conecta a un clúster con el editor de consultas antiguo, puede usar uno de los siguientes métodos de autenticación. Cada método requiere una combinación diferente de entrada de la consola de Amazon Redshift.

Connect con la contraseña de

Con este método, proporcione la contraseña de usuario principal para la base de datos predeterminada. Cuando creó el clúster de, proporcionó esta contraseña.

Credenciales temporales

Con este método, proporcione subbase de datos y Usuario de base de datos Valores.

Uso del editor de consultas

En el siguiente ejemplo, se utiliza el editor de consultas para realizar las siguientes tareas:

- Ejecutar comandos SQL.
- Ver detalles de ejecución de consultas.
- Guardar una consulta.
- Descargar un conjunto de resultados de consultas.

Para completar el siguiente ejemplo, necesita un clúster de Amazon Redshift. Si no dispone de un clúster, cree uno mediante el siguiente procedimiento que se describe en [Creación de un clúster \(p. 47\)](#).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para usar del editor de consultas en la consola de Amazon Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione EDITOR y conéctese a una base de datos de su clúster.
3. Para Schema (Esquema), elija public (público) para crear una nueva tabla basada en ese esquema.
4. En la ventana del editor de consultas, escriba lo siguiente y elija Run (Ejecutar) para crear una nueva tabla.

```
create table shoes(  
    shoetype varchar (10),  
    color varchar(10));
```

5. Elija Clear (Borrar).
6. Introduzca el siguiente comando en la ventana del editor de consultas y seleccione Run Query (Ejecutar consulta) para añadir filas a la tabla.

```
insert into shoes values  
( 'loafers', 'brown'),  
( 'sandals', 'black');
```

7. Elija Clear (Borrar).
8. En la ventana del editor de consultas, escriba el siguiente comando y elija Run (Ejecutar) para realizar una consulta en la nueva tabla.

```
select * from shoes;
```

Query results (Resultados de la consulta) mostrará los resultados.

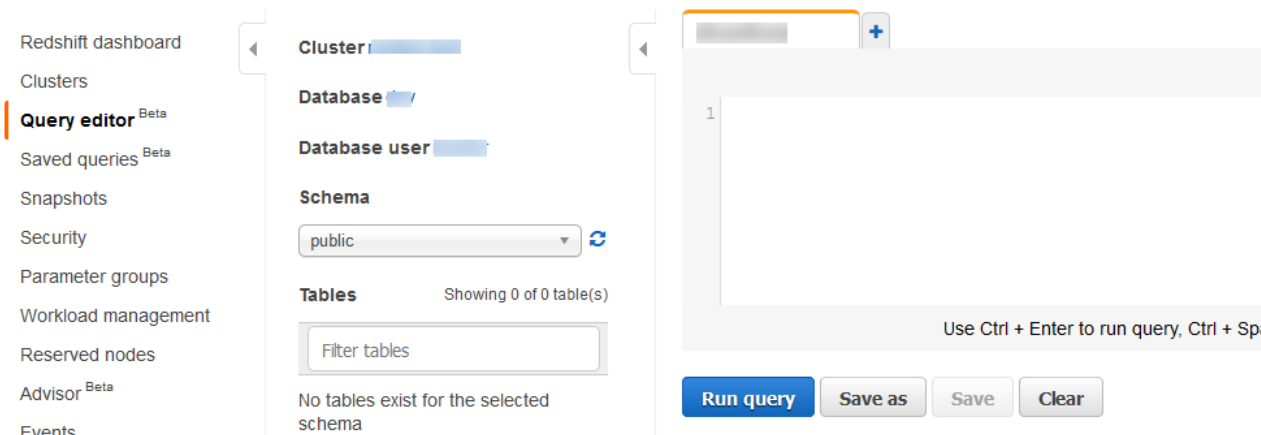
Tipo de calzado	Color
sandals	black
loafers	brown

9. Seleccione Execution (Ejecución) para ver los detalles de la ejecución.
10. Seleccione Data (Datos) y Export (Exportar) para descargar los resultados de la consulta como un archivo.

Consola original

Para usar del editor de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Query Editor (Editor de consultas).



3. Para Schema (Esquema), elija public (público) para crear una nueva tabla basada en ese esquema.
4. En la ventana del editor de consultas, escriba lo siguiente y elija Run Query (Ejecutar consulta) para crear una nueva tabla.

```
create table shoes(  
    shoetype varchar (10),  
    color varchar(10));
```

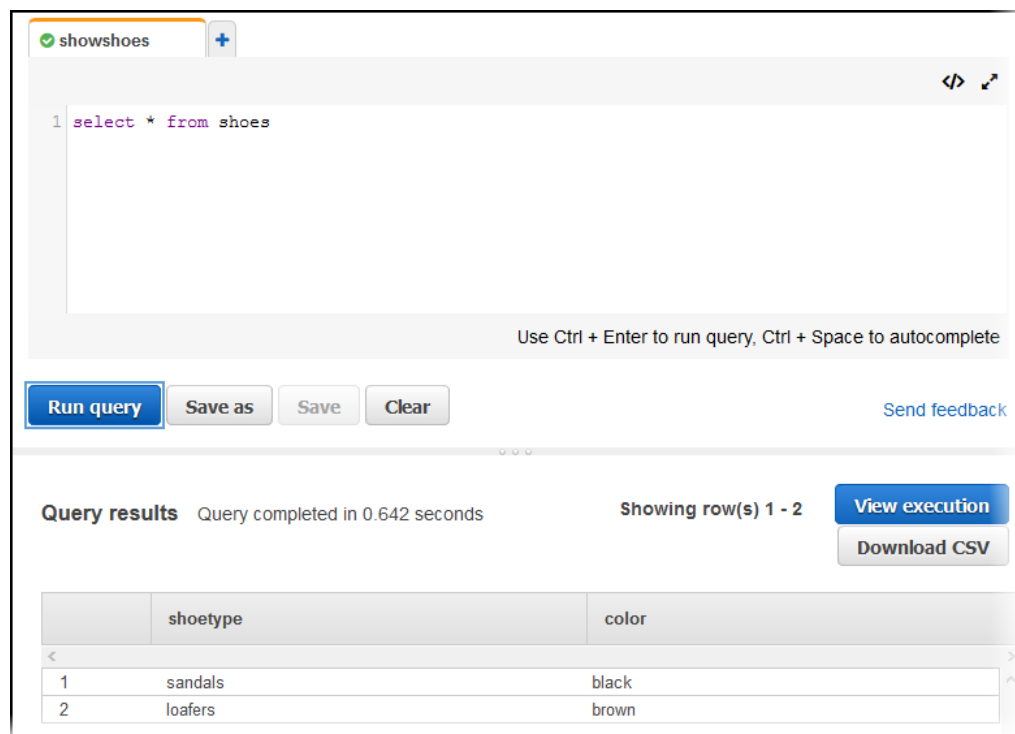
5. Elija Clear (Borrar).
6. En la ventana del editor de consultas, escriba el siguiente comando y elija Run Query (Ejecutar consulta) para agregar filas a la tabla.

```
insert into shoes values  
( 'loafers', 'brown'),  
( 'sandals', 'black');
```

7. Elija Clear (Borrar).
8. En la ventana del editor de consultas, escriba el siguiente comando y elija Run Query (Ejecutar consulta) para realizar una consulta en la nueva tabla.

```
select * from shoes;
```

Ahora debería ver los siguientes resultados.



9. Para ver los detalles de la ejecución, elija View execution (Ver ejecución).
10. Seleccione Download CSV (Descargar CSV) para descargar los resultados de la consulta como un archivo CSV.

Programar una consulta en la consola de Amazon Redshift

Para crear una programación para ejecutar una instrucción SQL, puede utilizar el editor de consultas en la consola de Amazon Redshift. Puede crear una programación para ejecutar la instrucción SQL en los intervalos de tiempo que coincidan con las necesidades de su empresa. Cuando llegue el momento de ejecutar la consulta programada, Amazon EventBridge inicia la consulta.

Para crear una programación para ejecutar una instrucción SQL en la consola de

1. Abra la consola y el editor de consultas como se describe en [Uso del editor de consultas \(p. 92\)](#).
2. Seleccione **Schedule** para crear una programación para ejecutar una instrucción SQL.

Cuando defina el programa, proporcione la siguiente información:

- Función de IAM que se utiliza para asumir los permisos necesarios para ejecutar la consulta. Para obtener más información, consulte [Configuración de permisos para programar una consulta en la consola de Amazon Redshift \(p. 96\)](#).
- Los valores de autenticación para AWS Secrets Manager credenciales temporales para autorizar el acceso al clúster. Para obtener más información, consulte [Autenticación de una consulta programada \(p. 97\)](#).
- El nombre de la consulta programada y una única instrucción SQL que se va a ejecutar.
- Las opciones de frecuencia de programación y repetición o un valor con formato cron.

- Si lo desea, puede habilitar las notificaciones de Amazon SNS para supervisar la consulta programada. Si su consulta se está ejecutando pero no ve mensajes publicados en su tema de SNS, consulte [Mi regla se activa pero no veo ningún mensaje publicado en mi tema de Amazon SNS](#) en la Guía del usuario de Amazon EventBridge.

También puede gestionar y actualizar consultas programadas mediante la consola de Amazon Redshift. Dependiendo de la versión de la consola, las consultas programadas pueden aparecer en los siguientes lugares:

- En la página **Schedules** de la página de detalles del clúster.
- En la lista de consultas programadas a la que puede acceder desde el panel de exploración. Para ver la lista, en el panel de navegación elija **QUERIES**, **Lista de consultas de programación**.
- En la página **Consultas programadas** del editor de consultas.

Si elige **Nombre del programador** en una de estas ubicaciones, puede ver y editar la definición de su consulta programada.

Configuración de permisos para programar una consulta en la consola de Amazon Redshift

Para programar consultas, el **AWS Identity and Access Management (IAM)** que define la programación y el rol de IAM asociado a la programación se debe configurar de la siguiente manera.

Para el usuario de IAM que ha iniciado sesión en la consola de Amazon Redshift, haga lo siguiente:

- Asociar el **AmazonEventBridgeFullAccess** AWS-política administrada.
- Asociar una política con el **sts:AssumeRole** El permiso de la IAM role (función de IAM) que especifica al definir la instrucción SQL programada.

En el siguiente ejemplo se muestra una política que asume un rol de IAM especificado.

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

Para el rol de IAM que especifique para permitir que el programador ejecute una consulta, haga lo siguiente:

- Asegúrese de que esta función de IAM especifique la entidad de servicio EventBridge (`events.amazonaws.com`). A continuación se muestra un ejemplo de relación de confianza.

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

```
        "Service": [
            "events.amazonaws.com"
        ],
        "Action": "sts:AssumeRole"
    }
]
```

Para obtener más información acerca de cómo crear un rol de IAM para eventos de EventBridge, consulte [Permisos necesarios para usar el programador de Amazon EventBridge \(p. 314\)](#).

- Asociar el `AmazonRedshiftDataFullAccess` AWSa la política administrada por IAM.
- Para permitir a los usuarios de IAM ver el historial de programación, edite el rol de IAM para agregar el `sts:AssumeRole` Permiso.

A continuación se muestra un ejemplo de la definición de un rol de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Sid": "AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/user-name"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

El siguiente fragmento de ejemplo permite a usuarios específicos de IAM ver el historial de programación.

```
{
  "Sid": "AssumeRole",
  "Effect": "Allow",
  "Principal": {
    "AWS": [
      "arn:aws:iam::account-id:user/testRedshiftUser",
      "arn:aws:iam::account-id:user/myusername"
    ]
  },
  "Action": "sts:AssumeRole"
}
```

Autenticación de una consulta programada

Cuando se programa una consulta, se utiliza uno de los métodos de autenticación siguientes cuando se ejecuta la consulta SQL. Cada método requiere una combinación diferente de entrada de la consola de Amazon Redshift.

AWS Secrets Manager

Con este método, proporcione un valor secreto para `secreto-arn` que se almacena en AWS Secrets Manager. Este secreto contiene credenciales para conectarse a la base de datos. El secreto debe estar etiquetado con la clave `RedshiftDataFullAccess`.

Para obtener más información sobre los permisos mínimos, consulte [Creación y administración de secretos con AWS Secrets Manager](#) en la [AWS Secrets Manager Guía del usuario](#).

Credenciales temporales

Con este método, proporcione `subase de datos` y `Usuario de base de datos` Valores.

La `AmazonRedshiftDataFullAccess` La política de `redshift_data_api_user` Permiso de `redshift:GetClusterCredentials`. Si desea utilizar un usuario de base de datos diferente para ejecutar la instrucción SQL, agregue una directiva a la función de IAM para permitir `redshift:GetClusterCredentials`. La política de ejemplo siguiente permite a los usuarios de la base `awsuser` y `myuser`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "UseTemporaryCredentialsForAllDbUsers",
      "Effect": "Allow",
      "Action": "redshift:GetClusterCredentials",
      "Resource": [
        "arn:aws:redshift:*:*:dbuser:*/awsuser",
        "arn:aws:redshift:*:*:dbuser:*/myuser"
      ]
    }
  ]
}
```

Conexión a un clúster de Amazon Redshift mediante herramientas de cliente SQL

Puede conectarse a clústeres de Amazon Redshift desde herramientas de cliente SQL mediante conexiones Java Database Connectivity (JDBC) y Open Database Connectivity (ODBC, Conectividad de base de datos abierta). Amazon Redshift no proporciona ni instala ninguna biblioteca o herramienta de cliente SQL. Para utilizar estas herramientas o bibliotecas para trabajar con datos de los clústeres, instálelas en el equipo cliente o instancia de Amazon EC2. Puede utilizar la mayoría de las herramientas de cliente SQL compatibles con los controladores JDBC u ODBC.

Puede utilizar las siguientes secciones para recorrer el proceso de configuración del equipo cliente o la instancia de Amazon EC2 para usar una conexión JDBC u ODBC. También discuten las opciones de seguridad relacionadas para la conexión del cliente al servidor. Además, a continuación, puede encontrar información sobre cómo configurar y conectar desde dos herramientas de cliente SQL de terceros, SQL Workbench/J y psql. Puede probar estas herramientas si aún no tiene una herramienta de inteligencia empresarial que usar. También puede utilizar esta sección para aprender sobre cómo conectarse a su clúster mediante programación. Por último, si surge algún problema cuando prueba conectarse a su clúster, puede revisar la información de solución de problemas de esta sección para identificar posibles soluciones.

Temas

- [Configuración de conexiones en Amazon Redshift \(p. 99\)](#)

- [Configuración de las opciones de seguridad para las conexiones \(p. 151\)](#)
- [Conexión a clústeres desde herramientas y código cliente \(p. 157\)](#)
- [Solución de problemas de conexión en Amazon Redshift \(p. 169\)](#)

Configuración de conexiones en Amazon Redshift

En la siguiente sección, puede encontrar cómo configurar conexiones JDBC y ODBC para conectarse al clúster desde las herramientas de cliente SQL. En esta sección se describe cómo configurar conexiones JDBC y ODBC. También describe cómo utilizar la Capa de conexión segura (SSL) y certificados de servidor para cifrar la comunicación entre el cliente y el servidor.

Temas

- [Controladores JDBC y ODBC para Amazon Redshift \(p. 99\)](#)
- [Configuración de una conexión de controlador JDBC versión 2.0 \(p. 100\)](#)
- [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#)
- [Configuración de una conexión ODBC \(p. 138\)](#)

Controladores JDBC y ODBC para Amazon Redshift

Para trabajar con datos en su clúster, necesita controladores JDBC u ODBC a fin de establecer una conectividad desde su equipo cliente o instancia. Cifre sus aplicaciones para usar una API de acceso a datos JDBC u ODBC y utilice las herramientas de cliente SQL que sean compatibles con JDBC o bien con ODBC.

Amazon Redshift ofrece controladores JDBC y ODBC para descargar. Anteriormente, Amazon Redshift recomendaba controladores PostgreSQL para JDBC y ODBC. Si utilizas estos controladores, te recomendamos que cambies a los nuevos controladores específicos de Amazon Redshift. Para obtener más información acerca de cómo descargar los controladores JDBC y ODBC y cómo configurar las conexiones al clúster, consulte [Configuración de una conexión de controlador JDBC versión 2.0 \(p. 100\)](#), [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#), y [Configuración de una conexión ODBC \(p. 138\)](#).

Para el controlador JDBC versión 1.2.47.1071 o posterior y la versión 1.4.16.1000 del controlador ODBC o posterior, Amazon Redshift debe ser la versión 1.0.17708 o posterior. Para verificar la versión de Amazon Redshift, consulte [VERSION](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Obtención de la cadena de conexión a su clúster

Para conectarse al clúster con su herramienta de cliente SQL, necesita la cadena de conexión al clúster. Puede encontrar la cadena de conexión al clúster en la consola de Amazon Redshift, en la página de detalles del clúster.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para encontrar la cadena de conexión de un clúster

1. Inicie sesión en la [AWS Management Console](#) y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.

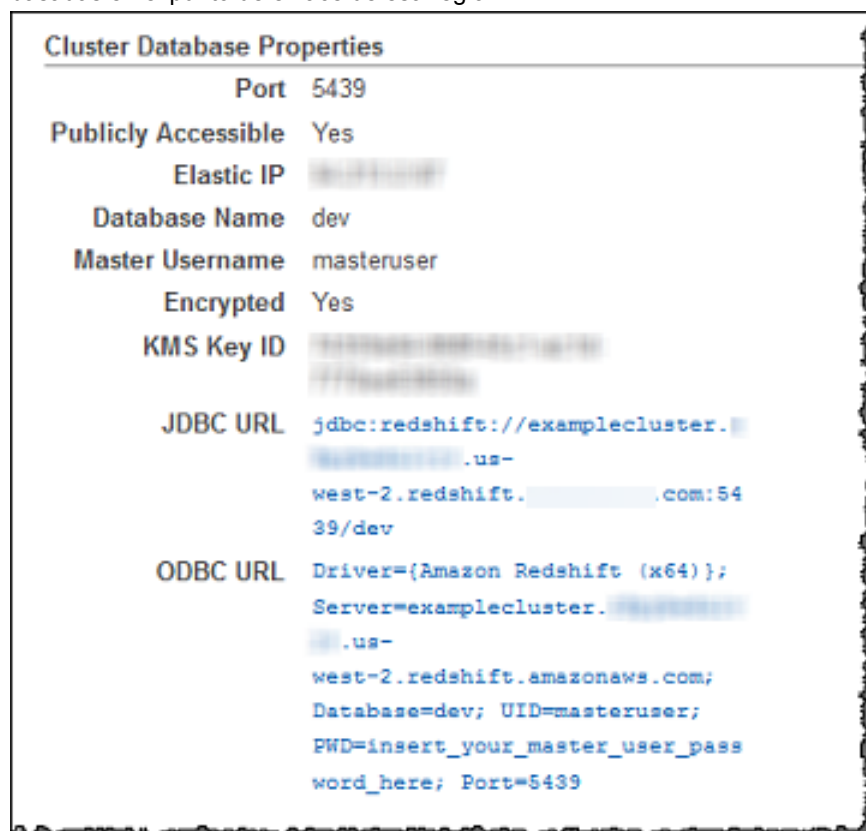
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles.
3. La DIRECCIÓN URL DE JDBC y DIRECCIÓN URL DE ODBC están disponibles, junto con detalles adicionales, en la sección Información general. Cada cadena se basa en la región de AWS en la que se ejecuta el clúster. Haga clic en el icono situado junto a la cadena de conexión adecuada para copiarlo.

Consola original

Pasos para obtener la cadena de conexión a su clúster

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En la página Clusters (Clústeres), haga clic en el nombre del clúster del que desea obtener la cadena de conexión.
3. En la pestaña Configuration (Configuración) del clúster, en JDBC URL (URL del JDBC) o en ODBC URL (URL del ODBC), copie la cadena de conexión.

En el siguiente ejemplo se muestran las cadenas de conexión de un clúster lanzado en la región EE. UU. Oeste (Oregón). Si inicia el clúster en una región de AWS, las cadenas de conexión están basadas en el punto de enlace de esa región.



Configuración de una conexión de controlador JDBC versión 2.0

Puede utilizar una conexión de controlador JDBC versión 2.0 para conectarse a su clúster de Amazon Redshift desde distintas herramientas de cliente SQL de terceros. Para hacer esto, descargue un controlador JDBC.

Para usar una conexión JDBC, consulte las siguientes secciones.

Temas

- [Descargue el controlador de Amazon Redshift JDBC versión 2.0](#) (p. 101)
- [Instalación del controlador JDBC de Amazon Redshift versión 2.0](#) (p. 102)
- [Hacer referencia a las bibliotecas de controladores JDBC](#) (p. 102)
- [Registro de la clase de controlador](#) (p. 102)
- [Obtención de la URL de JDBC](#) (p. 103)
- [Creación de la URL de conexión](#) (p. 104)
- [Configurar conexiones de mantenimiento de TCP para su conexión JDBC de su conexión JDBC de](#) (p. 105)
- [Configurar su conexión JDBC con Apache Maven](#) (p. 105)
- [Configurar la autenticación y SSL](#) (p. 107)
- [Configuración de registros de](#) (p. 110)
- [Convertir tipos de datos](#) (p. 112)
- [Utilizar compatibilidad con declaraciones preparadas](#) (p. 112)
- [Diferencias entre las versiones 2.x y 1.x del controlador JDBC](#) (p. 113)
- [Opciones de configuración del controlador JDBC versión 2.0](#) (p. 114)
- [Versiones anteriores del controlador JDBC versión 2.0](#) (p. 129)

Descargue el controlador de Amazon Redshift JDBC versión 2.0

Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2.

Para obtener información detallada acerca de cómo instalar el controlador JDBC de, consulte las bibliotecas de controladores JDBC y registre la clase de controlador, consulte los siguientes temas.

Los controladores JDBC versión 1.2.27.1051 y posteriores admiten los procedimientos almacenados de Amazon Redshift. Para obtener más información, consulte [Creación de procedimientos almacenados en Amazon Redshift](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Para cada equipo en el que utilice el controlador JDBC de Amazon Redshift versión 2.0, asegúrese de que Java Runtime Environment (JRE) 8.0 esté instalado.

Si utiliza el controlador JDBC de Amazon Redshift para la autenticación de bases de datos, asegúrese de tener AWS SDK for Java 1.11.118 o posterior en la ruta de clases de Java. Si no dispone de AWS SDK for Java instalado, descargue el archivo ZIP con el controlador compatible con JDBC 4.2 (sin AWS SDK) y las bibliotecas dependientes del controlador para AWS SDK:

- [Controlador compatible con JDBC 4.2 \(sin el AWS SDK\) y bibliotecas dependientes del controlador para AWS, archivos SDK, versión 2.0.](#)

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Este archivo ZIP contiene el controlador compatible con JDBC 4.2 (sin AWS SDK) y sus archivos de biblioteca dependientes. Descomprima los archivos jar dependientes en la misma ubicación que el controlador JDBC. Solo el controlador JDBC necesita estar en el CLASSPATH porque el archivo de manifiesto del controlador contiene todos los nombres de archivo de biblioteca dependientes que se encuentran en el mismo directorio que el controlador JDBC de.

Utilice este controlador JDBC de Amazon Redshift con el AWS SDK que se requiere para AWS Identity and Access Management Autenticación de base de datos de base de datos

- [Controlador compatible con JDBC 4.2 \(sin el AWS SDK\), versión 2.0.](#)

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Revise la licencia de software JDBC versión 2.0 y el archivo de registro de cambios:

- [Licencia del controlador JDBC versión 2.0](#)
- [Registro de cambios de la versión 2.0 del controlador JDBC](#)

Si su herramienta requiere una versión anterior específica de un controlador JDBC versión 2.0, consulte [Versiones anteriores del controlador JDBC versión 2.0](#) (p. 129).

Instalación del controlador JDBC de Amazon Redshift versión 2.0

Para instalar el controlador compatible con Amazon Redshift JDBC 4.2 (sinAWSSDK) y bibliotecas dependientes del controlador paraAWSSDK versión 2.0, extraiga los archivos del archivo ZIP al directorio de su elección.

Para instalar el controlador compatible con Amazon Redshift JDBC 4.2 (sinAWSSDK) versión 2.0, copie el archivo JAR en el directorio de su elección.

Para acceder a un almacén de datos de Amazon Redshift mediante el controlador JDBC de Amazon Redshift, debe realizar la configuración como se describe a continuación.

Hacer referencia a las bibliotecas de controladores JDBC

La aplicación JDBC o el código Java que utiliza para conectarse a los datos debe tener acceso a los archivos JAR del controlador. En la aplicación o el código, especifique todos los archivos JAR que extrajo del archivo ZIP.

Uso del controlador en una aplicación JDBC

Las aplicaciones JDBC generalmente proporcionan un conjunto de opciones de configuración para agregar una lista de archivos de biblioteca de controladores. Utilice las opciones proporcionadas para incluir todos los archivos JAR del archivo ZIP como parte de la configuración del controlador en la aplicación. Para obtener más información, consulte la documentación de su aplicación JDBC.

Usar el controlador en código Java

Debe incluir todos los archivos de biblioteca de controladores en la ruta de clase. Esta es la ruta que Java Runtime Environment busca clases y otros archivos de recursos. Para obtener más información, consulte la documentación correspondiente a Java SE para establecer la ruta de clase de su sistema operativo.

- Windows: <https://docs.oracle.com/javase/7/docs/technotes/tools/windows/classpath.html>
- Linux y Solaris: <https://docs.oracle.com/javase/7/docs/technotes/tools/solaris/classpath.html>

Registro de la clase de controlador

Asegúrese de registrar la clase adecuada para su aplicación. Utilice las siguientes clases para conectar el controlador JDBC de Amazon Redshift a los almacenes de datos de Amazon Redshift:

- `Driver` Extende `classesjava.sql.Driver`.
- `DataSource` Extenden `classesjavax.sql.DataSource` y `javax.sql.ConnectionPoolDataSource`.

El controlador admite los siguientes nombres de clase completamente cualificados que son independientes de la versión de JDBC:

- `com.amazon.redshift.jdbc.Driver`
- `com.amazon.redshift.jdbc.DataSource`

En el siguiente ejemplo se demuestra cómo usar la clase `DriverManager` para establecer una conexión para JDBC 4.2.

```
private static Connection connectViaDM() throws Exception
{
    Connection connection = null;
    connection = DriverManager.getConnection(CONNECTION_URL);
    return connection;
}
```

En el siguiente ejemplo se muestra cómo utilizar `DataSource` para establecer una conexión.

```
private static Connection connectViaDS() throws Exception
{
    Connection connection = null;
    11
    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;
}
```

Obtención de la URL de JDBC

Para poder conectarse a su clúster de Amazon Redshift desde una herramienta de cliente SQL, necesita saber la URL de JDBC de su clúster. El URL de JDBC tiene el siguiente formato:

`jdbc:redshift://endpoint:port/database`

Los campos del formato anterior tienen los siguientes valores.

Campo	Valor
<code>jdbc</code>	Protocolo para la conexión.
<code>redshift</code>	Subprotocolo que especifica el uso de un controlador de Amazon Redshift para conectarse a la base de datos.
<code><i>endpoint</i></code>	El punto de enlace del clúster de Amazon Redshift.
<code><i>port</i></code>	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.
<code><i>database</i></code>	Base de datos que creó para su clúster.

A continuación, se muestra un ejemplo de la URL de un JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Asegúrese de introducir los valores de URL, por ejemplo los valores de `SessionToken`, en formato codificado por URL.

Para obtener información acerca de cómo crear su propia conexión JDBC, consulte [Obtención de la cadena de conexión a su clúster](#) (p. 99).

Si el equipo cliente no puede conectarse a la base de datos, puede solucionar los posibles problemas. Para obtener más información, consulte [Solución de problemas de conexión en Amazon Redshift](#) (p. 169).

Creación de la URL de conexión

Utilice la dirección URL de conexión para proporcionar información de conexión al almacén de datos al que está accediendo. A continuación se muestra el formato de la dirección URL de conexión para el controlador JDBC de Amazon Redshift versión 2.0. Aquí, [Host] el punto final del servidor Amazon Redshift y [Puerto] es el número del puerto TCP que el servidor utiliza para escuchar las solicitudes de los clientes.

```
jdbc:redshift://[Host]:[Port]
```

De forma predeterminada, Amazon Redshift usa el puerto 5439.

A continuación se muestra el formato de una dirección URL de conexión que especifica algunas opciones de configuración.

```
jdbc:redshift://[Host]:[Port]/[Schema];[Property1]=[Value];  
[Property2]=[Value];
```

Por ejemplo, suponga que desea conectarse a puerto 9000 de un clúster de Amazon Redshift de la región EE. UU. Oeste (Norte de California) en AWS. También desea acceder al esquema denominado Predeterminado y autenticar la conexión mediante un nombre de usuario y una contraseña. En este caso, se utiliza la dirección URL de conexión siguiente.

```
jdbc:redshift://redshift.company.us-west-  
1.redshift.amazonaws.com:9000/Default;UID=amazon;PWD=amazon
```

Puede utilizar los siguientes caracteres para separar las opciones de configuración en la cadena URL:

- ;
- ?
- &

Por ejemplo, las siguientes cadenas de URL son equivalentes:

```
jdbc:redshift://my_host:5439/dev;ssl=false;defaultRowFetchSize=100
```

```
jdbc:redshift://my_host:5439/dev?ssl=false?defaultRowFetchSize=100
```

En el siguiente ejemplo de URL se especifica un nivel de registro de 6 y la ruta de acceso de los registros.

```
jdbc:redshift://redshift.amazonaws.com:5439/dev;DSILogLevel=6;LogPath=/home/user/logs";
```

No duplique propiedades en la dirección URL de conexión.

Para obtener una lista completa de las opciones de configuración que puede especificar, consulte [Opciones de configuración del controlador JDBC versión 2.0](#) (p. 114).

Configurar conexiones de mantenimiento de TCP para su conexión JDBC de su conexión JDBC de

De forma predeterminada, el controlador JDBC de Amazon Redshift está configurado para usar conexiones keepalive de TCP para evitar que se agote el tiempo de espera en las conexiones. Puede especificar cuándo comienza el controlador a enviar paquetes keepalive o deshabilitar la característica estableciendo las propiedades correspondientes en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte [Creación de la URL de conexión](#) (p. 104).

Propiedad	Descripción
<code>TCPKeepAliveMinutes</code>	Para especificar cuándo el controlador envía paquetes keepalive, establezca el número de minutos de inactividad antes de que el controlador comience a enviar paquetes TCP keepalive.
<code>TCPKeepAlive</code>	Para deshabilitar Keepalives TCP, establezca esta propiedad en <code>FALSE</code> .

Configurar su conexión JDBC con Apache Maven

Apache Maven es una herramienta de software para la comprensión y administración de proyectos. La AWS SDK for Java es compatible con los proyectos Apache Maven. Para obtener más información, consulte [Uso del SDK con Apache Maven](#) en la AWS SDK for Java Guía para desarrolladores de .

Si utiliza Apache Maven, puede configurar y crear sus proyectos de forma que utilicen un controlador JDBC de Amazon Redshift para conectarse al clúster de Amazon Redshift. Para hacerlo, agregue el controlador JDBC como dependencia en el archivo `pom.xml` de su proyecto. Si usa Maven para configurar su proyecto y desea usar una conexión JDBC, siga los pasos que se indican en la siguiente sección.

Configuración del controlador JDBC como una dependencia de Maven

Pasos para configurar el controlador JDBC como una dependencia de Maven

1. Añada el repositorio de Amazon o el repositorio de Maven Central a la sección de repositorios de `pom.xml`.

Note

La URL del siguiente código devuelve un error si se utiliza en un navegador. Utilice esta URL solo en el contexto de un proyecto Maven.

A. Repositorio de Amazon Maven.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
  </repository>
</repositories>
```

Para conectarse utilizando SSL, añada el siguiente repositorio al archivo `pom.xml`.

```
<repositories>
  <repository>
```

```
<id>redshift</id>
<url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
</repository>
</repositories>
```

B. Repositorio Central de Maven. Añada lo siguiente al archivo `pom.xml` file.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://repo1.maven.org/maven2</url>
  </repository>
</repositories>
```

2. Declare la versión del controlador que desea usar en la sección de dependencias de su archivo `pom.xml`.

Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2. Para obtener información acerca de la funcionalidad admitida por estos controladores, consulte [Descargar un controlador JDBC de Amazon Redshift \(p. 130\)](#).

Añada una dependencia para el controlador de la siguiente lista.

Reemplazar `driver-version` en el ejemplo siguiente con su versión del controlador. Por ejemplo, `2.0.0.0`.

- Controlador compatible con JDBC 4.2:

```
<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42</artifactId>
  <version>driver-version</version>
</dependency>
```

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Los controladores de Amazon Redshift Maven necesitan las siguientes dependencias opcionales cuando se utiliza la autenticación de base de datos de IAM.

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-core</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-redshift</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-sts</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
```

Si su herramienta requiere una versión anterior específica de un controlador, consulte [Uso de versiones anteriores del controlador JDBC con Maven](#) (p. 137).

Actualización a la versión más reciente del controlador

Para actualizar o cambiar el controlador JDBC de Amazon Redshift a la versión más reciente, modifique primero la sección de versión de la dependencia a la última versión del controlador. Luego limpie su proyecto con el Maven Clean Plugin, como se indica a continuación.

```
mvn clean
```

Configurar la autenticación y SSL

Para proteger los datos contra accesos no autorizados, los almacenes de datos de Amazon Redshift requieren la autenticación de todas las conexiones mediante credenciales de usuario. Algunos almacenes de datos también requieren que las conexiones se realicen a través del protocolo Secure Sockets Layer (SSL), ya sea con o sin autenticación unidireccional.

El controlador JDBC de Amazon Redshift versión 2.0 proporciona total compatibilidad con estos protocolos de autenticación.

La versión SSL que admite el controlador depende de la versión de JVM que esté utilizando. Para obtener información acerca de las versiones SSL compatibles con cada versión de Java, consulte [Diagnóstico de TLS, SSL y HTTPS](#) en el blog de administración de productos de Java Platform Group.

La versión SSL utilizada para la conexión es la versión más alta que admite el controlador y el servidor, que se determina en el momento de la conexión.

Configure el controlador JDBC de versión 2.0 de Amazon Redshift JDBC para autenticar la conexión de acuerdo con los requisitos de seguridad del servidor de Amazon Redshift al que se está conectando.

Siempre debe proporcionar su nombre de usuario y contraseña de Amazon Redshift para autenticar la conexión. En función de si SSL está habilitado y requerido en el servidor, es posible que también necesite configurar el controlador para que se conecte a través de SSL. O puede usar la autenticación SSL unidireccional para que el cliente (el propio controlador) verifique la identidad del servidor.

Proporcione la información de configuración al controlador en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte [Creación de la URL de conexión](#) (p. 104).

SSL indica TLS/SSL, tanto Seguridad de la capa de transporte como Capa de sockets seguros. El controlador admite versiones estándar del sector de TLS/SSL.

Uso de nombre de usuario y contraseña

Si el servidor al que se está conectando no utiliza SSL, solo necesita proporcionar su nombre de usuario y contraseña para autenticar la conexión.

Para configurar la autenticación utilizando sólo su nombre de usuario y contraseña

1. Establecimiento de la propiedad `USER` a su nombre de usuario para acceder al servidor de Amazon Redshift.
2. Establezca la propiedad `PWD` en la contraseña correspondiente a su nombre de usuario.

Uso de SSL sin verificación de identidad

Si el servidor al que se está conectando utiliza SSL pero no requiere verificación de identidad, puede configurar el controlador para que utilice una fábrica SSL no validada.

Para configurar una conexión SSL sin verificación de identidad

1. Establecimiento de la propiedad de `UID` a su nombre de usuario para acceder al servidor de Amazon Redshift.
2. Establecimiento de la propiedad de `PWD` a la contraseña correspondiente a su nombre de usuario.
3. Establecimiento de la propiedad de `SSLFactoryPropiedad` a `com.amazon.redshift.ssl.NonValidatingFactory`.

Uso de la autenticación SSL unidireccional

Si el servidor al que se está conectando utiliza SSL y tiene un certificado, puede configurar el controlador para verificar la identidad del servidor mediante la autenticación unidireccional.

La autenticación unidireccional requiere un certificado SSL firmado y de confianza para verificar la identidad del servidor. Puede configurar el controlador para que use un certificado específico o acceda a un `TrustStore` que contenga el certificado apropiado. Si no especifica un certificado o `TrustStore`, el controlador utiliza el `TrustStore` predeterminado de Java (normalmente `jssecacerts` o `cacerts`).

Para configurar la autenticación SSL unidireccional

1. Establezca la propiedad `UID` en su nombre de usuario para acceder al servidor de Amazon Redshift.
2. Establezca la propiedad `PWD` en la contraseña correspondiente a su nombre de usuario.
3. Establezca la propiedad `SSL` en `true`.
4. Establezca la propiedad `SSLRootCert` en la ubicación del certificado de CA raíz.
5. Si no utiliza uno de los `TrustStores` de Java predeterminados, realice alguna de las siguientes operaciones:
 - Para especificar un certificado de servidor, establezca la propiedad `SSLRootCert` en la ruta de acceso completa del certificado.
 - O bien, para especificar un `TrustStore`, haga lo siguiente:
 - a. Utilice el programa `keytool` para agregar el certificado de servidor al `TrustStore` que desea utilizar.
 - b. Especifique el `TrustStore` y la contraseña que se usarán al iniciar la aplicación Java con el controlador. Por ejemplo:

```
-Djavax.net.ssl.trustStore=[TrustStoreName]  
-Djavax.net.ssl.trustStorePassword=  
[TrustStorePassword]
```

6. Elija una:
 - Para validar el certificado, establezca la propiedad `SSLMode` en `verify-ca`.
 - O bien, para validar el certificado y verificar el nombre de host del certificado, establezca la propiedad `SSLMode` en `verify-full`.

Configuración de la autenticación IAM

Si se conecta a un servidor de Amazon Redshift mediante la autenticación de IAM, establezca las siguientes propiedades como parte de la cadena de conexión de origen de datos.

Para obtener más información acerca de la autenticación de IAM, consulte [Administración de identidades y accesos en Amazon Redshift \(p. 304\)](#).

Para utilizar la autenticación de IAM, utilice uno de los siguientes formatos de cadenas de conexión:

Cadena de conexión	Descripción
<code>jdbc:redshift:iam:// [host]:[port]/[db]</code>	Una cadena de conexión normal. El controlador deduce el ClusterID y la región del host.
<code>jdbc:redshift:iam:// [cluster-id]:[region]/[db]</code>	El controlador recupera la información del host, dado el ClusterID y la región.
<code>jdbc:redshift:iam:// [host]/[db]</code>	El controlador toma de forma predeterminada el puerto 5439 e infiere ClusterID y Región del host.

Especificación de perfiles

Si utiliza la autenticación de IAM, tiene la opción de especificar las propiedades de conexión adicionales requeridas u opcionales bajo un nombre de perfil. Esto le permite evitar poner cierta información directamente en la cadena de conexión. Especifique el nombre del perfil en la cadena de conexión mediante la propiedad Profile.

Los perfiles se pueden agregar a laAWSArchivo de credenciales. La ubicación predeterminada de este archivo es:~/.aws/credentials

Puede cambiar el valor predeterminado configurando la ruta en la siguiente variable de entorno:AWS_CREDENTIAL_PROFILES_FILE

Para obtener más información acerca de los perfiles, consulte[Uso deAWSCredenciales](#)en laAWS SDK for Java.

Uso de credenciales de perfil de instancia

Si ejecuta una aplicación en una instancia EC2 asociada con una función de IAM, puede conectarse mediante las credenciales de perfil de instancia.

Para ello, utilice uno de los formatos de cadena de conexión de IAM de la tabla anterior y establezca la propiedad de conexión dbuser en el nombre de usuario de Amazon Redshift con el que se está conectando.

Para obtener más información acerca de los perfiles de instancia, consulte[Administración de accesos](#)en laGuía del usuario de IAM.

Uso de proveedores de credenciales

El controlador también admite complementos de proveedor de credenciales de los siguientes servicios:

- AD FS
- Azure AD
- Okta
- PingFederate

Si utiliza uno de estos servicios, la dirección URL de conexión debe especificar las siguientes propiedades:

- Plugin_Name— La ruta de clase completa para la clase de complemento del proveedor de credenciales.
- IDP_host: — El host del servicio que está utilizando para autenticarse en Amazon Redshift.
- idp_port— El puerto que escucha el host para el servicio de autenticación. No es necesario para Okta.
- Usuario— El nombre de usuario del servidor idp_host.
- Contraseña— La contraseña asociada con el nombre de usuario idp_host.
- DbUser— El nombre de usuario de Amazon Redshift con el que se está conectando.

- `SSL_insecure`— Indica si se debe verificar el certificado del servidor IDP.
- `client_id`: el ID de cliente asociado con el nombre de usuario en el portal de Azure AD. Solo se usa para Azure AD.
- `client_secret`: secreto de cliente asociado con el ID de cliente en el portal de Azure AD. Solo se usa para Azure AD.
- `IDP_tenant`: el ID de inquilino de Azure AD para su aplicación de Amazon Redshift. Solo se usa para Azure AD.
- `app_id`— El ID de la aplicación de Okta para su aplicación de Amazon Redshift. Solo se usa para Okta.
- `App_Name`: el nombre opcional de la aplicación Okta para su aplicación de Amazon Redshift. Solo se usa para Okta.
- `Partner_SPID`— El valor opcional SPID (ID de proveedor de servicios) del socio. Sólo se usa para PingFederate.

Si está utilizando un complemento de navegador para uno de estos servicios, la URL de conexión también puede incluir:

- URL de inicio de sesión: la dirección URL del recurso en el sitio web del proveedor de identidades cuando se utilizan los servicios SAML o Azure AD a través de un complemento del explorador. Este parámetro es necesario si está utilizando un complemento de navegador.
- `Listen_port`: el puerto que utiliza el controlador para obtener la respuesta SAML del proveedor de identidades al usar los servicios SAML o Azure AD a través de un complemento del explorador.
- `IDP_Response_Timeout`— La cantidad de tiempo, en segundos, que el controlador espera la respuesta SAML del proveedor de identidades al usar los servicios SAML o Azure AD a través de un complemento del explorador.

Para obtener información sobre propiedades adicionales de cadenas de conexión, consulte [Opciones de configuración del controlador JDBC versión 2.0](#) (p. 114).

Configuración de registros de

Puede habilitar el registro en el controlador para ayudar a diagnosticar problemas.

Para registrar la información del controlador, tiene los siguientes métodos:

- Para guardar la información registrada en `archivos.log`, consulte [Uso de archivos de registro de](#) (p. 110).
- Para enviar información registrada a `LogStream` o `LogWriter` especificados en `DriverManager`, consulte [Uso de LogStream o LogWriter](#) (p. 111).

Proporcione la información de configuración al controlador en la URL de conexión. Para obtener más información acerca de la sintaxis de la URL de conexión, consulte [Creación de la URL de conexión](#) (p. 104).

Uso de archivos de registro de

Solo debe habilitar el registro el tiempo suficiente para capturar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Configure la clave `LogLevel` en la URL de conexión para habilitar el registro y especifique el nivel de detalles que se incluye en los archivos de registro. En la siguiente tabla se enumeran los niveles de registro proporcionados por el controlador JDBC de Amazon Redshift versión 2.0, con el fin de que sea menos detallado a más detallado.

LogLevel	Descripción
1	Registrar eventos de errores graves que harán que el controlador se anule.
2	Registrar eventos de errores que podrían permitir que el controlador siga ejecutándose.
3	Registrar eventos que pueden dar lugar a un error si no se realiza la acción.
4	Registrar información general que describa el progreso del controlador
5	Registrar información detallada útil para depurar el controlador
6	Registrar toda la actividad del controlador.

Para habilitar el registro que utiliza archivos de registro

1. Establezca la propiedad LogLevel en el nivel de información que desee incluir en los archivos de registro.
2. Establezca la propiedad LogPath en la ruta completa de la carpeta en la que desea guardar los archivos de registro.

Por ejemplo, la siguiente dirección URL de conexión habilita el nivel de registro 3 y guarda los archivos de registro en la carpeta C:\temp:jdbc:redshift://redshift.company.us-west-1.redshift.amazonaws.com:9000/Default;DSILogLevel=3; LogPath=C:\temp

3. Para asegurarse de que la nueva configuración surta efecto, reinicie la aplicación JDBC y vuelva a conectarse al servidor.

El controlador JDBC de Amazon Redshift produce los siguientes archivos de registro en la ubicación especificada en la propiedad LogPath:

- redshift_jdbc.log que registra la actividad del controlador que no es específica de una conexión.
- redshift_jdbc_connection_[Número].log para cada conexión realizada a la base de datos, donde [Número] es un número que identifica cada archivo de registro. Este archivo registra la actividad del controlador que es específica de la conexión.

Si el valor de LogPath no es válido, el controlador envía la información registrada a la secuencia de salida estándar (System.out)

Uso de LogStream o LogWriter

Solo habilite el registro el tiempo suficiente para capturar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Establezca la clave LogLevel en la dirección URL de conexión para habilitar el registro y especifique la cantidad de detalles enviados a LogStream o LogWriter especificados en DriverManager.

Para habilitar el registro que utiliza LogStream o LogWriter:

1. Para configurar el controlador para registrar información general que describe el progreso del controlador, establezca la propiedad LogLevel en 1 o INFO.
2. Para asegurarse de que la nueva configuración surta efecto, reinicie la aplicación JDBC y vuelva a conectarse al servidor.

Para deshabilitar el registro que utiliza LogStream o LogWriter:

1. Quite la propiedad LogLevel de la dirección URL de conexión.
2. Para asegurarse de que la nueva configuración surta efecto, reinicie la aplicación JDBC y vuelva a conectarse al servidor.

Convertir tipos de datos

El controlador JDBC de Amazon Redshift versión 2.0 admite muchos formatos de datos comunes, convirtiendo entre los tipos de datos de Amazon Redshift, SQL y Java.

En la tabla siguiente se muestran las asignaciones de tipos de datos admitidas.

Tipo de Amazon Redshift	Tipo de SQL	Tipo de Java
BIGINT	SQL_BIGINT	Long
BOOLEANO	SQL_BIT	Booleano
CHAR	SQL_CHAR	Cadena
FECHA	SQL_TYPE_DATE	java.sql.Date
DECIMAL	SQL_NUMÉRICO	BigDecimal
DOUBLE PRECISION	SQL_DOUBLE	Double
GEOMETRY	SQL_LONGVARBINARY	byte[]
INTEGER	SQL_INTEGER	Entero
OID	SQL_BIGINT	Long
SUPER	SQL_LONGVARCHAR	Cadena
REAL	SQL_REAL	Float
SMALLINT	SQL_SMALLINT	Short
TEXT	SQL_VARCHAR	Cadena
TIME	SQL_TYPE_TIME	java.sql.time
TIMETZ	SQL_TYPE_TIME	java.sql.time
TIMESTAMP	MARCA DE TIEMPO SQL_TYPE_	java.sql.Timestamp
TIMESTAMPTZ	MARCA DE TIEMPO SQL_TYPE_	java.sql.Timestamp
VARCHAR	SQL_VARCHAR	Cadena

Utilizar compatibilidad con declaraciones preparadas

El controlador JDBC de Amazon Redshift admite instrucciones preparadas. Puede utilizar instrucciones preparadas para mejorar el rendimiento de las consultas parametrizadas que deben ejecutarse varias veces durante la misma conexión.

Una declaración preparada es una instrucción SQL que se compila en el lado del servidor pero no se ejecuta inmediatamente. La instrucción compilada se almacena en el servidor como un objeto `PreparedStatement` hasta que cierre el objeto o la conexión. Mientras ese objeto existe, puede ejecutar la instrucción preparada tantas veces como sea necesario utilizando diferentes valores de parámetros, sin tener que compilar la sentencia de nuevo. Esta reducción de la sobrecarga permite que el conjunto de consultas se ejecute más rápidamente.

Para obtener más información acerca de las instrucciones preparadas, consulte «Uso de sentencias preparadas» en [Tutorial básico de JDBC de Oracle](#).

Puede preparar una instrucción que contenga varias consultas. Por ejemplo, la siguiente instrucción preparada contiene dos consultas `INSERT`:

```
PreparedStatement pstmt = conn.prepareStatement("INSERT INTO  
MyTable VALUES (1, 'abc'); INSERT INTO CompanyTable VALUES  
(1, 'abc');");
```

Tenga cuidado de que estas consultas no dependan de los resultados de otras consultas que se especifican dentro de la misma instrucción preparada. Debido a que las consultas no se ejecutan durante el paso de preparación, los resultados aún no se han devuelto y no están disponibles para otras consultas de la misma instrucción preparada.

Por ejemplo, la siguiente instrucción preparada, que crea una tabla y, a continuación, inserta valores en esa tabla recién creada, no está permitida:

```
PreparedStatement pstmt = conn.prepareStatement("CREATE  
TABLE MyTable(col1 int, col2 varchar); INSERT INTO myTable  
VALUES (1, 'abc');");
```

Si intenta preparar esta instrucción, el servidor devuelve un error que indica que la tabla de destino (`MyTable`) aún no existe. La consulta `CREATE` debe ejecutarse antes de que se pueda preparar la consulta `INSERT`.

Diferencias entre las versiones 2.x y 1.x del controlador JDBC

En esta sección se describen las diferencias en la información devuelta por las versiones 2.x y 1.x del controlador JDBC.

En la tabla siguiente se muestra la información de `DatabaseMetaData` devuelta por las funciones `getDatabaseProductName()` y `getDatabaseProductVersion()` para cada versión del controlador JDBC. La versión 2.x del controlador JDBC obtiene los valores mientras establece la conexión. La versión 1.x del controlador JDBC obtiene los valores como resultado de una consulta.

Versión del controlador JDBC	Resultado de <code>GetDatabaseProductName()</code>	Resultado <code>GetDatabaseProductVersion()</code>
2.x	Redshift	8.0.2
1.x	PostgreSQL	08.00.0002

En la tabla siguiente se muestra la información de `DatabaseMetaData` devuelta por la función `GetTypeInfo` para cada versión del controlador JDBC.

Versión del controlador JDBC	Resultado <code>getTypeInfo</code>
2.x	Consistente con los tipos de datos de Redshift

Versión del controlador JDBC	Resultado getTypeInfo
1.x	Consistente con los tipos de datos de PostgreSQL

Opciones de configuración del controlador JDBC versión 2.0

En esta sección se describen las opciones que puede especificar para el controlador de la versión 2.0 del controlador JDBC de Amazon Redshift.

Puede establecer las propiedades de configuración mediante la dirección URL de conexión. Para obtener más información, consulte [Creación de la URL de conexión \(p. 104\)](#).

Temas

- [AccessKeyID \(p. 115\)](#)
- [AllowDBUserOverride \(p. 115\)](#)
- [app_id \(p. 116\)](#)
- [App_Name \(p. 116\)](#)
- [AutoCreate \(p. 116\)](#)
- [client_id \(p. 116\)](#)
- [client_secret \(p. 117\)](#)
- [ClusterID \(p. 117\)](#)
- [databaseMetadataCurrentDbOnly \(p. 117\)](#)
- [DbUser \(p. 117\)](#)
- [DbGroups \(p. 117\)](#)
- [defaultRowFetchSize \(p. 118\)](#)
- [DisableIsValidQuery \(p. 118\)](#)
- [enableFetchRingBuffer \(p. 118\)](#)
- [enableMultiSqlSupport \(p. 119\)](#)
- [fetchRingBufferSize \(p. 119\)](#)
- [ForceLowercase \(p. 119\)](#)
- [IAMDisableCache \(p. 119\)](#)
- [IAMDuration \(p. 120\)](#)
- [idp_host \(p. 120\)](#)
- [idp_port \(p. 120\)](#)
- [IDP_tenant \(p. 120\)](#)
- [IDP_Response_Timeout \(p. 121\)](#)
- [URL de inicio de sesión \(p. 121\)](#)
- [LoginTimeout \(p. 121\)](#)
- [loginToRp \(p. 121\)](#)
- [LogLevel \(p. 121\)](#)
- [LogPath \(p. 122\)](#)
- [Partner_SPID \(p. 123\)](#)
- [Password \(p. 123\)](#)
- [Plugin_Name \(p. 123\)](#)

- [preferred_role](#) (p. 123)
- [Profile](#) (p. 124)
- [PWD](#) (p. 124)
- [queryGroup](#) (p. 124)
- [ReadOnly](#) (p. 124)
- [Region](#) (p. 124)
- [reWriteBatchedInsertsSize](#) (p. 125)
- [roleArn](#) (p. 125)
- [roleSessionName](#) (p. 125)
- [SecretAccessKey](#) (p. 125)
- [SessionToken](#) (p. 125)
- [SocketTimeout](#) (p. 126)
- [SSL](#) (p. 126)
- [SSL_insecure](#) (p. 126)
- [SSLCert](#) (p. 126)
- [SSLFactory](#) (p. 127)
- [SSLKey](#) (p. 127)
- [SSLMode](#) (p. 127)
- [SSLPassword](#) (p. 127)
- [SSLRootCert](#) (p. 128)
- [StsEndpointUrl](#) (p. 128)
- [TCPKeepAlive](#) (p. 128)
- [UID](#) (p. 128)
- [User](#) (p. 128)
- [webIdentityToken](#) (p. 129)

[AccessKeyId](#)

- Valor predeterminado— Ninguno
- Tipo de datos: String

Puede especificar este parámetro para especificar la clave de acceso de IAM para el usuario de IAM o rol. Por lo general, puede localizar la clave mirando y la cadena existente o el perfil de usuario. Si especifica este parámetro, también debe especificar el parámetro `SecretAccessKey`.

Este parámetro es opcional.

[AllowDBUserOverride](#)

- Valor predeterminado— 0
- Tipo de datos: String

Esta opción especifica si el controlador utiliza el valor `DbUser` de la aserción SAML o el valor especificado en la propiedad de conexión `DbUser` en la dirección URL de conexión.

Este parámetro es opcional.

1

El controlador utiliza el valor DbUser de la aserción SAML.

Si la aserción SAML no especifica un DbUser, el controlador utiliza el valor especificado en la propiedad de conexión DbUser. Si la propiedad connection tampoco especifica un valor, el controlador utiliza el valor especificado en el perfil de conexión.

0

El controlador utiliza el valor DbUser especificado en la propiedad de conexión DBUser.

Si la propiedad de conexión DbUser no especifica un valor, el controlador utiliza el valor especificado en el perfil de conexión. Si el perfil de conexión tampoco especifica un valor, el controlador utiliza el valor de la aserción SAML.

app_id

- Valor predeterminado— Ninguno
- Tipo de datos: String

El ID único proporcionado por Okta asociado a su aplicación de Amazon Redshift.

Este parámetro es necesario si se autentica a través del servicio Okta.

App_Name

- Valor predeterminado— Ninguno
- Tipo de datos: String

Nombre de la aplicación Okta que se utiliza para autenticar la conexión a Amazon Redshift.

Este parámetro es opcional.

AutoCreate

- Valor predeterminado— false
- Tipo de datos: Boolean

Esta opción especifica si el controlador hace que se cree un nuevo usuario cuando el usuario especificado no existe.

Este parámetro es opcional.

true

Si el usuario especificado por DbUser o UID no existe, se crea un nuevo usuario con ese nombre.

false

El controlador no hace que se creen nuevos usuarios. Si el usuario especificado no existe, la autenticación genera un error.

client_id

- Valor predeterminado— Ninguno
- Tipo de datos: String

El ID de cliente que se utilizará al autenticar la conexión mediante el servicio Azure AD.

Este parámetro es necesario si se autentica a través del servicio Azure AD.

`client_secret`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El secreto del cliente que se utilizará al autenticar la conexión mediante el servicio Azure AD.

Este parámetro es necesario si se autentica a través del servicio Azure AD.

`ClusterID`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El nombre del clúster de Amazon Redshift al que desea conectarse.

Este parámetro es opcional.

`databaseMetadataCurrentDbOnly`

- Valor predeterminado— true
- Tipo de datos: Boolean

Esta opción especifica si la API de metadatos recupera datos de todas las bases de datos accesibles o sólo de la base de datos conectada.

Este parámetro es opcional.

Puede especificar los valores siguientes:

true

La aplicación recupera metadatos de una única base de datos.

false

La aplicación recupera metadatos de todas las bases de datos accesibles.

`DbUser`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El ID de usuario que se va a utilizar con su cuenta de Amazon Redshift. Puede utilizar un Id. que no existe actualmente si ha habilitado la propiedad AutoCreate.

Este parámetro es opcional.

`DbGroups`

- Valor predeterminado— PÚBLICA

- Tipo de datos: String

Una lista de nombres de grupos de bases de datos existentes separada por comas a los que se une el DbUser para la sesión actual.

Este parámetro es opcional.

defaultRowFetchSize

- Valor predeterminado— 0
- Tipo de datos— Entero

Esta opción especifica un valor predeterminado para GetFetchSize.

Este parámetro es opcional.

Puede especificar los valores siguientes:

0

Obtiene todas las filas de una sola operación.

Entero positivo

Número de filas que se van a obtener de la base de datos para cada iteración de obtención del ResultSet.

DisableIsValidQuery

- Valor predeterminado— False
- Tipo de datos: Boolean

Esta opción especifica si el controlador envía una nueva consulta de base de datos al utilizar el método Connection.isValid () para determinar si la conexión de base de datos está activa.

Este parámetro es opcional.

true

El controlador no envía una consulta al utilizar Connection.isValid () para determinar si la conexión de base de datos está activa. Esto puede hacer que el controlador identifique incorrectamente la conexión de base de datos como activa si el servidor de base de datos se ha apagado inesperadamente.

false

El controlador envía una consulta al utilizar Connection.isValid () para determinar si la conexión de base de datos está activa.

enableFetchRingBuffer

- Valor predeterminado— true
- Tipo de datos: Boolean

Esta opción especifica que el controlador obtiene filas utilizando un búfer de anillo en un subproceso separado. El parámetro FetchRingBufferSize especifica el tamaño del búfer de anillo.

Este parámetro es opcional.

`enableMultiSqlSupport`

- Valor predeterminado— `true`
- Tipo de datos: Boolean

Esta opción especifica si se procesan varios comandos SQL separados por punto y coma en una sentencia.

Este parámetro es opcional.

Puede especificar los valores siguientes:

`true`

El controlador procesa varios comandos SQL, separados por punto y coma, en un objeto Statement.

`false`

El controlador devuelve un error para varios comandos SQL en una sola sentencia.

`fetchRingBufferSize`

- Valor predeterminado— `1G`
- Tipo de datos: String

Esta opción especifica el tamaño del búfer de anillo utilizado durante la obtención del conjunto de resultados. Puede especificar un tamaño en bytes, por ejemplo, `1K` para 1 KB, `5000` para 5.000 bytes, `1M` para 1 MB, `1G` para 1 GB, etc. También puede especificar un porcentaje de memoria de montón. El controlador deja de buscar filas al alcanzar el límite. La recuperación se reanuda cuando la aplicación lee filas y libera espacio en el búfer de anillo.

Este parámetro es opcional.

`ForceLowercase`

- Valor predeterminado— `false`
- Tipo de datos: Boolean

Esta opción especifica si el controlador minúscula todos los grupos de bases de datos (DBGroups) enviados desde el proveedor de identidades a Amazon Redshift cuando se utiliza la autenticación SSO.

Este parámetro es opcional.

`true`

El controlador reduce todos los grupos de base de datos que se envían desde el proveedor de identidades.

`false`

El controlador no modifica los grupos de bases de datos.

`IAMDisableCache`

- Valor predeterminado— `false`

- Tipo de datos: Boolean

Esta opción especifica si las credenciales de IAM se almacenan en caché.

Este parámetro es opcional.

true

Las credenciales de IAM no se almacenan en caché.

false

Las credenciales de IAM se almacenan en caché. Esto mejora el rendimiento cuando las solicitudes a la puerta de enlace API están restringidas, por ejemplo.

[IAMDuration](#)

- Valor predeterminado— 900
- Tipo de datos— Entero

Fecha de caducidad, en segundos, de las credenciales temporales de IAM.

- Valor mínimo— 900
- Valor máximo— 3.600

Este parámetro es opcional.

[idp_host](#)

- Valor predeterminado— Ninguno
- Tipo de datos: String

El host IdP (proveedor de identidades) que está utilizando para autenticarse en Amazon Redshift. Esto se puede especificar en la cadena de conexión o en un perfil.

Este parámetro es opcional.

[idp_port](#)

- Valor predeterminado— Ninguno
- Tipo de datos: String

El puerto utilizado por un IdP (proveedor de identidad). Esto se puede especificar en la cadena de conexión o en un perfil.

Este parámetro es opcional.

[IDP_tenant](#)

- Valor predeterminado— Ninguno
- Tipo de datos: String

El ID de inquilino de Azure AD para su aplicación de Amazon Redshift.

Este parámetro es necesario si se autentica a través del servicio Azure AD.

IDP_Response_Timeout

- Valor predeterminado— 120
- Tipo de datos— Entero

Cantidad de tiempo, en segundos, que el controlador espera la respuesta SAML del proveedor de identidades al usar los servicios SAML o Azure AD a través de un complemento del explorador.

Este parámetro es opcional.

URL de inicio de sesión

- Valor predeterminado— Ninguno
- Tipo de datos: String

La dirección URL del recurso en el sitio web del proveedor de identidades cuando se utilizan los servicios SAML o Azure AD a través de un complemento del explorador.

Este parámetro es necesario si se autentica con los servicios SAML o Azure AD a través de un complemento de navegador.

LoginTimeout

- Valor predeterminado— 0
- Tipo de datos— Entero

La cantidad de segundos que se debe esperar antes de que se agote el tiempo de espera cuando se conecta y se autentica al servidor. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión.

Cuando esta propiedad se establece en 0, las conexiones no tienen tiempo de inactividad.

Este parámetro es opcional.

loginToRp

- Valor predeterminado—`urn:amazon:webservices`
- Tipo de datos: String

La confianza de la parte que confía que desea utilizar para el tipo de autenticación de AD FS.

Este parámetro es opcional.

LogLevel

- Valor predeterminado— 0
- Tipo de datos— Entero

Utilice esta propiedad para habilitar o deshabilitar el registro en el controlador y para especificar el nivel de detalles que se incluye en los archivos de registro.

Habilite el registro sólo el tiempo suficiente para capturar un problema. El registro reduce el rendimiento y puede consumir una gran cantidad de espacio en el disco.

Este parámetro es opcional.

Establezca el parámetro en uno de los siguientes valores:

0

Desactivar todos los registros

1

Habilite el registro en el nivel FATAL, que registra eventos de errores muy graves que harán que el controlador se anule

2

Habilite el registro en el nivel ERROR, que registra eventos de errores que podrían hacer que el controlador siga ejecutándose.

3

Habilite el registro en el nivel ADVERTENCIA, que registra los eventos que podrían dar lugar a un error si no se realiza la acción.

4

Habilite el registro en el nivel INFO, que registra información general que describa el progreso del controlador.

5

Habilitar el registro en el nivel de depuración, que registra información detallada útil para depurar el controlador.

6

Habilite el registro en el nivel TRACE, que registra toda la actividad del controlador.

Cuando se habilita el registro, el controlador produce los siguientes archivos de registro en la ubicación especificada en el `LogPath` propiedad:

- **redshift_jdbc.log**— Archivo que registra la actividad del controlador que no es específica de una conexión.
- **redshift_jdbc_connection_[Number].log**— Archivo para cada conexión realizada a la base de datos, donde `[Number]` es un número que distingue cada archivo de registro de los demás. Este archivo registra la actividad del controlador que es específica de la conexión.

Si el valor de `LogPath` no es válido, el controlador envía la información registrada a la secuencia de salida estándar, `System.out`.

LogPath

- Valor predeterminado— El directorio de trabajo actual.
- Tipo de datos: String

Ruta de acceso completa a la carpeta donde el controlador guarda los archivos de registro cuando está habilitada la propiedad `dSiLogLevel`.

Para asegurarse de que la dirección URL de conexión es compatible con todas las aplicaciones JDBC, le recomendamos que evite las barras diagonales inversas (`\`) en la ruta del archivo escribiendo otra barra invertida.

Este parámetro es opcional.

Partner_SPID

- Valor predeterminado— Ninguno
- Tipo de datos: String

El valor SPID (ID de proveedor de servicios) del asociado que se utilizará al autenticar la conexión mediante el servicio PingFederate.

Este parámetro es opcional.

Password

- Valor predeterminado— Ninguno
- Tipo de datos: String

Cuando se conecta mediante autenticación de IAM a través de un IDP, esta es la contraseña del servidor IDP_Host. Cuando se utiliza la autenticación estándar, se puede utilizar para la contraseña de base de datos de Amazon Redshift en lugar de PWD.

Este parámetro es opcional.

Plugin_Name

- Valor predeterminado— Ninguno
- Tipo de datos: String

El nombre completo de la clase para implementar un complemento específico del proveedor de credenciales.

Este parámetro es opcional.

Se admiten las siguientes opciones de proveedor:

- **AdfsCredentialsProvider**— Active Directory Federation Service Service
- **AzureCredentialsProvider**— Servicio Microsoft Azure Active Directory (AD)
- **BasicJwtCredentialsProvider**— Servicio de tokens web JSON (JWT)
- **BrowserAzureCredentialsProvider**— Navegador de Microsoft Azure Active Directory (AD)
- **BrowserSamlCredentialsProvider**— Navegador SAML para servicios SAML como Okta, Ping o ADFS
- **OktaCredentialsProvider**— Servicio Okta
- **PingCredentialsProvider**— Servicio PingFederate

preferred_role

- Valor predeterminado— Ninguno
- Tipo de datos: String

Función de IAM que desea asumir durante la conexión a Amazon Redshift.

Este parámetro es opcional.

Profile

- Valor predeterminado— Ninguno
- Tipo de datos: String

Nombre del perfil que se va a utilizar para la autenticación de IAM. Este perfil contiene las propiedades de conexión adicionales no especificadas en la cadena de conexión.

Este parámetro es opcional.

PWD

- Valor predeterminado— Ninguno
- Tipo de datos: String

Contraseña correspondiente al nombre de usuario de Amazon Redshift que ha proporcionado mediante el UID de propiedad.

Este parámetro es opcional.

queryGroup

- Valor predeterminado— nulo
- Tipo de datos: String

Esta opción asigna una consulta a una cola en tiempo de ejecución asignando la consulta al grupo de consultas adecuado. El grupo de consultas está establecido para la sesión. Todas las consultas que se ejecutan en la conexión pertenecen a este grupo de consultas.

Este parámetro es opcional.

ReadOnly

- Valor predeterminado— false
- Tipo de datos: Boolean

Esta propiedad especifica si el controlador está en modo de solo lectura.

Este parámetro es opcional.

true

La conexión está en modo de sólo lectura y no puede escribir en el almacén de datos.

false

La conexión no está en modo de sólo lectura y puede escribir en el almacén de datos.

Region

- Valor predeterminado— nulo
- Tipo de datos: String

Esta opción especifica la propiedadAWSRegión donde está ubicado el clúster. Si especifica la opción StsendPoint, se omitirá la opción Región. El RedshiftGetClusterCredentialsLa operación API también utiliza la opción Región.

Este parámetro es opcional.

`rewriteBatchedInsertsSize`

- Valor predeterminado— 128
- Tipo de datos— Entero

Esta opción permite la optimización para reescribir y combinar sentencias INSERT compatibles que se agrupan por lotes. Este valor debe aumentar exponencialmente por la potencia de 2.

Este parámetro es opcional.

`roleArn`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El nombre de recurso de Amazon (ARN) del rol. Asegúrese de especificar este parámetro cuando especifique BasicJWTCredentialsProvider para la opción Plugin_Name. Especifique el ARN con el siguiente formato:

`arn:partition:service:region:account-id:resource-id`

Este parámetro es obligatorio si especifica BasicJWTCredentialsProvider para la opción Plugin_Name.

`roleSessionName`

- Valor predeterminado— `jwt_redshift_session`
- Tipo de datos: String

Un identificador de la sesión de rol asumido. Normalmente, se pasa el nombre o el identificador que está asociado con el usuario de la aplicación. Las credenciales de seguridad temporales que utiliza la aplicación están asociadas a ese usuario. Puede especificar este parámetro cuando especifica BasicJWTCredentialsProvider para la opción Plugin_Name.

Este parámetro es opcional.

`SecretAccessKey`

- Valor predeterminado— Ninguno
- Tipo de datos: String

La clave de acceso de IAM para el usuario o rol. Si se especifica esto, entonces también debe especificarse AccessKeyID.

Este parámetro es opcional.

`SessionToken`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El token de sesión temporal de IAM asociado al rol de IAM que está utilizando para autenticar.

Este parámetro es opcional.

SocketTimeout

- Valor predeterminado— 0
- Tipo de datos— Entero

La cantidad de segundos que se debe esperar durante las operaciones de lectura del conector antes de que se agote el tiempo de espera. Si la operación toma más que este umbral de tiempo, se cierra la conexión. Cuando esta propiedad se establece en 0, la conexión no tiene tiempo de espera.

Este parámetro es opcional.

SSL

- Valor predeterminado— TRUE
- Tipo de datos: String

Utilice esta propiedad para habilitar o deshabilitar SSL para la conexión.

Este parámetro es opcional.

Puede especificar los valores siguientes:

TRUE

El controlador se conecta al servidor a través de SSL.

FALSE

El controlador se conecta al servidor sin usar SSL. Esta opción no es compatible con la autenticación de IAM.

También puede configurar la propiedad AuthMech.

SSL_insecure

- Valor predeterminado— true
- Tipo de datos: String

Esta propiedad indica si se debe verificar el certificado de servidor de hosts de IDP.

Este parámetro es opcional.

Puede especificar los valores siguientes:

true

El controlador no comprueba la autenticidad del certificado de servidor de proveedor de identidad.

false

El controlador comprueba la autenticidad del certificado del servidor IDP.

SSLCert

- Valor predeterminado— Ninguno

- Tipo de datos: String

La ruta completa de un archivo .pem o .crt que contiene certificados de entidad de certificación de confianza adicionales para comprobar la instancia del servidor Amazon Redshift cuando se utiliza SSL.

Este parámetro es necesario si se especifica SSLKey.

SSLFactory

- Valor predeterminado— Ninguno
- Tipo de datos: String

La fábrica SSL que se utilizará cuando se conecte al servidor a través de TLS/SSL sin utilizar un certificado de servidor.

SSLKey

- Valor predeterminado— Ninguno
- Tipo de datos: String

Ruta de acceso completa del archivo.der que contiene el archivo de clave PKCS8 para verificar los certificados especificados en SSLCert.

Este parámetro es necesario si se especifica SSLCert.

SSLMode

- Valor predeterminado— verify-ca
- Tipo de datos: String

Utilice esta propiedad para especificar cómo el controlador valida los certificados cuando TLS/SSL está habilitado.

Este parámetro es opcional.

Puede especificar los valores siguientes:

verify-ca

El controlador comprueba que el certificado proviene de una entidad emisora de certificados (CA) de confianza.

verify-full

El controlador comprueba que el certificado proviene de una CA de confianza y que el nombre de host del certificado coincide con el nombre de host especificado en la dirección URL de conexión.

SSLPassword

- Valor predeterminado— 0
- Tipo de datos: String

Contraseña para el archivo de clave cifrado especificado en SSLKey.

Este parámetro es necesario si se especifica sslKey y el archivo de clave está cifrado.

SSLRootCert

- Valor predeterminado— Ninguno
- Tipo de datos: String

La ruta completa de un archivo .pem o .crt que contiene el certificado de entidad de certificación raíz para comprobar la instancia de Amazon Redshift Server cuando se utiliza SSL.

StsEndpointUrl

- Valor predeterminado: Null
- Tipo de datos: String

Puede especificar unaAWS Security Token Service(AWS STS). Si especifica esta opción, se omite la opción Región. Sólo puede especificar un protocolo seguro (HTTPS) para este extremo.

TCPKeepAlive

- Valor predeterminado— TRUE
- Tipo de datos: String

Utilice esta propiedad para habilitar o deshabilitar las conexiones de mantenimiento de TCP.

Este parámetro es opcional.

Puede especificar los valores siguientes:

TRUE

El controlador usa conexiones keepalive de TCP para evitar que se agote el tiempo de espera en las conexiones.

FALSE

El controlador no utiliza keepalives de TCP.

UID

- Valor predeterminado— Ninguno
- Tipo de datos: String

El nombre de usuario que se utiliza para obtener acceso a la base de datos.

Este parámetro es obligatorio.

User

- Valor predeterminado— Ninguno
- Tipo de datos: String

Cuando se conecta mediante la autenticación de IAM a través de un IDP, éste es el nombre de usuario del servidor idp_host. Al utilizar la autenticación estándar, esto se puede utilizar para el nombre de usuario de la base de datos de Amazon Redshift.

Este parámetro es opcional.

`webIdentityToken`

- Valor predeterminado— Ninguno
- Tipo de datos: String

El token de acceso de OAuth 2.0 o el ID de token de OpenID Connect proporcionado por el proveedor de identidad. Su aplicación debe obtener este token autenticando al usuario de su aplicación con un proveedor de identidad web. Asegúrese de especificar este parámetro cuando especifique `BasicJWTCredentialsProvider` para la opción `Plugin_Name`.

Este parámetro es obligatorio si especifica `BasicJWTCredentialsProvider` para la opción `Plugin_Name`.

Versiones anteriores del controlador JDBC versión 2.0

Descargue una versión anterior del controlador JDBC de Amazon Redshift versión 2.0 de solo si su herramienta requiere una versión específica del controlador.

Estos son controladores JDBC versión 2.0 compatibles con JDBC:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.4/redshift-jdbc42-2.0.0.4.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.4/redshift-jdbc42-2.0.0.4.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.3/redshift-jdbc42-2.0.0.3.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.3/redshift-jdbc42-2.0.0.3.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.2/redshift-jdbc42-2.0.0.2.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.2/redshift-jdbc42-2.0.0.2.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.1/redshift-jdbc42-2.0.0.1.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.1/redshift-jdbc42-2.0.0.1.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.0/redshift-jdbc42-2.0.0.0.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/2.0.0.0/redshift-jdbc42-2.0.0.0.jar>.

Configuración de una conexión de controlador JDBC versión 1.0

Puede utilizar una conexión de controlador JDBC versión 1.0 para conectarse a su clúster de Amazon Redshift de desde distintas herramientas de cliente SQL de terceros. Para hacer esto, descargue un controlador JDBC.

Si desea utilizar una conexión JDBC, siga los pasos siguientes.

Temas

- [Descargar un controlador JDBC de Amazon Redshift \(p. 130\)](#)
- [Obtención de la URL de JDBC \(p. 130\)](#)
- [Configurar la autenticación y SSL para la conexión JDBC \(p. 131\)](#)
- [Configurar conexiones keepalive de TCP para la conexión de JDBC \(p. 131\)](#)
- [Configurar el registro para la conexión JDBC \(p. 131\)](#)
- [Configuración de una conexión JDBC con Apache Maven \(p. 132\)](#)
- [Configurar las opciones del controlador JDBC \(p. 134\)](#)
- [Usar versiones anteriores de controladores JDBC versión 1.0 en algunos casos \(p. 134\)](#)

Descargar un controlador JDBC de Amazon Redshift

Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2. Para obtener información acerca de la funcionalidad admitida por estos controladores, consulte la [Notas de la versión del controlador JDBC de Amazon Redshift](#).

Para obtener información detallada acerca de cómo instalar el controlador JDBC versión 1.0, consulte las bibliotecas de controladores JDBC y registre la clase de controlador, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Para cada equipo en el que utilice el controlador JDBC de Amazon Redshift, asegúrese de que Java Runtime Environment (JRE) 8.0 esté instalado.

Si utiliza el controlador JDBC de Amazon Redshift para la autenticación de bases de datos, asegúrese de tener AWS SDK for Java 1.11.118 o posterior en la ruta de clases de Java. Si no dispone de AWS SDK for Java instalado, descargue el archivo ZIP con el controlador compatible con JDBC 4.2 (sin AWS SDK) y las bibliotecas dependientes del controlador para AWS SDK:

- [Controlador compatible con JDBC 4.2 \(sin el AWS SDK\) y bibliotecas dependientes del controlador para AWS SDK versión 1.2.54](#).

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Este archivo ZIP contiene el controlador compatible con JDBC 4.2 (sin el AWS SDK) y sus archivos de biblioteca dependientes. Descomprima los archivos jar dependientes en la misma ubicación que el controlador JDBC. Solo el controlador JDBC necesita estar en el CLASSPATH porque el archivo de manifiesto del controlador contiene todos los nombres de archivo de biblioteca dependientes que se encuentran en el mismo directorio que el controlador JDBC. Para obtener más información acerca de cómo instalar el controlador JDBC, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Utilice este controlador JDBC de Amazon Redshift con el AWS SDK necesario para la autenticación de la base de datos de IAM.

- [Controlador compatible con JDBC 4.2 \(sin el AWS SDK\) versión 1.2.54](#).

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Asegúrese de utilizar ANTLR versión 4.8.1. El `antlr4-runtime-4.8-1.jar` se incluye en el enlace de descarga ZIP anterior con el controlador compatible con JDBC 4.2 (sin el AWS SDK) y las bibliotecas dependientes del controlador para AWS SDK.

Para obtener más información acerca de las versiones anteriores de controladores, consulte [Utilice versiones anteriores del controlador JDBC con el AWS SDK for Java \(p. 137\)](#).

A continuación, descargue y lea las [Contrato de licencia del controlador ODBC de Amazon Redshift y JDBC de Amazon Redshift](#).

Si su herramienta requiere una versión anterior específica de un controlador, consulte [Usar versiones anteriores de controladores JDBC versión 1.0 en algunos casos \(p. 134\)](#).

Obtención de la URL de JDBC

Para poder conectarse a su clúster de Amazon Redshift desde una herramienta de cliente SQL, necesita saber el URL de JDBC de su clúster. El URL de JDBC tiene el siguiente formato:
`jdbc:redshift://endpoint:port/database`

Note

Una URL de JDBC especificada con el formato anterior de
`jdbc:postgresql://endpoint:port/database` todavía funciona.

Los campos del formato mostrado anteriormente tienen los siguientes valores.

Campo	Valor
<code>jdbc</code>	Protocolo para la conexión.
<code>redshift</code>	Subprotocolo que especifica el uso de un controlador de Amazon Redshift para conectarse a la base de datos.
<code>endpoint</code>	El punto de enlace del clúster de Amazon Redshift.
<code>port</code>	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.
<code>database</code>	Base de datos que creó para su clúster.

A continuación, se muestra un ejemplo de la URL de un JDBC: `jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev`

Para obtener información acerca de cómo crear su propia conexión JDBC, consulte [Obtención de la cadena de conexión a su clúster \(p. 99\)](#).

Si el equipo cliente no puede conectarse a la base de datos, puede solucionar los posibles problemas. Para obtener más información, consulte [Solución de problemas de conexión en Amazon Redshift \(p. 169\)](#).

Configurar la autenticación y SSL para la conexión JDBC

Configure el controlador JDBC de Amazon Redshift para autenticar la conexión de acuerdo con los requisitos de seguridad del servidor de Amazon Redshift al que se está conectando.

Para autenticar la conexión, proporcione siempre su nombre de usuario y contraseña de Amazon Redshift. La contraseña se transmite usando un hash MD5 salado de la contraseña. En función de si SSL está habilitado y requerido en el servidor, es posible que también necesite configurar el controlador para que se conecte a través de SSL. O es posible que necesite usar la autenticación SSL unidireccional para que el cliente (el propio controlador) verifique la identidad del servidor.

Para obtener información acerca de cómo configurar el controlador JDBC para autenticar la conexión, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Configurar conexiones keepalive de TCP para la conexión de JDBC

De forma predeterminada, el controlador JDBC de Amazon Redshift está configurado para usar conexiones keepalive de TCP para evitar que se agote el tiempo de espera en las conexiones. Puede especificar cuándo comienza el controlador a enviar paquetes keepalive o deshabilitar la característica estableciendo las propiedades correspondientes en la URL de conexión.

Para obtener información acerca de cómo configurar conexiones keepalive de TCP para el controlador JDBC, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Configurar el registro para la conexión JDBC

Para ayudar a solucionar problemas, puede habilitar el registro en el controlador JDBC.

Para obtener información acerca de cómo configurar el registro para la conexión JDBC, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Configuración de una conexión JDBC con Apache Maven

Apache Maven es una herramienta de software para la comprensión y administración de proyectos. La AWS SDK for Java es compatible con los proyectos Apache Maven. Para obtener más información, consulte [Uso del SDK con Apache Maven](#) en la AWS SDK for Java Guía para desarrolladores de .

Si utiliza Apache Maven, puede configurar y crear sus proyectos de forma que utilicen un controlador JDBC de Amazon Redshift para conectarse al clúster de Amazon Redshift. Para hacerlo, agregue el controlador JDBC como dependencia en el archivo `pom.xml` de su proyecto. Si usa Maven para configurar su proyecto y desea usar una conexión JDBC, siga los pasos que se indican en la siguiente sección.

Configuración del controlador JDBC como una dependencia de Maven

Pasos para configurar el controlador JDBC como una dependencia de Maven

1. Añada el siguiente repositorio a la sección de repositorios de su archivo `pom.xml`.

Note

La URL del siguiente código devuelve un error si se utiliza en un navegador. Utilice esta URL solo en el contexto de un proyecto Maven.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>http://redshift-maven-repository.s3-website-us-east-1.amazonaws.com/
release</url>
  </repository>
</repositories>
```

Para conectarse utilizando SSL, añada el siguiente repositorio al archivo `pom.xml`.

```
<repositories>
  <repository>
    <id>redshift</id>
    <url>https://s3.amazonaws.com/redshift-maven-repository/release</url>
  </repository>
</repositories>
```

2. Declare la versión del controlador que desea usar en la sección de dependencias de su archivo `pom.xml`.

Amazon Redshift ofrece controladores para herramientas compatibles con la API JDBC 4.2. Para obtener información acerca de la funcionalidad admitida por estos controladores, consulte [Descargar un controlador JDBC de Amazon Redshift \(p. 130\)](#).

Añada una dependencia para el controlador de la siguiente lista.

Note

Para la versión 1.2.1.1001 y versiones posteriores, puede usar el nombre genérico `com.amazon.redshift.jdbc.Driver` de la clase de controlador, o bien el nombre de clase específico de la versión que figura junto al controlador en la siguiente lista, por ejemplo `com.amazon.redshift.jdbc42.Driver`. Para versiones anteriores a la 1.2.1.1001, solo se admiten los nombres de clases específicos a la versión.

Reemplace la **versión del controlador** en el siguiente ejemplo por su versión del controlador. Por ejemplo, 1.2.45.1069.

- Controlador compatible con JDBC 4.2:

```
<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42</artifactId>
  <version>driver-version</version>
</dependency>
```

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

3. Descargue y lea las [Contrato de licencia del controlador ODBC de Amazon Redshift y JDBC de Amazon Redshift](#).

Los controladores JDBC estándar de Amazon Redshift incluyen AWS SDK necesario para usar la autenticación de base de datos de IAM. Le recomendamos que utilice los controladores estándar a menos que el tamaño de los archivos del controlador suponga un problema para su aplicación. Si necesita archivos de controlador más pequeños y no utiliza la autenticación de base de datos de IAM, o si ya tiene AWS SDK for Java 1.11.118 o versiones posteriores en la ruta de clases de Java, agregue una dependencia para el controlador de la lista siguiente.

Reemplace la **versión del controlador** en el siguiente ejemplo por su versión del controlador. Por ejemplo, 1.2.45.1069.

- Controlador compatible con JDBC 4.2:

```
<dependency>
  <groupId>com.amazon.redshift</groupId>
  <artifactId>redshift-jdbc42-no-awssdk</artifactId>
  <version>driver-version</version>
</dependency>
```

El nombre de clase para este controlador es `com.amazon.redshift.jdbc42.Driver`.

Los controladores de Amazon Redshift Maven de sin SDK incluyen la siguiente dependencia necesaria que debe incluir en su proyecto.

```
<dependency>
  <groupId>org.antlr</groupId>
  <artifactId>antlr4</artifactId>
  <version>4.5.3</version>
  <scope>runtime</scope>
  <optional>>false</optional>
</dependency>
```

Los controladores de Amazon Redshift Maven sin SDK incluyen las siguientes dependencias opcionales que puede incluir en el proyecto según sea necesario.

```
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-core</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
  <optional>>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-redshift</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
```



```
<optional>true</optional>
</dependency>
<dependency>
  <groupId>com.amazonaws</groupId>
  <artifactId>aws-java-sdk-sts</artifactId>
  <version>1.11.118</version>
  <scope>runtime</scope>
  <optional>true</optional>
</dependency>
```

Si su herramienta requiere una versión anterior específica de un controlador, consulte [Uso de versiones anteriores del controlador JDBC con Maven](#) (p. 137).

Actualización a la versión más reciente del controlador

Para actualizar o cambiar el controlador JDBC de Amazon Redshift a la versión más reciente, modifique primero la sección de versión de la dependencia a la última versión del controlador. Luego limpie su proyecto con el Maven Clean Plugin, como se indica a continuación.

```
mvn clean
```

Configurar las opciones del controlador JDBC

Para controlar el comportamiento del controlador JDBC de Amazon Redshift JDBC, puede anexar opciones de configuración a la dirección URL de JDBC. Por ejemplo, la siguiente URL de JDBC se conecta a su clúster mediante SSL (Capa de conexión segura), usuario (UID) y contraseña (PWD).

```
jdbc:redshift://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev?
ssl=true&UID=your_username&PWD=your_password
```

Para obtener más información acerca de las opciones SSL, consulte [Conexión mediante una SSL](#) (p. 152).

Para obtener información acerca de cómo configurar las opciones de configuración del controlador JDBC, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

Usar versiones anteriores de controladores JDBC versión 1.0 en algunos casos

Descargue una versión anterior del controlador JDBC de Amazon Redshift de solo si su herramienta requiere una versión específica del controlador. Para obtener información sobre la funcionalidad admitida en estas versiones de los controladores, consulte [Descargar un controlador JDBC de Amazon Redshift](#) (p. 130).

A continuación, descargue y lea las [Contrato de licencia del controlador ODBC de Amazon Redshift y JDBC de Amazon Redshift](#).

Para la autenticación mediante AWS Identity and Access Management (IAM) o las credenciales de un proveedor de identidad (IdP), use el controlador JDBC de Amazon Redshift versión 1.2.8.1005 o posterior.

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Si tiene que usar una versión del controlador anterior a 1.2.8.1005, es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL](#) (p. 155).

Si utiliza el controlador JDBC de Amazon Redshift para la autenticación de bases de datos, asegúrese de tener AWS SDK for Java 1.11.118 o posterior en la ruta de clases de Java. Si no dispone de AWS SDK for Java, puede usar un controlador que incluya el controlador de AWS SDK. Para obtener más información, consulte [Utilice versiones anteriores del controlador JDBC con el AWS SDK for Java](#) (p. 137).

Estos son controladores compatibles con JDBC 4.2:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.54.1082/RedshiftJDBC42-no-awssdk-1.2.54.1082.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.53.1080/RedshiftJDBC42-no-awssdk-1.2.53.1080.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.51.1078/RedshiftJDBC42-no-awssdk-1.2.51.1078.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.50.1077/RedshiftJDBC42-no-awssdk-1.2.50.1077.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.47.1071/RedshiftJDBC42-no-awssdk-1.2.47.1071.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.45.1069/RedshiftJDBC42-no-awssdk-1.2.45.1069.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.43.1067/RedshiftJDBC42-no-awssdk-1.2.43.1067.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.41.1065/RedshiftJDBC42-no-awssdk-1.2.41.1065.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC42-no-awssdk-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC42-no-awssdk-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC42-no-awssdk-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.32.1056/RedshiftJDBC42-no-awssdk-1.2.32.1056.jar>.
- <https://RedshiftJDBC42.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC42-no-awssdk-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC42-no-awssdk-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.16.1027/RedshiftJDBC42-no-awssdk-1.2.16.1027.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.15.1025/RedshiftJDBC42-no-awssdk-1.2.15.1025.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.12.1017/RedshiftJDBC42-no-awssdk-1.2.12.1017.jar>.

Estos archivos ZIP contienen controladores compatibles con JDBC 4.2 (sin la opción AWSSDK) y sus archivos de biblioteca dependientes. Descomprima los archivos jar dependientes en la misma ubicación que el controlador JDBC. Solo el controlador JDBC necesita estar en el CLASSPATH porque el archivo de manifiesto del controlador contiene todos los nombres de archivo de biblioteca dependientes que se encuentran en el mismo directorio que el controlador JDBC. Para obtener más información acerca de cómo instalar el controlador JDBC, consulte [Guía de instalación y configuración del controlador JDBC de Amazon Redshift](#).

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.54.1082/RedshiftJDBC42-1.2.54.1082.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.53.1080/RedshiftJDBC42-1.2.53.1080.zip>.

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.51.1078/RedshiftJDBC42-1.2.51.1078.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.50.1077/RedshiftJDBC42-1.2.50.1077.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.47.1071/RedshiftJDBC42-1.2.47.1071.zip>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.45.1069/RedshiftJDBC42-1.2.45.1069.zip>.

Estos son controladores anteriores compatibles con JDBC 4.1:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.43.1065/RedshiftJDBC41-no-awssdk-1.2.43.1067.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.41.1065/RedshiftJDBC41-no-awssdk-1.2.41.1065.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC41-no-awssdk-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC41-no-awssdk-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC41-no-awssdk-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.32.1056/RedshiftJDBC41-no-awssdk-1.2.32.1056.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC41-no-awssdk-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC41-no-awssdk-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.16.1027/RedshiftJDBC41-no-awssdk-1.2.16.1027.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.15.1025/RedshiftJDBC41-no-awssdk-1.2.15.1025.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.12.1017/RedshiftJDBC41-no-awssdk-1.2.12.1017.jar>.

Estos son controladores anteriores compatibles con JDBC 4.0:

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.43.1067/RedshiftJDBC4-no-awssdk-1.2.43.1067.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.41.1065/RedshiftJDBC4-no-awssdk-1.2.41.1065.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC4-no-awssdk-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC4-no-awssdk-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC4-no-awssdk-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.32.1056/RedshiftJDBC4-no-awssdk-1.2.32.1056.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC4-no-awssdk-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC4-no-awssdk-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.16.1027/RedshiftJDBC4-no-awssdk-1.2.16.1027.jar>.

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.15.1025/RedshiftJDBC4-no-awssdk-1.2.15.1025.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.12.1017/RedshiftJDBC4-no-awssdk-1.2.12.1017.jar>.

Utilice versiones anteriores del controlador JDBC con elAWS SDK for Java

Si utiliza el controlador JDBC para la autenticación de bases de datos, asegúrese de tenerAWS SDK for Java1.11.118 o posterior en la ruta de clases de Java. Si no dispone deAWS SDK for Javainstalado, puede utilizar uno de los siguientes controladores que incluya el controladorAWSSDK.

- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.43.1067/RedshiftJDBC42-1.2.43.1067.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.41.1065/RedshiftJDBC42-1.2.41.1065.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC42-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC41-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.37.1061/RedshiftJDBC4-1.2.37.1061.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC42-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC41-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.36.1060/RedshiftJDBC4-1.2.36.1060.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC42-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC41-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.34.1058/RedshiftJDBC4-1.2.34.1058.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC4-no-awssdk-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.32.1056/RedshiftJDBC41-1.2.32.1056.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.32.1056/RedshiftJDBC4-1.2.32.1056.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC42-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC41-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC4-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC42-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC41-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.27.1051/RedshiftJDBC4-1.2.27.1051.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC42-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC41-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.20.1043/RedshiftJDBC4-1.2.20.1043.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.16.1027/RedshiftJDBC42-1.2.16.1027.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.15.1025/RedshiftJDBC42-1.2.15.1025.jar>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/jdbc/1.2.12.1017/RedshiftJDBC42-1.2.12.1017.jar>.

Uso de versiones anteriores del controlador JDBC con Maven

Añada una versión anterior del controlador JDBC de Amazon Redshift a su proyecto solo si su herramienta requiere una versión específica del controlador. Para obtener información sobre la funcionalidad admitida en estas versiones de los controladores, consulte [Descargar un controlador JDBC de Amazon Redshift](#) (p. 130). Para obtener información acerca de cómo configurar con Maven, consulte [Configuración de una conexión JDBC con Apache Maven](#) (p. 132).

Configuración de una conexión ODBC

Puede utilizar una conexión ODBC para conectarse a su clúster de Amazon Redshift desde distintas aplicaciones y herramientas de cliente SQL de terceros. Para hacerlo, configure la conexión en su equipo cliente o en una instancia de Amazon EC2. Si su equipo cliente es compatible con JDBC, puede elegir utilizar ese tipo de conexión, en lugar de una conexión ODBC ya que JDBC es más fácil de configurar. Sin embargo, si su herramienta de cliente no es compatible con JDBC, siga los pasos de esta sección para configurar una conexión ODBC.

Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y macOS X. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL. De lo contrario, la conexión no funciona. Si usa más de una herramienta del cliente SQL en el mismo equipo o instancia, asegúrese de descargar los controladores adecuados. Es posible que necesite instalar tanto los controladores de 32 bits y 64 bits si las herramientas difieren en su arquitectura de sistema.

Para obtener la información más reciente acerca de la funcionalidad del controlador ODBC y los requisitos previos, consulte [Notas de la versión del controlador ODBC de Amazon Redshift](#).

Para obtener información sobre la instalación y la configuración de los controladores ODBC de Amazon Redshift, consulte [Guía de instalación y configuración del controlador ODBC de Amazon Redshift](#).

Si desea utilizar una conexión ODBC, siga los pasos siguientes.

Temas

- [Obtención del URL de ODBC para su clúster \(p. 138\)](#)
- [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows \(p. 139\)](#)
- [Instalación del controlador ODBC de Amazon Redshift en Linux \(p. 141\)](#)
- [Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X \(p. 143\)](#)
- [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X \(p. 144\)](#)
- [Configurar las opciones del controlador ODBC \(p. 148\)](#)
- [Usar versiones anteriores de controladores ODBC en algunos casos \(p. 148\)](#)

Obtención del URL de ODBC para su clúster

Amazon Redshift muestra la URL del ODBC del clúster en la consola de Amazon Redshift. Esta dirección URL contiene la información que necesita para configurar la conexión entre su equipo cliente y la base de datos.

Una URL de ODBC tiene el siguiente formato:

`Driver={driver};Server=endpoint;Database=database_name;UID=user_name;PWD=password;Port=port;`

Los campos del formato mostrado anteriormente tienen los siguientes valores.

Campo	Valor
Driver	Nombre del controlador ODBC que se va a utilizar. Dependiendo del controlador que descargue para su arquitectura, los valores son Amazon Redshift (x86)(para el controlador de 32 bits) Amazon Redshift (x64)(para el controlador de 64 bits).
Server	El punto de enlace del clúster de Amazon Redshift.
Database	Base de datos que creó para su clúster.

Campo	Valor
UID	Nombre de usuario de una cuenta de usuario que tiene permiso para conectarse a la base de datos. Este valor es un permiso de la base de datos, no un permiso de Amazon Redshift, aunque puede utilizar la cuenta de usuario maestro que configuró cuando lanzó el clúster.
PWD	Contraseña de la cuenta de usuario para conectarse a la base de datos.
Port	Número de puerto que especificó cuando lanzó el clúster. Si tiene un firewall, asegúrese de que este puerto esté abierto para poder usarlo.

A continuación, se muestra un ejemplo de la URL de un ODBC: `Driver={Amazon Redshift (x64)}; Server=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com; Database=dev; UID=masteruser; PWD=insert_your_master_user_password_here; Port=5439`

Para obtener información acerca de cómo crear su propia conexión ODBC, consulte [Obtención de la cadena de conexión a su clúster \(p. 99\)](#).

Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacén de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte [Guía de instalación y configuración del controlador ODBC de Amazon Redshift](#).

Instalación del controlador Amazon Redshift en sistemas operativos Windows

Utilice el procedimiento siguiente para descargar los controladores ODBC de Amazon Redshift para los sistemas operativos Windows. Utilice un controlador diferente solo si está ejecutando una aplicación de terceros que está certificada para usarse con Amazon Redshift y que requiere un controlador específico.

Pasos para instalar el controlador ODBC de

1. Descargue alguno de los siguientes controladores, según la arquitectura de sistema de su aplicación o su herramienta de cliente SQL:

- [Controlador ODBC de 32 bits versión 1.4.27](#)

El nombre de este controlador es Amazon Redshift (x86).

- [Controlador ODBC de 64 bits versión 1.4.27](#)

El nombre de este controlador es Amazon Redshift (x64).

Note

Descargue el paquete MSI que corresponde a la arquitectura de sistema de su aplicación o su herramienta de cliente SQL. Por ejemplo, si su herramienta de cliente SQL es de 64 bits, instale el controlador de 64 bits.

A continuación, descargue y lea las [Contrato de licencia del controlador ODBC y JDBC de Amazon Redshift](#).

2. Haga doble clic en el archivo .msi y, luego, siga los pasos en el asistente para instalar el controlador.

Creación de una entrada de sistema DSN para una conexión ODBC en Microsoft Windows

Después de descargar e instalar el controlador ODBC, agregue una entrada de Data Source Name (DSN, Nombre de origen de datos) al equipo cliente o a la instancia de Amazon EC2. Las herramientas de cliente SQL utilizan este origen de datos para conectarse a la base de datos de Amazon Redshift.

Se recomienda crear un DSN del sistema en lugar de un DSN de usuario. Algunas aplicaciones cargan los datos con una cuenta de usuario diferente. Es posible que estas aplicaciones no puedan detectar DSN de usuario que se crean en otra cuenta de usuario.

Note

Para la autenticación con credenciales de AWS Identity and Access Management (IAM) o credenciales de proveedor de identidad (IdP), se requieren pasos adicionales. Para obtener más información, consulte [Configurar una conexión JDBC u ODBC para usar credenciales de IAM](#) (p. 330).

Para obtener información acerca de cómo crear una entrada DSN del sistema, consulte [Guía de instalación y configuración del controlador ODBC de Amazon Redshift](#).

Para crear una entrada DSN del sistema para una conexión ODBC en Windows

1. En el menú Start (Inicio), abra ODBC Data Sources (Orígenes de datos ODBC).
Asegúrese de elegir el Administrador de orígenes de datos ODBC que tenga el mismo valor de bits que la aplicación cliente que está utilizando para conectarse a Amazon Redshift.
2. En el ODBC Data Source Administrator (Administrador de orígenes de datos ODBC), elija la pestaña Driver (Controlador) y busque la carpeta del controlador.

Note

Si instaló el controlador de 32 bits, la carpeta se llamará Controlador ODBC de Amazon Redshift (32 bits). Si instaló el controlador de 64 bits, la carpeta se llamará Controlador ODBC de Amazon Redshift (64 bits). Si instaló ambos controladores, tiene una carpeta para cada controlador.

3. Elija la pestaña System DSN (DNS de sistema) para configurar el controlador para todos los usuarios del equipo o la pestaña User DSN (DSN de usuario) si para configurar solamente el controlador para la cuenta de usuario.
4. Elija Add (Agregar). Se abrirá la ventana Create New Data Source (Crear nuevo origen de datos).
5. Elija el icono Amazon Redshift Controlador ODBC y, a continuación, elija Finish. La Configuración de DSN del controlador ODBC de Amazon Redshift se abre la ventana.
6. En Connection Settings (Configuración de conexión), escriba la siguiente información:

Nombre de origen de datos

Escriba un nombre para el origen de datos. Puede usar cualquier nombre que desee para identificar el origen de datos más adelante cuando cree la conexión al clúster. Por ejemplo, si ha seguido el Amazon Redshift Introducción, podría escribir `exampleclusterdsn` para que sea más fácil recordar el clúster que asocia con este DSN.

Server

Especifique el punto de enlace para su clúster de Amazon Redshift. Puede encontrar esta información en la consola de Amazon Redshift en la página de detalles del clúster. Para obtener más información, consulte [Configuración de conexiones en Amazon Redshift](#) (p. 99).

Port

Escriba el número de puerto que usa la base de datos. De forma predeterminada, Amazon Redshift usa el 5439, pero utilice el puerto configurado para el clúster en el momento del lanzamiento.

Database

Escriba el nombre de la base de datos de Amazon Redshift. Si ha lanzado el clúster sin especificar un nombre de base de datos, escriba **dev**. De lo contrario, utilice el nombre que eligió durante el proceso de inicio. Si siguió las especificaciones de Amazon Redshift Introducción, introduzca **dev**.

7. En Authentication (Autenticación), especifique las opciones de configuración para configurar la autenticación de IAM o estándar. Para obtener información acerca de las distintas opciones de autenticación, consulte «Configuración de la autenticación en Windows» en Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.
8. En SSL Settings (Configuración de SSL), especifique un valor para el siguiente campo:

Autenticación SSL

Elija un modo para controlar la Capa de conexión segura (SSL). En un entorno de prueba, podría usar `prefer`. Sin embargo, para entornos de producción y cuando se requiera un intercambio seguro de datos, use `verify-ca` o `verify-full`. Para obtener más información acerca del uso de SSL en Windows, consulte «Configuración de la verificación SSL en Windows» en Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.

9. En Additional Options (Opciones adicionales), especifique las opciones sobre cómo devolver los resultados de la consulta a la herramienta o aplicación cliente SQL. Para obtener más información, consulte «Configuración de opciones adicionales en Windows» en Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.
10. En Logging Options (Opciones de registro), especifique valores para la opción de registro. Para obtener más información, consulte «Configuración de las opciones de registro en Windows» en Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.

A continuación, seleccione OK (Aceptar).

11. En Data Type Options (Opciones de tipo de datos), especifique valores para los tipos de datos. Para obtener más información, consulte «Configuración de opciones de tipo de datos en Windows» en Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.

A continuación, seleccione OK (Aceptar).

12. Seleccione Test (Probar). Si el equipo cliente puede conectarse a la base de datos de Amazon Redshift, verá el siguiente mensaje: Conexión realizada correctamente.

Si el equipo cliente no puede conectarse a la base de datos, puede solucionar los posibles problemas. Para obtener más información, consulte [Solución de problemas de conexión en Amazon Redshift \(p. 169\)](#).

13. Configure las conexiones keepalive de TCP en Windows para evitar que se agote el tiempo de espera en las conexiones. Para obtener información acerca de cómo configurar conexiones keepalive de TCP en Windows, consulte Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.
14. Para ayudar a solucionar problemas, configure el registro. Para obtener información acerca de cómo configurar el registro en Windows, consulte Guía de Instalación y configuración del controlador ODBC de Amazon Redshift.

Instalación del controlador ODBC de Amazon Redshift en Linux

Requisitos del sistema

Debe instalar el controlador ODBC de Amazon Redshift en los equipos cliente que tienen acceso a un almacén de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista

de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte [Guía de instalación y configuración del controlador ODBC de Amazon Redshift](#).

Instalación del controlador de Amazon Redshift en sistemas operativos Linux

Siga los pasos en esta sección para descargar e instalar los controladores ODBC de Amazon Redshift en una distribución Linux compatible. El proceso de instalación instala los archivos del controlador en los siguientes directorios:

- /opt/amazon/redshiftodbc/lib/32 (para un controlador de 32 bits)
- /opt/amazon/redshiftodbc/lib/64 (para un controlador de 64 bits)
- /opt/amazon/redshiftodbc/ErrorMessage
- /opt/amazon/redshiftodbc/Setup

Para instalar el controlador ODBC de Amazon Redshift

1. Descargue alguno de los siguientes controladores, según la arquitectura de sistema de su aplicación o su herramienta de cliente SQL:
 - [Versión del controlador RPM de 32 bits](#)
 - [Versión del controlador RPM de 64 bits](#)
 - [Versión del controlador Debian de 32 bits](#)
 - [Versión del controlador Debian de 64 bits](#)

El nombre de cada uno de estos controladores Amazon Redshift ODBC de.

Note

Descargue el paquete que corresponde a la arquitectura de sistema de su aplicación o su herramienta de cliente SQL. Por ejemplo, si su herramienta de cliente es de 64 bits, instale un controlador de 64 bits.

A continuación, descargue y lea el [Contrato de licencia del controlador ODBC y JDBC de Amazon Redshift](#).

2. Vaya a la ubicación en la que descargó el paquete y, a continuación, ejecute alguno de los siguientes comandos. Utilice el comando que corresponda a su distribución Linux.
 - En los sistemas operativos RHEL y CentOS , ejecute el siguiente comando.

```
yum --nogpgcheck localinstall RPMFileName
```

Reemplace *RPMFileName* por el nombre de archivo del paquete RPM. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 32 bits.

```
yum --nogpgcheck localinstall AmazonRedshiftODBC-32bit-1.x.x.xxxx-x.x86_64.deb
```

- En SLES, ejecute el siguiente comando.

```
zypper install RPMFileName
```

Reemplace *RPMFileName* por el nombre de archivo del paquete RPM. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits.

```
zypper install AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.rpm
```

- En Debian, ejecute el siguiente comando.

```
sudo apt install ./DEBFileName.deb
```

Sustituya *DEBFileName.deb* por el nombre del archivo del paquete Debian. Por ejemplo, el siguiente comando demuestra cómo instalar el controlador de 64 bits.

```
sudo apt install ./AmazonRedshiftODBC-1.x.x.xxxx-x.x86_64.deb
```

Important

Cuando haya terminado de instalar los controladores, configúrelos para usarlos en su sistema. Para obtener más información acerca de la configuración de los controladores, consulte [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X](#) (p. 144).

Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X

Requisitos del sistema

Debe instalar el controlador en los equipos cliente que acceden a un almacén de datos de Amazon Redshift. Cada equipo en el que instala el controlador debe cumplir una lista de requisitos mínimos de sistema: Para obtener información acerca de los requisitos mínimos del sistema, consulte [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Instalación del controlador ODBC de Amazon Redshift en macOS X

Siga los pasos indicados en esta sección para descargar e instalar el controlador ODBC de Amazon Redshift ODBC en una versión compatible con macOS X. El proceso de instalación instala los archivos del controlador en los siguientes directorios:

- /opt/amazon/redshift/lib/universal
- /opt/amazon/redshift/ErrorMessage
- /opt/amazon/redshift/Setup

Para instalar el controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X

1. Descarga de [controlador de macOS X versión 1.4.27](#). El nombre de este controlador es controlador ODBC de Amazon Redshift.

Important

Después de la rotación del certificado el 4 de septiembre de 2020, el controlador ODBC versión 1.4.8.1000 o anterior en macOS no podrá establecer conexiones con clústeres de Amazon Redshift. Para obtener más información, consulte [Se requiere actualización del controlador para el controlador ODBC de Amazon Redshift anterior a 1.4.10 en macOS de Apple](#).

A continuación, descargue y lea el [Contrato de licencia del controlador ODBC y JDBC de Amazon Redshift](#).

2. Haga doble clic en AmazonRedshiftODBC.dmg para montar la imagen del disco.
3. Haga doble clic en AmazonRedshiftODBC.pkg para ejecutar el instalador.

4. Siga los pasos del instalador para completar el proceso de instalación del controlador. Para llevar a cabo la instalación, acepte los términos del acuerdo de licencia.

Important

Cuando haya terminado de instalar el controlador, configúrelo para usarlo en su sistema. Para obtener más información acerca de la configuración de los controladores, consulte [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X](#) (p. 144).

Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X

En los sistemas operativos Linux y Mac OS X, debe utilizar un administrador de controlador ODBC para configurar la conexión ODBC. Los administradores del controlador ODBC usan archivos de configuración para definir y configurar los controladores y el origen de datos de ODBC. El administrador del controlador ODBC que utiliza depende del sistema operativo que utiliza:

- Administrador de controladores de UnixODBC (para sistemas operativos Linux)
- Administrador de controladores IODBC (para el sistema operativo macOS X)

Para obtener más información acerca de los administradores de controladores ODBC compatibles que se utilizan para configurar los controladores ODBC de Amazon Redshift, consulte [Requisitos del sistema](#) (p. 141) Para sistemas operativos Linux y [Requisitos del sistema](#) (p. 143) Para sistemas operativos macOS X. Además, consulte «Especificación de administradores de controladores ODBC en máquinas que no sean de Windows» en [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Se necesitan tres archivos para configurar el controlador ODBC de Amazon Redshift: `amazon.redshiftodbc.ini`, `odbc.ini`, `yodbcinst.ini`.

Si instaló el controlador en la ubicación predeterminada, el archivo de configuración `amazon.redshiftodbc.ini` se encuentra en alguno de los siguientes directorios:

- `/opt/amazon/redshiftodbc/lib/32` (para el controlador de 32 bits en sistemas operativos Linux)
- `/opt/amazon/redshiftodbc/lib/64` (para el controlador de 64 bits en sistemas operativos Linux)
- `/opt/amazon/redshift/lib` (para el controlador en Mac OS X)

Además, `/opt/amazon/redshiftodbc/Setup` en Linux o `/opt/amazon/redshift/setup` en Mac OS X, hay archivos `odbc.ini` y `odbcinst.ini` de ejemplo. Puede utilizar estos archivos como ejemplos para configurar el controlador ODBC de Amazon Redshift y el nombre de origen de datos (DSN).

No le recomendamos utilizar el directorio de instalación del controlador ODBC de Amazon Redshift para los archivos de configuración. Los archivos de muestra del directorio `Setup` son solo para fines de ejemplo. Si vuelve a instalar el controlador ODBC de Amazon Redshift ODBC más adelante o actualiza a una versión más reciente, se sobrescribirá el directorio de instalación. A continuación, perderá los cambios que haya realizado en esos archivos.

Para evitarlo, copie el archivo `amazon.redshiftodbc.ini` en un directorio distinto al directorio de instalación. Si copia este archivo en el directorio principal del usuario, añada un punto (.) al principio del nombre del archivo para convertirlo en un archivo oculto.

Para los archivos `odbc.ini` y `odbcinst.ini`, utilice los archivos de configuración en el directorio principal del usuario o cree nuevas versiones en otro directorio. De forma predeterminada, su sistema operativo Linux o Mac OS X debe tener un archivo `odbc.ini` y un archivo `odbcinst.ini` en el directorio de inicio del usuario (`/home/$USER` o `~/`). Estos archivos predeterminados son archivos ocultos, que se

indica con el punto (.) delante de cada nombre de archivo. Estos archivos solo se muestran cuando se utiliza el indicador -a para enumerar el contenido del directorio.

Cualquiera que sea la opción que elija para los archivos `odbc.ini` y `odbcinst.ini`, modifique los archivos para agregar información de configuración del controlador y DSN. Si selecciona crear archivos nuevos, también deberá configurar variables de entorno para especificar la ubicación de estos archivos de configuración.

De forma predeterminada, los administradores de controladores ODBC están configurados para usar versiones ocultas de los archivos de configuración `odbc.ini` y `odbcinst.ini` (denominados `.odbc.ini` y `.odbcinst.ini`) ubicados en el directorio de inicio. También están configurados para utilizar el archivo `amazon.redshiftoDBC.ini` en la subcarpeta `/lib` del directorio de instalación del controlador. Si almacena estos archivos de configuración en otro lugar, establezca las variables de entorno que se describen a continuación para que el administrador de controladores pueda localizar los archivos. Para obtener más información, consulte «Especificación de las ubicaciones de los archivos de configuración del controlador» en [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Creación de un nombre de origen de datos en sistemas operativos Linux y Mac OS X

Cuando se conecte al almacenamiento de datos mediante un nombre de origen de datos (DSN), configure el archivo `odbc.ini` para definir los DSN. Establezca las propiedades del archivo `odbc.ini` para crear un DSN que especifique la información de conexión para el almacén de datos.

Para obtener información acerca de cómo configurar `laodbcini` Para obtener información acerca de «Creación de un nombre de origen de datos en una máquina que no sea de Windows» en [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Utilice el siguiente formato en sistemas operativos 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
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbc.ini` para sistemas operativos Linux.

```
[ODBC Data Sources]
Amazon_Redshift_x32=Amazon Redshift (x86)
Amazon_Redshift_x64=Amazon Redshift (x64)

[Amazon Redshift (x86)]
Driver=/opt/amazon/redshiftoDBC/lib/32/libamazonredshiftoDBC32.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US

[Amazon Redshift (x64)]
Driver=/opt/amazon/redshiftoDBC/lib/64/libamazonredshiftoDBC64.so
Host=examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com
Port=5932
Database=dev
locale=en-US
```

Utilice el siguiente formato en sistemas operativos Mac OS 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
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbc.ini` en sistemas operativos Mac OS 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
```

Configuración de una conexión sin DSN en sistemas operativos Linux y Mac OS X

Para conectarse al almacén de datos a través de una conexión que no tenga DSN, defina el controlador en el archivo `odbcinst.ini`. A continuación, proporcione una cadena de conexión sin DSN en su aplicación.

Para obtener información acerca de cómo configurar `laodbcinst.ini` En este caso, consulte «Configuración de una conexión sin DSN en una máquina que no sea de Windows» en [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Utilice el siguiente formato en sistemas operativos Linux:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/driver_file
...
```

En el siguiente ejemplo, se muestra la configuración de `odbcinst.ini` para los controladores de 32 y 64 bits que se instalan en los directorios predeterminados en sistemas operativos Linux.

```
[ODBC Drivers]
Amazon Redshift (x86)=Installed
Amazon Redshift (x64)=Installed

[Amazon Redshift (x86)]
Description=Amazon Redshift ODBC Driver (32-bit)
Driver=/opt/amazon/redshiftodbc/lib/32/libamazonredshiftodbc32.so

[Amazon Redshift (x64)]
Description=Amazon Redshift ODBC Driver (64-bit)
Driver=/opt/amazon/redshiftodbc/lib/64/libamazonredshiftodbc64.so
```

Utilice el siguiente formato en sistemas operativos Mac OS X:

```
[ODBC Drivers]
driver_name=Installed
...

[driver_name]
Description=driver_description
Driver=path/lib/amazonredshiftodbc.dylib
...
```

En el siguiente ejemplo, se muestra la configuración del archivo `odbcinst.ini` para el controlador que se instala en el directorio predeterminado en sistemas operativos Mac OS 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
```

Configuración de variables de entorno

Utilice el administrador de controladores ODBC correcto para cargar el controlador correcto. Para ello, configure la variable de entorno de ruta de biblioteca. Para obtener más información, consulte «Especificación de administradores de controladores ODBC en máquinas que no sean Windows» en [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

De forma predeterminada, los administradores de controladores ODBC están configurados para usar versiones ocultas de los archivos de configuración `odbc.ini` y `odbcinst.ini` (denominados `.odbc.ini` y `.odbcinst.ini`) ubicados en el directorio de inicio. También están configurados para utilizar el archivo `amazon.redshiftodbc.ini` en la subcarpeta `/lib` del directorio de instalación del controlador. Si almacena estos archivos de configuración en otro lugar, las variables de entorno para que el administrador de controladores pueda localizar los archivos. Para obtener más información, consulte «Especificación de las ubicaciones de los archivos de configuración del controlador» en [Guía de Instalación y configuración de controladores ODBC de Amazon Redshift](#).

Configuración de las características de conexión

Puede configurar las siguientes características de conexión para la configuración de ODBC:

- Configure el controlador ODBC de para proporcionar credenciales y autenticar la conexión a la base de datos de Amazon Redshift.
- Configure el controlador ODBC de para conectarse a un socket habilitado con la Capa de conexión segura (SSL), si se está conectando a un servidor de Amazon Redshift que tenga SSL habilitado.
- Configure el controlador ODBC para conectarse a Amazon Redshift a través de un servidor proxy.
- Configure el controlador ODBC para utilizar un modo de procesamiento de consultas para evitar que las consultas consuman demasiada memoria.
- Configure el controlador ODBC para que transfiera los procesos de autenticación de IAM a través de un servidor proxy.
- Configure el controlador ODBC para que utilice conexiones keepalive de TCP para evitar que se agote el tiempo de espera en las conexiones.

Para obtener información acerca de estas características de conexión, consulte [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Configurar las opciones del controlador ODBC

Puede utilizar las opciones de configuración para controlar el comportamiento del controlador ODBC de Amazon Redshift.

En Microsoft Windows, por lo general, las opciones del controlador se configuran cuando configura un nombre de origen de datos (DSN). También puede establecer opciones de controlador en la cadena de conexión cuando se conecta mediante programación o agregando o cambiando claves del Registro en `HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\your_DSN`. Para obtener más información acerca de la configuración de un DSN, consulte [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows](#) (p. 139). Para ver un ejemplo de la configuración de las opciones del controlador en una cadena de conexión, consulte [Conexión a su clúster mediante programación](#) (p. 166).

En Linux y Mac OS X, se establecen las opciones de configuración del controlador en los archivos `odbc.ini` y `amazon.redshiftodbc.ini`, como se describe en [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X](#) (p. 144). Las opciones de configuración establecidas en un archivo `amazon.redshiftodbc.ini` se aplican a todas las conexiones. Sin embargo, las opciones de configuración establecidas en un archivo `odbc.ini` son específicas de una conexión. Las opciones de configuración establecidas en `odbc.ini` tienen prioridad sobre las opciones de configuración establecidas en `amazon.redshiftodbc.ini`.

Para obtener información acerca de cómo configurar las opciones de configuración del controlador ODBC, consulte [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Usar versiones anteriores de controladores ODBC en algunos casos

Descargue una versión anterior del controlador ODBC de Amazon Redshift de solo si su herramienta requiere una versión específica del controlador.

Para la autenticación mediante AWS Identity and Access Management para las credenciales de (IAM) o las credenciales de un proveedor de identidad (IdP), use el controlador ODBC de Amazon Redshift versión 1.3.6.1000 o posterior.

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Si tiene que usar una versión del controlador anterior a 1.3.7.1000, es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL](#) (p. 155).

Usar versiones anteriores del controlador ODBC para Windows

Los siguientes son los controladores de 32 bits:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC32-1.4.27.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC32-1.4.20.1001.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC32-1.4.18.1001.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC32-1.4.17.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC32-1.4.16.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC32-1.4.14.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC32-1.4.13.1000.msi>.

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC32-1.4.11.1000.msi> .
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC32-1.4.10.1000.msi> .
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC32-1.4.8.1000.msi>.

Los siguientes son los controladores de 64 bits:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC64-1.4.27.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC64-1.4.20.1001.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC64-1.4.18.1001.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC64-1.4.17.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC64-1.4.16.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC64-1.4.14.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC64-1.4.13.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC64-1.4.11.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC64-1.4.10.1000.msi>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC64-1.4.8.1000.msi>.

Usar versiones anteriores del controlador ODBC para Linux

Las siguientes son las versiones del controlador de 32 bits:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC-32-bit-1.4.27.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC-32-bit-1.4.20.1001-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC-32-bit-1.4.20.1001-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC-32-bit-1.4.18.1001-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC-32-bit-1.4.18.1001-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC-32-bit-1.4.17.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC-32-bit-1.4.17.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC-32-bit-1.4.16.1000-1.i686.rpm>.

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC-32-bit-1.4.16.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC-32-bit-1.4.14.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC-32-bit-1.4.14.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC-32-bit-1.4.13.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC-32-bit-1.4.13.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC-32-bit-1.4.11.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC-32-bit-1.4.11.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC-32-bit-1.4.10.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC-32-bit-1.4.10.1000-1.i686.deb>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC-32-bit-1.4.8.1000-1.i686.rpm>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC-32-bit-1.4.8.1000-1.i686.deb>.

Las siguientes son las versiones del controlador de 64 bits:

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC-64-bit-1.4.27.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC-64-bit-1.4.27.1000-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC-64-bit-1.4.20.1001-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC-64-bit-1.4.20.1001-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC-64-bit-1.4.18.1001-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC-64-bit-1.4.18.1001-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC-64-bit-1.4.17.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC-64-bit-1.4.17.1000-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC-64-bit-1.4.16.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC-64-bit-1.4.16.1000-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC-64-bit-1.4.14.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC-64-bit-1.4.14.1000-1.x86_64.deb.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC-64-bit-1.4.13.1000-1.x86_64.rpm.

- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC-64-bit-1.4.13.1000-1.x86_64.deb .
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC-64-bit-1.4.11.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC-64-bit-1.4.11.1000-1.x86_64.deb .
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC-64-bit-1.4.10.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC-64-bit-1.4.10.1000-1.x86_64.deb .
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC-64-bit-1.4.8.1000-1.x86_64.rpm.
- https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.8.1000/AmazonRedshiftODBC-64-bit-1.4.8.1000-1.x86_64.deb .

Usar versiones anteriores del controlador ODBC para Mac OS X

A continuación, se muestran las versiones del controlador ODBC de Amazon Redshift para macOS X:

- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.27.1000/AmazonRedshiftODBC-1.4.27.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.20.1001/AmazonRedshiftODBC-1.4.20.1001.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.18.1001/AmazonRedshiftODBC-1.4.18.1001.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.17.1000/AmazonRedshiftODBC-1.4.17.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.16.1000/AmazonRedshiftODBC-1.4.16.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.14.1000/AmazonRedshiftODBC-1.4.14.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.13.1000/AmazonRedshiftODBC-1.4.13.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.11.1000/AmazonRedshiftODBC-1.4.11.1000.dmg>.
- <https://s3.amazonaws.com/redshift-downloads/drivers/odbc/1.4.10.1000/AmazonRedshiftODBC-1.4.10.1000.dmg>.

Important

Después de la rotación del certificado el 4 de septiembre de 2020, el controlador ODBC versión 1.4.8.1000 o anterior en macOS no podrá establecer conexiones con clústeres de Amazon Redshift. Para obtener más información, consulte [Se requiere actualización del controlador para el controlador ODBC de Amazon Redshift anterior a 1.4.10 en macOS de Apple](#).

Configuración de las opciones de seguridad para las conexiones

Amazon Redshift admite conexiones de Secure Sockets Layer (SSL) para cifrar datos y certificados de servidor para validar el certificado de servidor al que se conecta el cliente.

Conexión mediante una SSL

Para admitir conexiones SSL, Amazon Redshift crea e instala un [AWS Certificate Manager \(ACM\)](#) emitió el certificado SSL en cada clúster. Puede encontrar el conjunto de entidades de certificación en las que debe confiar para permitir SSL en <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt>. Si el paquete de certificados no se descarga, abra el menú contextual (haga clic con el botón derecho) del enlace y elija Guardar enlace como....

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL](#) (p. 155).

En las regiones de China el 5 de enero de 2021, Amazon Redshift está sustituyendo los certificados SSL de sus clústeres por [AWS Certificate Manager \(ACM\)](#) expidió certificados. Este cambio le afecta si sus clientes SQL o aplicaciones se conectan a Amazon Redshift mediante SSL con el `sslMode` opción de conexión establecida en `require, verify-ca`, o bien `verify-full`. El paquete de certificados anterior (<https://s3.cn-north-1.amazonaws.com.cn/redshift-downloads-cn/redshift-ssl-ca-cert.pem>) no funcionará después de la migración.

Utilice el paquete actualizado de <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt>. El número de suma de comprobación MD5 esperado es `a3081eb4a7448982df1c23cd6aec9a87`. La suma de comprobación sha256 es `df6aeb84a2e65feb00bfb72a786d69000916c90218005cc3d92800226c06da8`.

De manera predeterminada, las bases de datos del clúster aceptan una conexión, independientemente de que use una SSL o no. Para configurar que su clúster requiera una conexión SSL, establezca el parámetro `require_ssl` en `true` en el grupo de parámetros asociado al clúster.

Amazon Redshift admite un modo SSL que cumpla con el Estándar de procesamiento de la información federal (FIPS) 140-2. El modo SSL compatible con FIPS está deshabilitado de forma predeterminada.

Important

Habilite el modo SSL compatible con FIPS solo si el sistema debe ser compatible con FIPS.

Para habilitar el modo SSL compatible con FIPS, establezca tanto el parámetro `use_fips_ssl` como `require_ssl` en `true` en el grupo de parámetros asociado al clúster. Para obtener información acerca de cómo modificar un grupo de parámetros, consulte [Grupos de parámetros de Amazon Redshift](#) (p. 210).

Amazon Redshift es compatible con el protocolo de acuerdo de clave de elliptic Curve Diffie—Hellman Ephemeral (ECDHE). Con ECDHE, tanto el cliente como el servidor tienen un par de claves pública-privada de curva elíptica que se usa para establecer un código secreto compartido sobre un canal inseguro. No es necesario que configure nada en Amazon Redshift para habilitar ECDHE. Si se conecta desde una herramienta de cliente SQL que utiliza ECDHE para cifrar la comunicación entre el cliente y el servidor, Amazon Redshift utilizará la lista de cifrado proporcionada para establecer la conexión correspondiente. Para obtener más información, consulte [Diffie de curva elíptica—hellman](#) en Wikipedia y [Cifrados](#) en el sitio web de OpenSSL.

Uso de certificados SSL y de entidad de certificación de confianza en ODBC

Si se conecta usando los controladores ODBC de Amazon Redshift más recientes (versión 1.3.7.1000 o posterior), puede omitir esta sección. Para descargar los controladores más recientes, consulte [Configuración de una conexión ODBC](#) (p. 138).

Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL](#) (p. 155).

El paquete de entidades de certificación de Amazon Redshift se almacena en <https://s3.amazonaws.com/redshift-downloads/redshift-ca-bundle.crt>

Puede verificar que el certificado que descargó coincide con el número de suma de comprobación MD5 esperado. Para hacer esto, puede usar el programa Md5sum en sistemas operativos Linux u otra herramienta en sistemas operativos Windows y Mac OS X.

Los DSN ODBC contienen un `sslmode` Una configuración que determina cómo administrar el cifrado de las conexiones cliente y la verificación de certificados del servidor. Amazon Redshift admite los siguientes `sslmode` de la conexión del cliente:

- `disable`

SSL está deshabilitada y la conexión no está cifrada.

- `allow`

Se utiliza SSL si el servidor lo requiere.

- `prefer`

Se utiliza SSL si el servidor lo admite. Amazon Redshift admite SSL, por lo que se utiliza cuando se establece `sslmode` de `prefer`.

- `require`

SSL es obligatoria.

- `verify-ca`

Se debe utilizar SSL y se debe comprobar el certificado de servidor.

- `verify-full`

Se debe utilizar SSL. Se debe comprobar el certificado de servidor y el nombre del host debe coincidir con el atributo del nombre de host del certificado.

Puede determinar si se utiliza SSL y si se verifican los certificados del servidor en una conexión entre el cliente y el servidor. Para ello, debe revisar el `sslmode` para el DSN de ODBC en el cliente y el `require_ssl` para el clúster de Amazon Redshift del servidor. En la tabla a continuación, se describe el resultado del cifrado para diferentes combinaciones de configuraciones de clientes y servidores:

sslmode (cliente)	require_ssl (servidor)	Resultado
disable	false	La conexión no está cifrada.
disable	true	No se puede establecer la conexión porque el servidor requiere SSL y el cliente tiene SSL deshabilitado para la conexión.
allow	true	La conexión está cifrada.
allow	false	La conexión no está cifrada.
prefer o bien require	true	La conexión está cifrada.
prefer o bien require	false	La conexión está cifrada.
verify-ca	true	La conexión está cifrada y se comprueba el certificado de servidor.
verify-ca	false	La conexión está cifrada y se comprueba el certificado de servidor.

sslmode (cliente)	require_SSL (servidor)	Resultado
verify-full	true	La conexión está cifrada y se comprueba el certificado de servidor y el nombre de host.
verify-full	false	La conexión está cifrada y se comprueba el certificado de servidor y el nombre de host.

Conexión a través del certificado de servidor con ODBC en Microsoft Windows

Si desea conectarse al clúster mediante SSL y el certificado de servidor, descargue primero el certificado en el equipo cliente o instancia de Amazon EC2. A continuación, configure el DSN ODBC.

1. Descarga de [Paquete de entidades de certificación de Amazon Redshift](#) a su equipo cliente en el libEn el directorio de instalación del controlador y guarde el archivo como `root.crt`.
2. Abra ODBC Data Source Administrator (Administrador de orígenes de datos de ODBC) y añada o edite la entrada DSN del sistema de su conexión ODBC. En SSL Mode (Modo SSL), seleccione `verify-full` a menos que use un alias DNS. Si usa un alias DNS, seleccione `verify-ca`. A continuación, elija Save.

Para obtener más información acerca de la configuración del DSN de ODBC, consulte [Configuración de una conexión ODBC \(p. 138\)](#).

Uso de certificados SSL y de servidor en Java

SSL proporciona una capa de seguridad al cifrar los datos que se mueven entre su cliente y el clúster. El uso de un certificado de servidor proporciona una capa adicional de seguridad, ya que comprueba que el clúster sea un clúster de Amazon Redshift. La validación la hace comprobando que el certificado de servidor se instale automáticamente en todos los clústeres que usted aprovisiona. Para obtener más información acerca del uso de certificados de servidor con JDBC, visite [Configuring the Client](#) en la documentación de PostgreSQL.

Conexión mediante certificados de entidad de certificación en Java

Si se conecta usando los controladores JDBC de Amazon Redshift más recientes (versión 1.2.8.1005 o posterior), puede omitir esta sección. Para descargar los controladores más recientes, consulte [Configuración de una conexión JDBC](#).

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL \(p. 155\)](#).

Para conectarse mediante certificados de CA de confianza

Puede utilizar la herramienta `redshift-keytool.jar` Para importar los certificados de entidad de certificación del paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java o en su TrustStore privado.

1. Si usa la opción `-Djavax.net.ssl.trustStore` de la línea de comandos de Java, elimínala de la línea de comandos, si es posible.
2. Descargue [redshift-keytool.jar](#).
3. Aplique alguna de las siguientes acciones:

- Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java, ejecute el siguiente comando.

```
java -jar redshift-keytool.jar -s
```

- Para importar el paquete de entidades de certificación de Amazon Redshift en su TrustStore privado, ejecute el siguiente comando:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -p <keystore_password>
```

Migración a certificados de ACM para las conexiones SSL

Amazon Redshift está sustituyendo los certificados SSL de sus clústeres por [AWS Certificate Manager \(ACM\)](#) Certificados emitidos. ACM es una entidad de certificación (CA) pública de confianza en la que confían la mayoría de los sistemas actuales. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL.

Este cambio solo le afecta si se dan las siguientes circunstancias:

- Sus clientes SQL o aplicaciones se conectan a clústeres de Amazon Redshift mediante SSL con el conjunto de opciones de conexión `sslMode` establecido en la opción de configuración `require`, `verify-ca` o `verify-full`.
- No va a usar los controladores ODBC u JDBC de Amazon Redshift ODBC o usa controladores de Amazon Redshift anteriores a ODBC versión 1.3.7.1000 o JDBC versión 1.2.8.1005.

Si este cambio le afecta en regiones comerciales de Amazon Redshift, debe actualizar los certificados de entidad de certificación raíz de confianza actuales antes del 23 de octubre de 2017. Amazon Redshift migrará sus clústeres para usar certificados de ACM entre la fecha actual y el 23 de octubre de 2017. El cambio apenas debería tener efecto en el rendimiento o la disponibilidad de sus clústeres.

Si este cambio le afecta en AWS GovCloud (US) Para evitar la interrupción del servicio, debe actualizar sus certificados de CA raíz actuales antes del 1 de abril de 2020. A partir de esta fecha, los clientes que se conectan a clústeres de Amazon Redshift mediante conexiones cifradas SSL necesitan una entidad de certificación (CA) de confianza adicional. Los clientes utilizan entidades de certificación de confianza para confirmar la identidad del clúster de Amazon Redshift cuando se conectan a él. Su acción es necesaria para actualizar los clientes y aplicaciones SQL para utilizar un paquete de certificados actualizado que incluya la nueva entidad de certificación de confianza.

Important

En las regiones de China el 5 de enero de 2021, Amazon Redshift está sustituyendo los certificados SSL de sus clústeres por [AWS Certificate Manager \(ACM\)](#) expidió certificados. Si este cambio le afecta en la región China (Beijing) o la región China (Ningxia), debe actualizar los certificados de entidad de certificación raíz de confianza actuales antes del 5 de enero de 2021 para evitar la interrupción del servicio. A partir de esta fecha, los clientes que se conectan a clústeres de Amazon Redshift mediante conexiones cifradas SSL necesitan una entidad de certificación (CA) de confianza adicional. Los clientes utilizan entidades de certificación de confianza para confirmar la identidad del clúster de Amazon Redshift cuando se conectan a él. Su acción es necesaria para actualizar los clientes y aplicaciones SQL para utilizar un paquete de certificados actualizado que incluya la nueva entidad de certificación de confianza.

- [Uso de los controladores ODBC o JDBC de Amazon Redshift más recientes \(p. 156\)](#)
- [Uso de controladores ODBC o JDBC de Amazon Redshift anteriores \(p. 156\)](#)
- [Uso de otros tipos de conexión SSL \(p. 157\)](#)

Uso de los controladores ODBC o JDBC de Amazon Redshift más recientes

El método preferido es usar los controladores ODBC o JDBC de Amazon Redshift más recientes. Los controladores ODBC de Amazon Redshift a partir de la versión 1.3.7.1000 y JDBC a partir de la versión 1.2.8.1005 realizan la migración automáticamente desde un certificado autofirmado de Amazon Redshift a un certificado de ACM. Para descargar los controladores más recientes, consulte [Configuración de una conexión ODBC \(p. 138\)](#) o [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#).

Si usa el controlador JDBC de Amazon Redshift más reciente, es aconsejable que no use `-Djavax.net.ssl.trustStore` en las opciones de JVM. Si debe usar `-Djavax.net.ssl.trustStore`, importe el [paquete de entidades de certificación de Redshift](#) en el TrustStore al que apunta. Para obtener más información, consulte [Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore \(p. 156\)](#).

Uso de controladores ODBC o JDBC de Amazon Redshift anteriores

Si debe usar un controlador ODBC de Amazon Redshift anterior a la versión 1.3.7.1000, descargue el [Paquete de entidades de certificación de Redshift](#) y sobrescriba el archivo de certificado antiguo.

- Si el DSN de ODBC está configurado con `SSLCertPath`, sobrescriba el archivo de certificado en la ruta especificada.
- Si `SSLCertPath` no está establecido, sobrescriba el archivo de certificado `root.crt` en la ubicación de la DLL del controlador.

Si debe usar un controlador JDBC de Amazon Redshift anterior a la versión 1.2.8.1005, realice una de las siguientes acciones:

- Si la cadena de conexión de JDBC usa la opción `sslCert`, elimine la opción `sslCert`. A continuación, importe el [Paquete de entidades de certificación de Redshift](#) en su TrustStore de Java. Para obtener más información, consulte [Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore \(p. 156\)](#).
- Si usa la opción `-Djavax.net.ssl.trustStore` de la línea de comandos de Java, elimínala de la línea de comandos, si es posible. A continuación, importe el [Paquete de entidades de certificación de Redshift](#) en su TrustStore de Java. Para obtener más información, consulte [Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore \(p. 156\)](#).

Importación del paquete de entidades de certificación de Amazon Redshift en un TrustStore

Puede usar `redshift-keytool.jar` para importar los certificados de entidad de certificación del paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java o en su truststore privado.

Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore

1. Descargue [redshift-keytool.jar](#).
2. Aplique alguna de las siguientes acciones:
 - Para importar el paquete de entidades de certificación de Amazon Redshift en un TrustStore de Java, ejecute el siguiente comando.

```
java -jar redshift-keytool.jar -s
```

- Para importar el paquete de entidades de certificación de Amazon Redshift en su TrustStore privado, ejecute el siguiente comando:

```
java -jar redshift-keytool.jar -k <your_private_trust_store> -p <keystore_password>
```

Uso de otros tipos de conexión SSL

Siga los pasos de esta sección si se conecta mediante alguno de los métodos siguientes:

- Controlador ODBC de código abierto
- Controlador JDBC de código abierto
- La interfaz de línea de comandos de `psql`
- Alguna conexión de lenguaje de programación basada en `libpq`, como `psycopg2` (Python) y `ruby-pg` (Ruby)

Para usar certificados de ACM con otros tipos de conexión SSL:

1. Descarga de [Paquete de entidades de certificación de Amazon Redshift](#).
2. Coloque los certificados del paquete en su archivo `root.crt`.
 - En los sistemas operativos Linux y Mac OS X, el archivo es `~/.postgresql/root.crt`
 - En Microsoft Windows, el archivo es `%APPDATA%\postgresql\root.crt`

Conexión a clústeres desde herramientas y código cliente

En esta sección, se proporcionan algunas opciones para que herramientas de terceros se conecten al clúster si todavía no tiene una herramienta de inteligencia empresarial para hacerlo. Además, se describe cómo conectarse a su clúster mediante programación.

Temas

- [Conexión a su clúster mediante SQL Workbench/J](#) (p. 157)
- [Conexión a su clúster a través de la herramienta `psql`](#) (p. 161)
- [Conexión a su clúster mediante programación](#) (p. 166)

Conexión a su clúster mediante SQL Workbench/J

Amazon Redshift no proporciona ni instala ninguna biblioteca o herramienta de cliente SQL, por lo que debe instalar la que desee usar con sus clústeres. Si ya tiene una aplicación de inteligencia empresarial o cualquier otra aplicación que pueda conectarse a sus clústeres a través de un controlador estándar JDBC u ODBC de PostgreSQL, puede omitir el contenido en esta sección. Si todavía no tiene una aplicación que pueda conectarse a su clúster, en esta sección se presenta una opción para hacerlo a través de SQL Workbench/J, una herramienta de consultas de SQL multiplataforma, gratuita y que no depende de un Database Management System (DBMS, Sistema de gestión de bases de datos).

Instalación de SQL Workbench/J

La Amazon Redshift En esta sección, explicaremos en detalle cómo puede conectarse a su clúster mediante SQL Workbench/J.

Pasos para instalar SQL Workbench/J

1. Consulte la [licencia de software de SQL Workbench/J](#).
2. Vaya a [SQL Workbench/J](#) Descargue el paquete adecuado para su sistema operativo en su equipo cliente o en la instancia de Amazon EC2.
3. Diríjase a la página [Installing and starting SQL Workbench/J](#). Siga las instrucciones para instalar SQL Workbench/J en su sistema.

Note

SQL Workbench/J requiere que tenga Java Runtime Environment (JRE) instalado en su sistema. Asegúrese de que está utilizando la versión correcta de JRE que requiere el cliente SQL Workbench/J. Para determinar qué versión de Java Runtime Environment se está ejecutando en su sistema, realice alguna de las siguientes operaciones:

- Mac: En el navegador Preferencias del sistema, haga clic en el icono de Java.
- Windows: En el navegador Panel de control, haga clic en el icono de Java.
- Cualquier sistema: En un shell de comandos, escriba `java -version`. También puede visitar <https://www.java.com>, hacer clic en el enlace [Verify Java \(¿Tengo Java?\)](#) y hacer clic en el botón Verify Java (Comprobar la versión de Java).

Para obtener más información sobre la instalación y configuración de Java Runtime Environment, vaya a <https://www.java.com>.

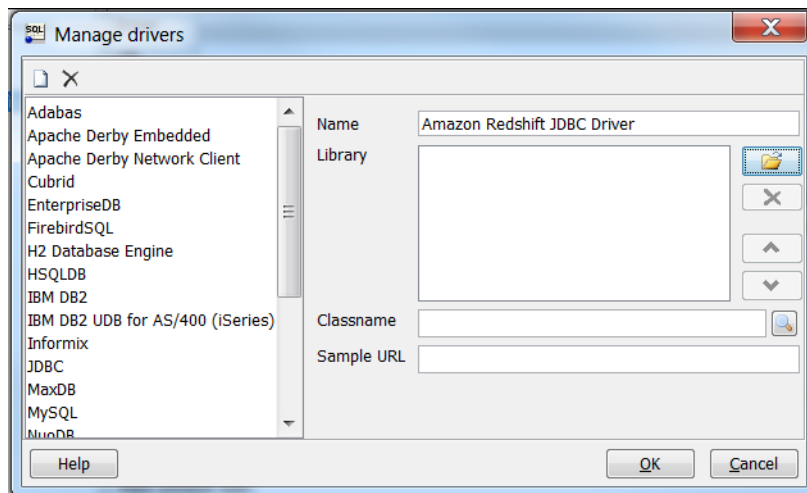
Conexión a su clúster a través de una conexión JDBC en SQL Workbench/J

Important

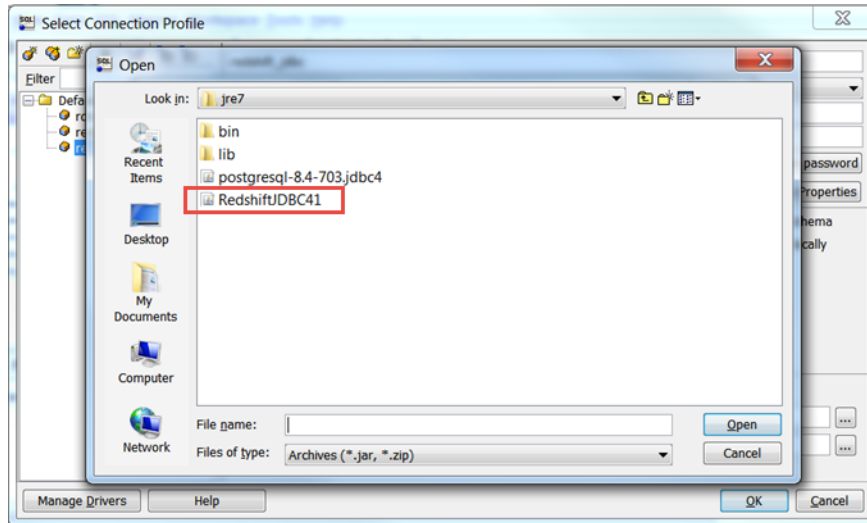
Antes de seguir los pasos indicados en este procedimiento, asegúrese de que el equipo cliente o la instancia de Amazon EC2 tengan el Amazon Redshift JDBC de recomendado. Para obtener los enlaces para descargar la versión más reciente de los controladores, consulte [Descargar un controlador JDBC de Amazon Redshift \(p. 130\)](#). Asegúrese también de que ha configurado los ajustes del firewall para permitir el acceso al clúster. Para obtener más información, consulte [Paso 4: Autorización de acceso al clúster](#).

Pasos para usar una conexión JDBC en SQL Workbench/J

1. Abra el SQL Workbench/J.
2. Seleccione File (Archivo) y Connect window (Ventana de conexión).
3. Seleccione Create a new connection profile (Crear nuevo perfil de conexión).
4. En el cuadro New profile (Nuevo perfil), escriba un nombre para el perfil. Por ejemplo, `examplecluster_jdbc`.
5. Seleccione Manage Drivers (Administrar controladores). Se abrirá el cuadro de diálogo Manage Drivers (Administrar controladores). En el cuadro Name (Nombre), escriba un nombre para el controlador.



Elija el icono de carpeta que se encuentra junto a la casilla Library (Biblioteca), navegue hasta la ubicación del controlador, elíjalo y haga clic en Open (Abrir).



Si aparece el cuadro de diálogo Please select one driver (Seleccione un controlador), elija com.amazon.redshift.jdbc4.Driver o com.amazon.redshift.jdbc41.Driver y haga clic en OK (Aceptar). SQL Workbench/J completa la casilla Classname (Nombre de clase) de forma automática. Deje la casilla Sample URL (URL de ejemplo) en blanco y seleccione OK (Aceptar).

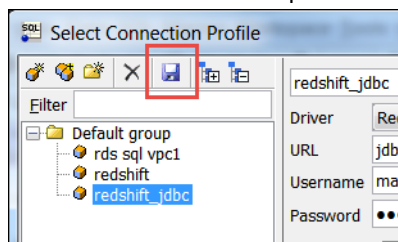
6. En la casilla Driver (Controlador), seleccione el controlador que acaba de añadir.
7. En URL Copie la URL de JDBC de la consola de Amazon Redshift y péguela aquí.

Para obtener más información acerca de cómo encontrar el URL de JDBC, consulte [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#).

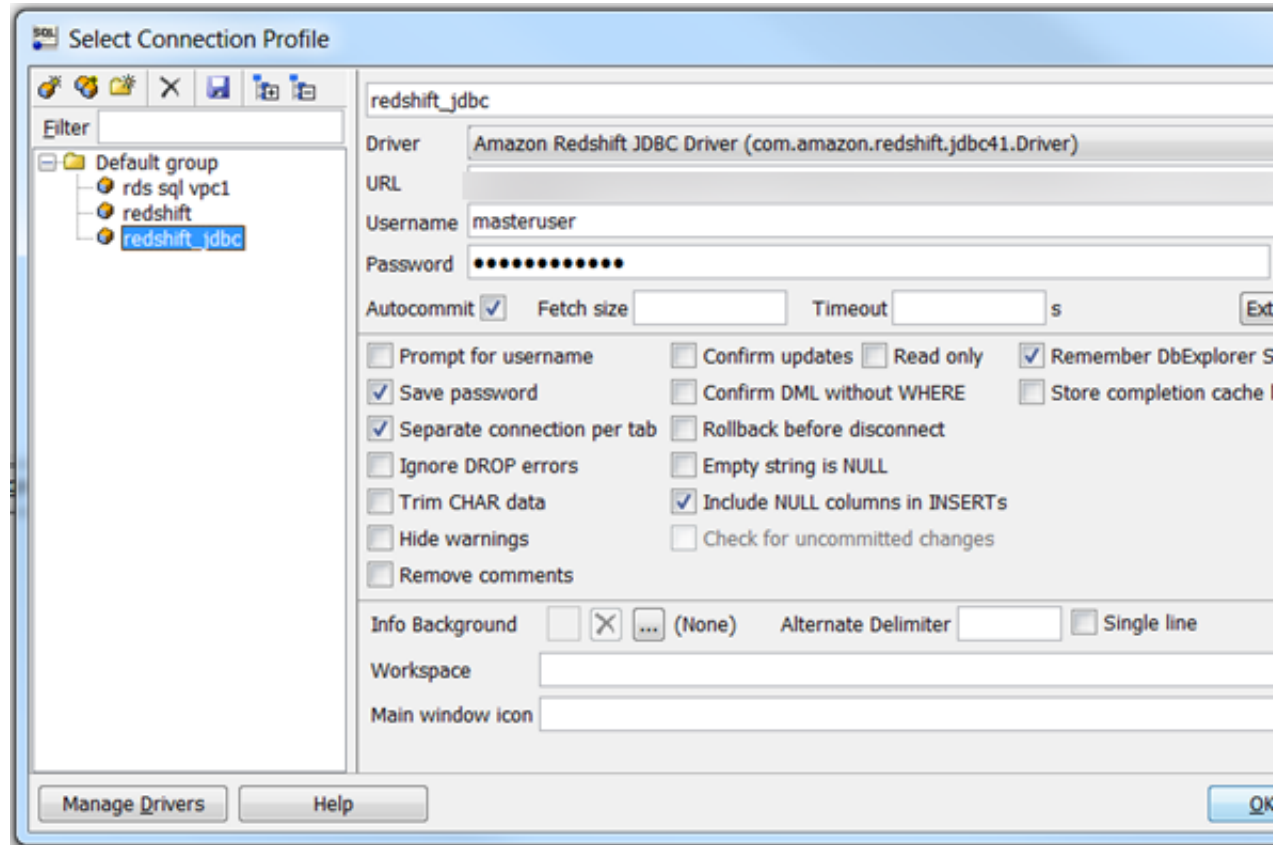
8. En Username (Nombre de usuario), escriba el nombre del usuario maestro.

Si está siguiendo el Amazon Redshift, escriba *masteruser*.

9. En Password (Contraseña), escriba la contraseña asociada con la cuenta de usuario principal.
10. Active la casilla Autocommit (Confirmar automáticamente).
11. Seleccione el icono Save profile list (Guardar lista de perfiles), tal y como se muestra a continuación:



12. Seleccione OK (Aceptar).



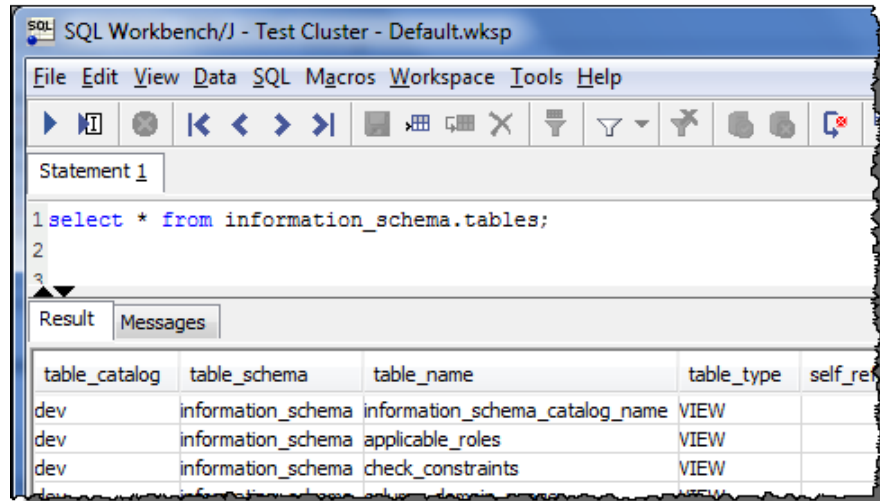
Prueba de la conexión de SQL Workbench/J

Una vez que haya configurado la conexión JDBC u ODBC, puede probar la conexión ejecutando una consulta de muestra.

1. Puede utilizar la siguiente consulta para probar su conexión.

```
select * from information_schema.tables;
```

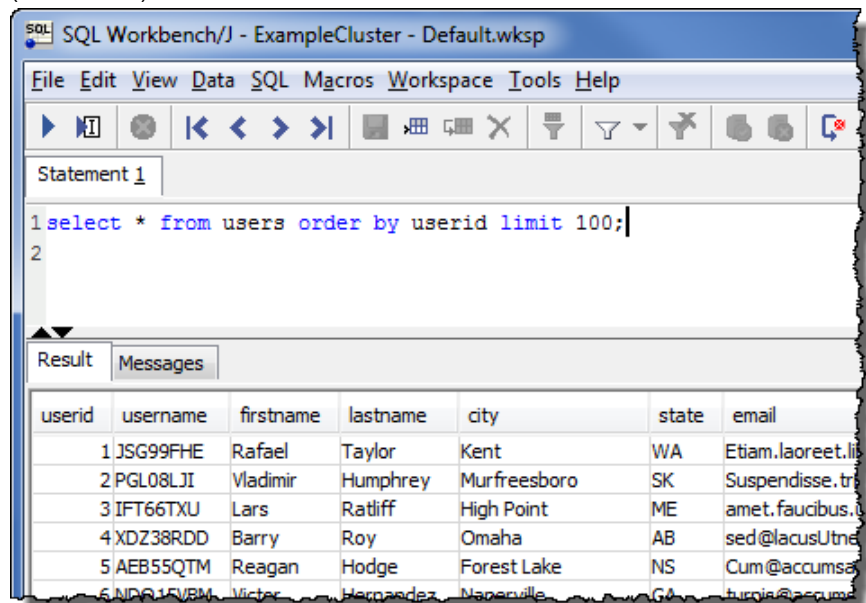
Si la conexión se realiza con éxito, aparecerá una lista de registros en la pestaña Results (Resultados).



2. Como alternativa, si cargó las tablas y los datos de muestra desde la página [Amazon Redshift](#) Para probar su conexión, escriba la siguiente consulta en el cuadro de texto Instrucción:

```
select * from users order by userid limit 100;
```

Si la conexión se realiza con éxito, aparecerá una lista de registros en la pestaña Results (Resultados).



Conexión a su clúster a través de la herramienta psql

Una vez que haya creado un clúster de Amazon Redshift, puede utilizar psql, una interfaz de usuario de PostgreSQL basada en terminales, para consultar los datos del clúster. Puede escribir las consultas de forma interactiva o leerlas desde un archivo. Para conectarse desde psql, debe especificar el punto de enlace del clúster, la base de datos y el puerto.

Note

Amazon Redshift no proporciona la herramienta psql; se instala con PostgreSQL. Para obtener información sobre el uso de psql, vaya a <https://www.postgresql.org/docs/8.4/static/app-psql.html>. Para obtener información sobre la instalación de las herramientas de cliente de PostgreSQL, seleccione el sistema operativo en la página de descargas binarias de PostgreSQL que encontrará en <https://www.postgresql.org/download/>.

Si tiene problemas para conectarse de un símbolo del sistema de Microsoft Windows debido a un valor de `client_encoding` no válido, establezca la variable de entorno `PGCLIENTENCODING` en UTF-8 antes de ejecutar psql.

```
set PGCLIENTENCODING=UTF8
```

Conexión mediante la configuración predeterminada de psql

De manera predeterminada, psql no comprueba el servicio de Amazon Redshift; realiza una conexión cifrada mediante Secure Sockets Layer (SSL, Capa de conexión segura).

Pasos para conectarse a través de la configuración predeterminada de psql

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. Elija uno de los siguientes pasos en función de qué consola de Amazon Redshift de esté utilizando:
 - (Nueva consola) En el panel de navegación, seleccione CLUSTERS (CLÚSTERES). Luego seleccione el nombre del clúster en la lista para abrir sus detalles. En la pestaña Properties (Propiedades) y en la sección Database configurations (Configuración de la base de datos), registre el Database name (Nombre de la base de datos) y el Port (Puerto). Consulte la sección Connection details (Detalles de conexión) y registre el Endpoint (Punto de enlace) que se encuentra en el siguiente formulario:

```
endpoint:port/databasename
```

- (Consola original) En el panel de navegación, seleccione Clusters (Clústeres). Haga clic en su clúster para abrirlo. En Cluster Database Properties (Propiedades de base de datos de clúster), registre los valores de Endpoint (Punto de enlace), Port (Puerto) y Database Name (Nombre de base de datos).

Cluster Database Properties	
Port	5439
Publicly Accessible	Yes
Elastic IP	
Database Name	dev
Master Username	masteruser
Encrypted	Yes
KMS Key ID	
JDBC URL	jdbc:redshift://examplecluster. .us- west-2.redshift. .com:5439/dev
ODBC URL	Driver={Amazon Redshift (x64)}; Server=examplecluster. .us- west-2.redshift.amazonaws.com; Database=dev; UID=masteruser; PWD=insert_your_master_user_pass word_here; Port=5439

3. En el símbolo del sistema, especifique la información de conexión usando los parámetros de línea de comando, o bien una cadena de información de conexión. Pasos para usar los parámetros:

```
psql -h <endpoint> -U <userid> -d <databasename> -p <port>
```

Donde:

- **<endpoint>** en el punto de enlace que registró en el paso anterior.
- **<userid>** es un ID de usuario con permisos para conectarse al clúster.
- **<databasename>** es el nombre de base de datos que registró en el paso anterior.
- **<port>** es el puerto que registró en el paso anterior.

Por ejemplo:

```
psql -h examplecluster.<XXXXXXXXXXXX>.us-west-2.redshift.amazonaws.com -U masteruser -d dev -p 5439
```

4. Cuando se le solicite la contraseña de psql, especifique la contraseña del usuario **<userid>**.

Está conectado al clúster y puede ingresar comandos de forma interactiva.

Conexión mediante un certificado

Para controlar si psql autentica el servicio mediante un certificado, debe usar una cadena de información de conexión para especificar la información de conexión y especificar la palabra clave `sslmode`. De manera predeterminada, psql funciona con `sslmode=prefer`. Para especificar que psql abra una

conexión cifrada y use un certificado de Amazon Redshift para comprobar el servicio, descargue un certificado de Amazon Redshift en su equipo. Especifique `verify-full` a menos que use un alias DNS. Si usa un alias DNS, seleccione `verify-ca`. Especifique `sslrootcert` con la ubicación del certificado. Para obtener más información acerca de `sslmode`, consulte [Configuración de las opciones de seguridad para las conexiones](#) (p. 151).

Para obtener más información sobre los parámetros de la cadena de información de conexión, consulte <https://www.postgresql.org/docs/8.4/static/libpq-connect.html>.

Pasos para conectarse mediante un certificado

1. Guarde la descarga del [paquete de entidades de certificación de Redshift](#) en un archivo `.crt` del equipo. Si realiza una operación File\Save as con Internet Explorer, especifique el tipo de archivo como Archivo de texto (*.txt) y elimine la extensión `.txt`. Por ejemplo, guárdelo como un archivo `c:\MyDownloads\redshift-ca-bundle.crt`.
2. Elija uno de los siguientes pasos en función de qué consola de Amazon Redshift de esté utilizando:
 - (Nueva consola) En el panel de navegación, seleccione CLUSTERS (CLÚSTERES). Luego seleccione el nombre del clúster en la lista para abrir sus detalles. En la pestaña Properties (Propiedades) y en la sección Database configurations (Configuración de la base de datos), registre el Database name (Nombre de la base de datos) y el Port (Puerto). Consulte la sección Connection details (Detalles de conexión) y registre el Endpoint (Punto de enlace) que se encuentra en el siguiente formulario:

`endpoint:port/databasename`

- (Consola original) En el panel de navegación, seleccione Clusters (Clústeres). Haga clic en su clúster para abrirlo. En Cluster Database Properties (Propiedades de base de datos de clúster), registre los valores de Endpoint (Punto de enlace), Port (Puerto) y Database Name (Nombre de base de datos).

Cluster Database Properties	
Port	5439
Publicly Accessible	Yes
Elastic IP	
Database Name	dev
Master Username	masteruser
Encrypted	Yes
KMS Key ID	
JDBC URL	<code>jdbc:redshift://examplecluster. us- west-2.redshift. com:54 39/dev</code>
ODBC URL	<code>Driver={Amazon Redshift (x64)}; Server=examplecluster. us- west-2.redshift.amazonaws.com; Database=dev; UID=masteruser; PWD=insert_your_master_user_pass word_here; Port=5439</code>

3. En el símbolo del sistema, especifique la información de conexión usando una cadena de información de conexión:

```
psql "host=<endpoint> user=<userid> dbname=<databasename> port=<port> sslmode=verify-ca  
sslrootcert=<certificate>"
```

Donde:

- **<endpoint>** en el punto de enlace que registró en el paso anterior.
- **<userid>** es un ID de usuario con permisos para conectarse al clúster.
- **<databasename>** es el nombre de base de datos que registró en el paso anterior.
- **<port>** es el puerto que registró en el paso anterior.
- **<certificate>** es la ruta completa del archivo del certificado. En sistemas Windows, se debe especificar la ruta del certificado con separadores / estilo Linux, en lugar de separadores \ de Windows.

En los sistemas operativos Linux y Mac OS X, la ruta es

```
~/postgresql/root.crt
```

En Microsoft Windows, la ruta es

```
%APPDATA%/postgresql/root.crt
```


Por ejemplo:

```
psql "host=examplecluster.<XXXXXXXXXXXX>.us-west-2.redshift.amazonaws.com
      user=masteruser dbname=dev port=5439 sslmode=verify-ca sslrootcert=C:/MyDownloads/
      redshift-ca-bundle.crt"
```

4. Cuando se le solicite la contraseña de psql, especifique la contraseña del usuario `<userid>`.

Está conectado al clúster y puede ingresar comandos de forma interactiva.

Conexión a su clúster mediante programación

En esta sección, se explica cómo conectarse a su clúster mediante programación. Si está usando una aplicación como SQL Workbench/J que le administra sus conexiones cliente, puede omitir el contenido en esta sección.

Conexión a un clúster mediante Java

Cuando usa Java para conectarse a su clúster mediante programación, puede hacerlo con o sin autenticación de servidor. Si piensa utilizar la autenticación del servidor, siga las instrucciones que se indican en [Configuración de las opciones de seguridad para las conexiones \(p. 151\)](#) para colocar el certificado de servidor de Amazon Redshift en un almacén de claves. Puede indicar el keystore especificando una propiedad cuando ejecute su código de la siguiente manera:

```
-Djavax.net.ssl.trustStore=<path to keystore>
-Djavax.net.ssl.trustStorePassword=<keystore password>
```

Example Conectar a un clúster mediante Java

En el siguiente ejemplo, se conecta a un clúster y se ejecuta una consulta de muestra que devuelve tablas de sistema. No es necesario tener datos en su base de datos para usar este ejemplo.

Si está usando un certificado de servidor para autenticar su clúster, puede restaurar la línea que usa el keystore, que aparece con comentarios:

```
props.setProperty("ssl", "true");
```

Para obtener más información acerca del certificado de servidor, consulte [Configuración de las opciones de seguridad para las conexiones \(p. 151\)](#).

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#).

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */
```

```
// snippet-sourcedescription:[ConnectToClusterExample demonstrates how to connect to an
Amazon Redshift cluster and run a sample query.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[Connect]
// snippet-keyword:[JDBC]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ConnectToCluster.complete]

package connection;

import java.sql.*;
import java.util.Properties;

public class ConnectToCluster {
    //Redshift driver: "jdbc:redshift://x.y.us-west-2.redshift.amazonaws.com:5439/dev";
    static final String dbURL = "***jdbc cluster connection string ***";
    static final String MasterUsername = "***master user name***";
    static final String MasterUserPassword = "***master user password***";

    public static void main(String[] args) {
        Connection conn = null;
        Statement stmt = null;
        try{
            //Dynamically load driver at runtime.
            //Redshift JDBC 4.1 driver: com.amazon.redshift.jdbc41.Driver
            //Redshift JDBC 4 driver: com.amazon.redshift.jdbc4.Driver
            Class.forName("com.amazon.redshift.jdbc.Driver");

            //Open a connection and define properties.
            System.out.println("Connecting to database...");
            Properties props = new Properties();

            //Uncomment the following line if using a keystore.
            //props.setProperty("ssl", "true");
            props.setProperty("user", MasterUsername);
            props.setProperty("password", MasterUserPassword);
            conn = DriverManager.getConnection(dbURL, props);

            //Try a simple query.
            System.out.println("Listing system tables...");
            stmt = conn.createStatement();
            String sql;
            sql = "select * from information_schema.tables;";
            ResultSet rs = stmt.executeQuery(sql);

            //Get the data from the result set.
            while(rs.next()){
                //Retrieve two columns.
                String catalog = rs.getString("table_catalog");
                String name = rs.getString("table_name");

                //Display values.
                System.out.print("Catalog: " + catalog);
                System.out.println(", Name: " + name);
            }
            rs.close();
            stmt.close();
            conn.close();
        }catch(Exception ex){
            //For convenience, handle all errors here.
            ex.printStackTrace();
        }
    }
}
```

```
    }finally{
        //Finally block to close resources.
        try{
            if(stmt!=null)
                stmt.close();
        }catch(Exception ex){
        }// nothing we can do
        try{
            if(conn!=null)
                conn.close();
        }catch(Exception ex){
            ex.printStackTrace();
        }
    }
    System.out.println("Finished connectivity test.");
}
// snippet-end:[redshift.java.ConnectToCluster.complete]
```

Conexión a un clúster mediante .NET

Cuando usa .NET (C#) para conectarse a su clúster mediante programación, puede hacerlo con o sin autenticación de servidor. Si piensa utilizar la autenticación del servidor, siga las instrucciones que se indican en [Configuración de las opciones de seguridad para las conexiones \(p. 151\)](#) Para descargar el certificado de servidor de Amazon Redshift y, a continuación, coloque el certificado en la forma adecuada para su código .NET.

Example Conectar a un clúster mediante .NET

En el siguiente ejemplo, se conecta a un clúster y se ejecuta una consulta de muestra que devuelve tablas de sistema. No muestra autenticación del servidor. No es necesario tener datos en su base de datos para usar este ejemplo. En este ejemplo, se usa el [espacio de nombres System.Data.Odbc](#), un proveedor de datos de .NET Framework para ODBC.

```
using System;
using System.Data;
using System.Data.Odbc;

namespace redshift.amazon.com.docsamples
{
    class ConnectToClusterExample
    {
        public static void Main(string[] args)
        {

            DataSet ds = new DataSet();
            DataTable dt = new DataTable();

            // Server, e.g. "examplecluster.xyz.us-west-2.redshift.amazonaws.com"
            string server = "***provide server name part of connection string***";

            // Port, e.g. "5439"
            string port = "***provide port***";

            // MasterUserName, e.g. "masteruser".
            string masterUsername = "***provide master user name***";

            // MasterUserPassword, e.g. "mypassword".
            string masterUserPassword = "***provide master user password***";

            // DBName, e.g. "dev"
            string DBName = "***provide name of database***";
```

```
string query = "select * from information_schema.tables;";

try
{
    // Create the ODBC connection string.
    //Redshift ODBC Driver - 64 bits
    /*
    string connString = "Driver={Amazon Redshift (x64)};" +
        String.Format("Server={0};Database={1};" +
            "UID={2};PWD={3};Port={4};SSL=true;Sslmode=Require",
            server, DBName, masterUsername,
            masterUserPassword, port);
    */

    //Redshift ODBC Driver - 32 bits
    string connString = "Driver={Amazon Redshift (x86)};" +
        String.Format("Server={0};Database={1};" +
            "UID={2};PWD={3};Port={4};SSL=true;Sslmode=Require",
            server, DBName, masterUsername,
            masterUserPassword, port);

    // Make a connection using the psqLODBC provider.
    OdbcConnection conn = new OdbcConnection(connString);
    conn.Open();

    // Try a simple query.
    string sql = query;
    OdbcDataAdapter da = new OdbcDataAdapter(sql, conn);
    da.Fill(ds);
    dt = ds.Tables[0];
    foreach (DataRow row in dt.Rows)
    {
        Console.WriteLine(row["table_catalog"] + ", " + row["table_name"]);
    }

    conn.Close();
    Console.ReadKey();
}
catch (Exception ex)
{
    Console.Error.WriteLine(ex.Message);
}
}
```

Solución de problemas de conexión en Amazon Redshift

Si tiene problemas para conectarse a su clúster desde una herramienta de cliente SQL, hay distintos puntos que puede controlar para acotar la solución del problema. Si está usando certificados SSL o de servidor, primero elimine esta complejidad mientras solucione el problema de conexión. Una vez que haya encontrado una solución, vuelva a añadirla. Para obtener más información, consulte [Configuración de las opciones de seguridad para las conexiones](#) (p. 151).

Important

Amazon Redshift ha cambiado la forma en que se administran los certificados SSL. Si tiene problemas para conectarse mediante SSL, es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL](#) (p. 155).

En la siguiente sección, se muestran algunos ejemplos de mensajes de error y posibles soluciones para los problemas de conexión. Como las diferentes herramientas de cliente SQL proporcionan diferentes mensajes de error, esta no es una lista completa, pero debe ser un buen punto de partida para la solución de problemas.

Temas

- [Conexión desde fuera de Amazon EC2: problema de tiempo de espera del cortafuegos \(p. 170\)](#)
- [La conexión devuelve un error o se rechaza \(p. 172\)](#)
- [El cliente y el controlador son incompatibles \(p. 173\)](#)
- [Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster \(p. 173\)](#)

Conexión desde fuera de Amazon EC2: problema de tiempo de espera del cortafuegos

Problema de ejemplo

Su conexión cliente a la base de datos parece que dejó de funcionar o que superó el tiempo de espera mientras ejecutaba consultas largas, como un comando COPY. En este caso, puede observar que la consola de Amazon Redshift muestra que la consulta ha terminado, pero, aparentemente, la herramienta propia del cliente está ejecutando la consulta. Los resultados de la consulta podrían ser que falta procesar o que está incompleta según cuándo se haya detenido la conexión.

Posibles soluciones:

Este problema ocurre cuando se conecta a Amazon Redshift desde una máquina que no sea una instancia de Amazon EC2. En este caso, las conexiones inactivas se terminan mediante un componente de red intermedio, como un firewall, después de un período de inactividad. Este comportamiento suele producirse cuando se inicia sesión desde una red privada virtual (VPN) o desde la red local.

Para evitar estos tiempos de espera, le recomendamos realizar los siguientes cambios:

- Aumentar los valores del sistema cliente que administran los tiempos de espera de TCP/IP. Realice estos cambios en el equipo que está usando para conectarse a su clúster. El período de tiempo de espera debe adaptarse a su cliente y su red. Para obtener más información, consulte [Modificación de la configuración del tiempo de espera de TCP/IP \(p. 170\)](#).
- Si lo prefiere, configure el comportamiento de keepalive en el nivel de DSN. Para obtener más información, consulte [Modificación de la configuración del tiempo de espera del DSN \(p. 171\)](#).

Modificación de la configuración del tiempo de espera de TCP/IP

Para cambiar la configuración del tiempo de espera de TCP/IP, establezca las configuraciones de tiempo de espera conforme al sistema operativo que usa para conectarse a su clúster.

- Linux: si su cliente se está ejecutando en Linux, ejecute el siguiente comando como el usuario raíz para cambiar la configuración de tiempo de espera para la sesión actual:

```
/sbin/sysctl -w net.ipv4.tcp_keepalive_time=200 net.ipv4.tcp_keepalive_intvl=200  
net.ipv4.tcp_keepalive_probes=5
```

Para continuar con la configuración, cree o modifique el archivo `/etc/sysctl.conf` con los siguientes valores y, luego, reinicie su sistema.

```
net.ipv4.tcp_keepalive_time=200
```

```
net.ipv4.tcp_keepalive_intvl=200
net.ipv4.tcp_keepalive_probes=5
```

- Windows: si su cliente se ejecuta en Windows, edite los valores para las siguientes configuraciones de registro en HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControlSet\ Services\ Tcpip\ Parameters\:
 - KeepAliveTime: 30000
 - KeepAliveInterval: 1 000
 - TcpMaxDataRetransmissions: 10

Estas configuraciones usan tipos de datos DWORD. Si no existen en la ruta de registro, puede crear las configuraciones y especificar estos valores recomendados. Para obtener más información acerca de cómo editar el registro de Windows, consulte la documentación de Windows.

Después de configurar estos valores, reinicie su equipo para que se apliquen los cambios.

- Mac: Si su cliente se está ejecutando en una Mac, ejecute los siguientes comandos para cambiar la configuración de tiempo de espera para la sesión actual:

```
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
```

Para continuar con la configuración, cree o modifique el archivo `/etc/sysctl.conf` con los siguientes valores:

```
net.inet.tcp.keepidle=200000
net.inet.tcp.keepintvl=200000
net.inet.tcp.keepinit=200000
net.inet.tcp.always_keepalive=1
```

Reinicie su equipo y, luego, ejecute los siguientes comandos para controlar que los valores están configurados.

```
sysctl net.inet.tcp.keepidle
sysctl net.inet.tcp.keepintvl
sysctl net.inet.tcp.keepinit
sysctl net.inet.tcp.always_keepalive
```

Modificación de la configuración del tiempo de espera del DSN

Puede configurar el comportamiento de keepalive en el nivel de DSN que elija. Puede hacerlo añadiendo o modificando los siguientes parámetros en el archivo `odbc.ini`:

KeepAlivesCount

La cantidad de paquetes keepalive de TCP que se pueden perder antes de que se considere que se interrumpió la conexión.

KeepAlivesIdle

La cantidad de segundos de inactividad antes de que el controlador envíe un paquete keepalive de TCP.

KeepAlivesInterval

La cantidad de segundos entre cada retransmisión de keepalive de TCP.

En Windows, modifique estos parámetros en el Registro añadiendo o modificando las claves de HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\su_DSN. En Linux y Mac OS, agregue o modifique estos parámetros en la entrada del DSN destino directamente en el archivo odbc.ini. Para obtener más información acerca de cómo modificar el archivo odbc.ini en equipos Linux y Mac OS, consulte [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X \(p. 144\)](#).

Si estos parámetros no existen o si tienen un valor 0, el sistema usará los parámetros keepalive especificados para TCP/IP a fin de determinar el comportamiento keepalive del DSN. En Windows, puede encontrar los parámetros TCP/IP en el registro en HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\. En Linux y Mac OS, puede encontrar los parámetros de TCP/IP en el archivo sysctl.conf.

La conexión devuelve un error o se rechaza

Ejemplos de errores

- "No se pudo establecer conexión con `<endpoint>`".
- «No se ha podido establecer una conexión con el servidor: El tiempo de espera de la conexión. ¿El servidor se está ejecutando en el host '`<endpoint>`' y acepta conexiones TCP/IP en el puerto '`<port>`'?»
- "Conexión rechazada. Compruebe que el nombre de host y el puerto sean los correctos y que el administrador de correo acepte conexiones TCP/IP".

Posibles soluciones:

Por lo general, cuando recibe un mensaje de error que le indica que hay un error para establecer una conexión, se trata de un error con el permiso para obtener acceso al clúster.

Para conectarse al clúster desde una herramienta de cliente fuera de la red en la que se encuentra el clúster, añada una regla de entrada. Añada la regla en el grupo de seguridad del clúster para el CIDR/IP desde el que se está conectando:

- Si creó su clúster de Amazon Redshift en una nube privada virtual (VPC) basada en Amazon VPC, añada su dirección CIDR/IP de cliente al grupo de seguridad de VPC en Amazon VPC. Para obtener más información acerca de cómo configurar los grupos de seguridad de VPC para su clúster, consulte [Administración de clústeres en una VPC \(p. 75\)](#).
- Si creó su clúster de Amazon Redshift fuera de una VPC, añada su dirección CIDR/IP de cliente al grupo de seguridad del clúster en Amazon Redshift. Para obtener más información acerca de cómo configurar los grupos de seguridad del clúster, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#).

Si intenta conectarse al clúster desde una herramienta de cliente en una instancia de Amazon EC2, también debe añadir una regla de entrada. En este caso, añada la regla al grupo de seguridad del clúster para el grupo de seguridad de Amazon EC2 asociado con la instancia de Amazon EC2. Para obtener más información acerca de cómo configurar los grupos de seguridad del clúster, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#).

En algunos casos, es posible que tenga una capa entre el cliente y el servidor, como un firewall. En estos casos, asegúrese de que el firewall acepte conexiones entrantes a través del puerto que configuró para el clúster.

El cliente y el controlador son incompatibles

Ejemplo de error

"El DSN especificado presenta una incompatibilidad de arquitectura entre el controlador y la aplicación".

Posible solución

Cuando intenta conectarse y obtiene un error sobre una discordancia de arquitectura, esto significa que la herramienta cliente y el controlador no son compatibles. Esto ocurre porque su arquitectura del sistema no coincide. Por ejemplo, esto puede ocurrir si tiene una herramienta de cliente de 32 bits, pero tiene instalada la versión de 64 bits del controlador. Algunas veces, las herramientas de cliente de 64 bits pueden usar controladores de 32 bits, pero no puede usar aplicaciones de 32 bits con controladores de 64 bits. Asegúrese de que el controlador y la herramienta de cliente estén usando la misma versión de arquitectura de sistema.

Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster

Problema de ejemplo

Tiene un problema con la finalización de las consultas. Aparentemente, las consultas se están ejecutando pero dejan de responder en la herramienta de cliente SQL. Algunas veces, las consultas no aparecen en el clúster, como en las tablas del sistema o en la consola de Amazon Redshift.

Posible solución

Este problema puede ocurrir debido a la pérdida de paquetes. En este caso, hay una diferencia en el tamaño máximo de la unidad de transmisión (MTU) en la ruta de red entre dos hosts de Internet Protocol (IP). El tamaño de la MTU determina el tamaño máximo, en bytes, de un paquete que puede ser transferido en una trama Ethernet desde una conexión de red. En AWS, algunos tipos de instancia de Amazon EC2 admiten una MTU de 1500 (tramas Ethernet v2) y otros tipos de instancia admiten una MTU de 9001 (tramas gigantes TCP/IP).

Para evitar problemas relacionados con las diferencias en tamaños de la MTU, recomendamos realizar alguna de las siguientes operaciones:

- Si el clúster utiliza la plataforma EC2-VPC, configure el grupo de seguridad de Amazon VPC con una regla de entrada personalizada del Protocolo de mensajes de control de Internet (ICMP) que devuelva `Destination Unreachable`. Por lo tanto, la regla indica al host de origen que utilice el tamaño mínimo de MTU a lo largo de la ruta de red. Para obtener más información acerca de este método, consulte [Configuración de los grupos de seguridad para permitir el ICMP "Destination Unreachable"](#) (p. 173).
- Si el clúster usa la plataforma EC2-Classic o si no puede permitir la regla entrante de ICMP, deshabilite las tramas gigantes TCP/IP para que se usen las tramas Ethernet v2. Para obtener más información acerca de este método, consulte [Configuración de la MTU de una instancia](#) (p. 174).

Configuración de los grupos de seguridad para permitir el ICMP "Destination Unreachable"

Cuando haya una diferencia en el tamaño de la MTU en la red entre los dos hosts, primero asegúrese de que su configuración de red no bloquee la detección de la MTU de la ruta (PMTUD). La PMTUD permite que el host receptor responda al host origen con el siguiente mensaje de ICMP: `Destination Unreachable: fragmentation needed and DF set` (ICMP Type 3, Code 4). Este mensaje le indica al host origen que use el mínimo tamaño de la MTU en la ruta de la red para volver a enviar la solicitud. Sin esta negociación, puede perderse el paquete porque la solicitud es muy grande para que la

acepte el host receptor. Para obtener más información acerca de este mensaje de ICMP, consulte [RFC792](#) en el sitio web Internet Engineering Task Force (IETF).

Si no configura de forma explícita esta regla entrante de ICMP para su grupo de seguridad de Amazon VPC, se bloquea la PMTUD. En AWS, los grupos de seguridad son como un firewall virtual que especifican reglas para controlar el tráfico entrante y saliente de una instancia. Para obtener información acerca del grupo de seguridad del clúster de Amazon Redshift, consulte [Grupos de seguridad de clúster de Amazon Redshift \(p. 390\)](#). Para los clústeres que usa la plataforma EC2-VPC, Amazon Redshift usa grupos de seguridad de Virtual Cloud (VPC, Virtual privada) para permitir o rechazar el tráfico al clúster. De manera predeterminada, los grupos de seguridad están bloqueados y rechazan el tráfico entrante. Para obtener información acerca de cómo configurar reglas de entrada y salida para instancias EC2-Classic o EC2-VPC, consulte [Diferencias entre las instancias de EC2-Classic y VPC](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Para obtener más información acerca de cómo añadir reglas a los grupos de seguridad de VPC, consulte [Administración de grupos de seguridad de VPC para un clúster \(p. 79\)](#). Para obtener más información acerca de la configuración específica de PMTUD que se requiere en esta regla, consulte [Detección de MTU de ruta](#) en la Guía del usuario de Amazon EC2 para instancias de Linux.

Configuración de la MTU de una instancia

En algunos casos, el clúster puede usar la plataforma EC2-Classic o no puede permitir la regla ICMP personalizada para el tráfico entrante. En estos casos, se recomienda ajustar la MTU a 1500 en la interfaz de red (NIC) de las instancias EC2 desde las que se conecta al clúster de Amazon Redshift. Este ajuste deshabilita las tramas gigantes TCP/IP para garantizar que las conexiones usen siempre el mismo tamaño de paquete. Sin embargo, esta opción reduce el rendimiento máximo de su red para toda la instancia, no solo para las conexiones a Amazon Redshift. Para obtener más información, consulte los siguientes procedimientos.

Pasos para configurar la MTU en un sistema operativo Microsoft Windows

Si su cliente se ejecuta en un sistema operativo Microsoft Windows, puede revisar y configurar el valor de la MTU para el adaptador Ethernet usando el comando `netsh`.

1. Ejecute el siguiente comando para determinar el valor actual de la MTU:

```
netsh interface ipv4 show subinterfaces
```

2. Revise el valor de MTU para el adaptador Ethernet en la salida.
3. Si el valor no es 1500, ejecute el siguiente comando para verlo:

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500 store=persistent
```

Después de configurar este valor, reinicie su equipo para que se apliquen los cambios.

Pasos para configurar la MTU en un sistema operativo Linux

Si su cliente se ejecuta en un sistema operativo Linux, puede revisar y configurar el valor de la MTU usando el comando `ip`.

1. Ejecute el siguiente comando para determinar el valor actual de la MTU:

```
$ ip link show eth0
```

2. Revise el valor posterior a `mtu` en la salida.
3. Si el valor no es 1500, ejecute el siguiente comando para verlo:

```
$ sudo ip link set dev eth0 mtu 1500
```

Pasos para configurar la MTU en un sistema operativo Mac

- Sigue las instrucciones del sitio de soporte técnico de macOS sobre [How to change the MTU for troubleshooting purposes](#). Para obtener más información, busque el [sitio de soporte](#).

Uso de la API de datos de Amazon Redshift

Puede acceder a su base de datos de Amazon Redshift mediante la API de datos integrada de Amazon Redshift. Mediante esta API, puede obtener acceso a los datos de Amazon Redshift con aplicaciones basadas en servicios web, como AWS Lambda, los portátiles de Amazon SageMaker y AWS Cloud9. Para obtener más información sobre estas aplicaciones, consulte [AWS Lambda](#), [Amazon SageMaker](#), y [AWS Cloud9](#).

La API de datos no requiere una conexión persistente al clúster. En su lugar, proporciona un punto de enlace HTTP seguro e integración con los AWS SDK. Puede usar el punto de enlace para ejecutar instrucciones SQL sin administrar conexiones. Las llamadas a la API de datos son asíncronas.

La API de datos utiliza las credenciales almacenadas en AWS Secrets Manager o credenciales temporales de base de datos. No necesita pasar contraseñas en las llamadas a la API con ninguno de los métodos de autorización. Para obtener más información acerca de AWS Secrets Manager, consulte [Qué es AWS Secrets Manager?](#) en la [AWS Secrets Manager Guía del usuario](#).

Para obtener más información sobre las operaciones de API de datos, consulte la [Referencia a la API de datos de Amazon Redshift](#).

Uso de la API de datos de Amazon Redshift

Antes de utilizar la API de datos de Amazon Redshift, revise los siguientes pasos:

1. Determine si usted, como autor de la llamada de la API de datos, está autorizado. Para obtener más información acerca de la autorización, consulte [Autorización del acceso a la API de datos de Amazon Redshift \(p. 175\)](#).
2. Determine si planea llamar a la API de datos con credenciales de autenticación desde Secrets Manager o credenciales temporales. Para obtener más información, consulte [Elegir credenciales de autenticación al llamar a la API de datos de Amazon Redshift \(p. 179\)](#).
3. Configure un secreto si utiliza el Secrets Manager para las credenciales de autenticación. Para obtener más información, consulte [Almacenamiento de credenciales de base de datos en AWS Secrets Manager \(p. 177\)](#).
4. Revise las consideraciones y limitaciones al llamar a la API de datos. Para obtener más información, consulte [Consideraciones al llamar a la API de datos de Amazon Redshift \(p. 179\)](#).
5. Llamadas a la API de datos desde la AWS Command Line Interface (AWS CLI), desde su propio código o utilizando el editor de consultas de la consola de Amazon Redshift. Para ver ejemplos de llamadas desde la AWS CLI, consulte [Llamadas a la API de datos con la AWS CLI \(p. 181\)](#).

Autorización del acceso a la API de datos de Amazon Redshift

Para obtener acceso a la API de datos, un usuario debe estar autorizado. Puede autorizar a un usuario a obtener acceso a la API de datos, añadiendo una política administrada, que es una [AWS Identity and](#)

Access Management(IAM), a ese usuario. Para ver los permisos permitidos y denegados por las directivas administradas, consulte la consola de IAM (<https://console.aws.amazon.com/iam/>).

Amazon Redshift proporciona el `AmazonRedshiftDataFullAccess` política administrada. Esta política proporciona acceso completo a las operaciones de la API de datos de Amazon Redshift. Esta política también permite el acceso con ámbito a Amazon Redshift específico, AWS Secrets Managery las operaciones de API de IAM necesarias para autenticar y acceder a un clúster de Amazon Redshift. Si usa AWS Secrets Manager para autenticar, la política permite el uso de `secretsmanager:GetSecretValue` acción para recuperar el secreto etiquetado con la clave `RedshiftDataFullAccess`. Si utiliza credenciales temporales para autenticarse, la directiva permite el uso de `redshift:GetClusterCredentials` Para el nombre de usuario de la base de datos `redshift_data_api_user` para cualquier base de datos del clúster. Este nombre de usuario ya se tiene que haber creado en la base de datos.

También puede crear su propia política de IAM que le permita obtener acceso a recursos específicos. Para crear su política, utilice el `AmazonRedshiftDataFullAccess` como plantilla de inicio. Tras crear la política, añádala a todos los usuarios que tengan que obtener acceso a la API de datos.

Para ejecutar una consulta en un clúster propiedad de otra cuenta, la cuenta propietaria debe proporcionar un rol de IAM que la API de datos puede asumir en la cuenta que llama. Por ejemplo, supongamos que la cuenta B posee un clúster al que la cuenta A necesita tener acceso. La cuenta B puede adjuntar la directiva administrada por `AWSAmazonRedshiftDataFullAccess` a la función de IAM de la Cuenta B. A continuación, la cuenta B confía en la cuenta A mediante una política de confianza como la siguiente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::accountID-of-account-A:role/someRoleA"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Por último, el rol de IAM de cuenta A debe poder asumir el rol de IAM de cuenta B.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::accountID-of-account-B:role/someRoleB"
  }
}
```

En los siguientes enlaces se ofrece más información acerca de AWS Identity and Access Management en la Guía del usuario de IAM.

- Para obtener información sobre la creación de un rol de IAM, consulte [Creación de roles de IAM](#).
- Para obtener información sobre la creación de una política de IAM, consulte [Creación de directivas de IAM](#).
- Para obtener información sobre cómo añadir una política de IAM a un usuario, consulte [Agregar y eliminar permisos de identidad de IAM](#).

Almacenamiento de credenciales de base de datos en AWS Secrets Manager

Al llamar a la API de datos, puede transferir las credenciales del clúster mediante un secreto en AWS Secrets Manager. Para pasar credenciales mediante este método, especifique el nombre del secreto o el Nombre de recurso de Amazon (ARN) del secreto.

Para almacenar credenciales con Secrets Manager, necesita `SecretManagerReadWrite` permiso de directiva administrada. Para obtener más información sobre los permisos mínimos de, consulte [Creación y administración de secretos con AWS Secrets Manager](#) en la AWS Secrets Manager Guía del usuario.

Para almacenar sus credenciales en secreto para un clúster de Amazon Redshift

1. Usar AWS Secrets Manager Para crear un secreto que contenga credenciales para el clúster de:

- Cuando elige Almacenar un nuevo secreto, elija Credenciales para el clúster de Redshift.
- Almacene sus valores para User name (Nombre de usuario):(usuario de la base de datos), Contraseña, y Clúster de base de datos (identificador de clúster) en su secreto.
- Etiquetar el secreto con la clave `RedshiftDataFullAccess`. La política administrada de `AWSAmazonRedshiftDataFullAccess` solo permite la acción `secretsmanager:GetSecretValue` para los secretos etiquetados con la clave `RedshiftDataFullAccess`.

Para obtener instrucciones, consulte [Creación de un secreto básico](#) en la AWS Secrets Manager Guía del usuario.

2. Utilice la consola de AWS Secrets Manager para ver los detalles del secreto que ha creado, o ejecute el comando de la AWS CLI `aws secretsmanager describe-secret`.

Anote el nombre y el ARN del secreto. Puede utilizarlos en llamadas a la API de datos.

Creación de un punto de enlace de Amazon VPC (AWS PrivateLink) para la API de datos

Amazon Virtual Private Cloud (Amazon VPC) le permite lanzar AWS Recursos de, como clústeres y aplicaciones de Amazon Redshift, en una nube virtual privada (VPC). AWS PrivateLink proporciona conectividad privada entre Amazon VPC y AWS de forma segura en la red de Amazon. Uso AWS PrivateLink , puede crear puntos de enlace de Amazon VPC, que le permiten conectarse a servicios a través de diferentes cuentas y VPC basados en Amazon VPC. Para obtener más información acerca de AWS PrivateLink , consulte [Servicios de punto de enlace de la VPC \(AWS PrivateLink \)](#) en la Guía del usuario de Amazon Virtual Private Cloud.

Puede llamar a la API de datos con los puntos de enlace de la Amazon VPC. El uso de un endpoint de Amazon VPC mantiene el tráfico entre las aplicaciones de su Amazon VPC y la API de datos en el AWS, sin usar direcciones IP públicas. Los puntos de enlace de Amazon VPC pueden ayudarle a cumplir los requisitos reglamentarios y de conformidad relacionados con la limitación de la conectividad a Internet público. Por ejemplo, si utiliza un punto de enlace de la Amazon VPC, puede mantener el tráfico entre una aplicación que se ejecuta en una instancia Amazon EC2 y la API de datos en las VPC donde se contienen.

Después de crear el punto de enlace de la Amazon VPC, puede comenzar a usarlo sin realizar ningún cambio de código o configuración en la aplicación.

Para crear un punto de enlace de la Amazon VPC para la API de datos

1. Inicie sesión en AWS Management Console y abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. Elija Endpoints (Puntos de enlace) y, a continuación, elija Create Endpoint (Crear punto de enlace).
3. En la página Create Endpoint (Crear punto de enlace), en Service category (Categoría de servicio), elija AWS services (Servicios de AWS). Para Nombre del servicio, elija `redshift-data.com.amazonaws.region.redshift-data`.
4. Para VPC, elija la VPC en la que crear el punto de enlace.

Elija la VPC que contiene la aplicación que realiza llamadas a la API de datos.

5. En Subnets (Subredes), elija la subred para cada zona de disponibilidad (AZ) utilizada por el servicio de AWS que ejecuta la aplicación.

Para crear un punto de enlace de Amazon VPC, especifique el rango de direcciones IP privadas en el que se puede acceder al punto de enlace. Para ello, elija la subred para cada zona de disponibilidad. Al hacerlo, se restringe el punto de enlace de la VPC al rango de direcciones IP privadas específico de cada zona de disponibilidad y también se crea un punto de enlace de la Amazon VPC en cada zona de disponibilidad.

6. En Enable Private DNS Name (Habilitar nombre de DNS privado), seleccione Enable for this endpoint (Habilitar para este punto de enlace).

El DNS privado resuelve el nombre de host de DNS de la API de datos estándar (`https://redshift-data.region.amazonaws.com`) en las direcciones IP privadas asociadas con el nombre de host de DNS específico del punto de enlace de la Amazon VPC. Como resultado, puede acceder al punto de enlace de la VPC de la API de datos utilizando los SDK de AWS CLI o la AWS sin realizar ningún cambio de código o configuración para actualizar la URL del punto de enlace de la API de datos.

7. En Security group (Grupo de seguridad), elija los grupos de seguridad que deban asociarse al punto de enlace de la Amazon VPC.

Elija el grupo de seguridad que permita el acceso al servicio de AWS que ejecuta la aplicación. Por ejemplo, si una instancia Amazon EC2 está ejecutando la aplicación, elija el grupo de seguridad que permita el acceso a la instancia Amazon EC2. El grupo de seguridad le permite controlar el tráfico al punto de enlace de la Amazon VPC desde los recursos de la VPC.

8. Elija Create endpoint.

Una vez creado el punto de enlace, elija el vínculo en la AWS Management Console para ver los detalles del punto de enlace.

La ficha Details (Detalles) del punto de enlace muestra los nombres de host de DNS que se generaron al crear el punto de enlace de la Amazon VPC.

Puede utilizar el punto de enlace estándar (`redshift-data.region.amazonaws.com`) o uno de los puntos de enlace específicos de la VPC para llamar a la API de datos dentro de la Amazon VPC. El punto de enlace de la API de datos estándar se dirige automáticamente al punto de enlace de la Amazon VPC. Este enrutamiento se produce porque cuando se creó el punto de enlace de la Amazon VPC se habilitó el nombre de host de DNS privado.

Cuando utiliza un punto de enlace de la Amazon VPC en una llamada a la API de datos, todo el tráfico entre la aplicación y la API de datos permanece en las Amazon VPC donde se contienen. Puede usar un punto de enlace de la Amazon VPC para cualquier tipo de llamada a la API de datos. Para obtener más información sobre la llamada a la API de datos, consulte [Consideraciones al llamar a la API de datos de Amazon Redshift \(p. 179\)](#).

Consideraciones al llamar a la API de datos de Amazon Redshift

Tenga en cuenta lo siguiente al llamar a la API de datos:

- La duración máxima de una consulta es de 24 horas.
- El número máximo de consultas activas (`STARTED`/`SUBMITTED` consultas) por clúster de Amazon Redshift es 200.
- El tamaño máximo de resultado de la consulta es de 100 MB. Si una llamada devuelve más de 100 MB de datos de respuesta, se terminará la llamada.
- El tiempo máximo de retención para los resultados de la consulta es de 24 horas.
- El tamaño máximo de instrucción de consulta es de 100 KB.
- La API de datos está disponible para consultar clústeres de un solo nodo y de varios nodos de los siguientes tipos de nodo:
 - `dc2.large`
 - `dc2.8xlarge`
 - `ds2.xlarge`
 - `ds2.8xlarge`
 - `ra3.xlplus`
 - `ra3.4xlarge`
 - `ra3.16xlarge`
- El clúster debe estar en una nube virtual privada (VPC) basada en el servicio de Amazon VPC.
- De forma predeterminada, los usuarios con el mismo rol de IAM o usuario de IAM que el corredor de un `ExecuteStatement` La operación de la API puede actuar en la misma instrucción con `CancelStatement`, `DescribeStatement`, `GetStatementResult`, y `ListStatements` Operaciones de la API.
- Para obtener una lista de `AWS` Regiones donde la API de datos está disponible, consulte [Puntos de enlace de la API de datos Redshift](#) en la Referencia general de Amazon Web Services.

Elegir credenciales de autenticación al llamar a la API de datos de Amazon Redshift

Cuando se llama a la API de datos, se utiliza uno de los siguientes métodos de autenticación para algunas operaciones de API. Cada método requiere una combinación diferente de parámetros.

AWS Secrets Manager

Con este método, proporcione el `secret-arn` valor secreto que se almacena en AWS Secrets Manager. El secreto especificado contiene credenciales para conectarse a la base de datos. También proporciona un valor para `cluster-identifier` que coincida con el identificador del clúster en el secreto.

Credenciales temporales

Con este método, proporcione su `cluster-identifier`, `database`, y `ydb-user` Valores.

Con cualquiera de los métodos, también puede proporcionar un `region` que especifica el valor `AWS` Región en la que se encuentra el clúster de.

Asignación de tipos de datos JDBC al llamar a la API de datos de Amazon Redshift

En la tabla siguiente se mapean los tipos de datos de Java Database Connectivity (JDBC) con los tipos de datos que especifica en las llamadas a la API de datos.

Tipo de datos JDBC	Tipo de datos de la API de datos
INTEGER, TINYINT, SMALLINT, BIGINT	LONG
FLOAT, REAL, DOUBLE	DOUBLE
DECIMAL	STRING
BOOLEAN, BIT	BOOLEAN
BLOB, BINARY, LONGVARBINARY, VARBINARY	BLOB
CLOB	STRING
Otros tipos (incluidos los tipos relacionados con la fecha y hora)	STRING

Los valores de cadena se pasan a la base de datos de Amazon Redshift y se convierten implícitamente en un tipo de datos de base de datos.

Note

Actualmente, la API de datos no admite matrices de identificadores únicos universales (UUID).

Ejecución de sentencias SQL con parámetros al llamar a la API de datos de Amazon Redshift

Puede controlar el texto SQL enviado al motor de base de datos llamando a la operación API de datos utilizando parámetros para partes de la instrucción SQL. Los parámetros con nombre proporcionan una forma flexible de pasar parámetros sin codificarlos en el texto SQL. Le ayudan a reutilizar texto SQL y a evitar problemas de inyección SQL.

En el siguiente ejemplo se muestran los parámetros con nombre de `unparametersfield` de `unexecute statement`.

```
--parameters [{"name": "id", "value": "1"}, {"name": "address", "value": "Seattle"}]
```

Tenga en cuenta lo siguiente al usar parámetros con nombre asignado:

- Los parámetros con nombre pueden estar en cualquier orden y los parámetros se pueden usar más de una vez en el texto SQL. La opción de parámetros mostrada en el ejemplo anterior, los valores `1` y `Seattle` se insertan en las columnas de la tabla `id` y `address`. En el texto SQL, especifique los parámetros con nombre de la siguiente manera:

```
--sql "insert into mytable values (:id, :address)"
```

- Cuando se ejecuta el SQL, los datos se convierten implícitamente en un tipo de datos. Para obtener más información sobre la conversión de tipos de datos, consulte [Tipos de datos](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

- No se puede establecer un valor en NULL. La API de datos lo interpreta como la cadena literalNULL. En el ejemplo siguiente se reemplaza idLa cadena literalnull. No es el valor NULL de SQL.

```
--parameters "[{\"name\": \"id\", \"value\": \"null\"}]"
```

- No se puede establecer un valor de longitud cero. Error en la instrucción SQL de la API de datos. En el siguiente ejemplo se intenta establecer idcon un valor de longitud cero y da como resultado un error de la instrucción SQL.

```
--parameters "[{\"name\": \"id\", \"value\": \"\"}]"
```

- No se puede establecer un nombre de tabla en la instrucción SQL con un parámetro. La API de datos sigue la regla del JDBCPreparedStatement.
- La salida de la describe statementdevuelve los parámetros de consulta de una instrucción SQL.

Llamadas a la API de datos

Puede llamar a la API de datos o alAWS CLIpara ejecutar instrucciones SQL en el clúster de. La operación principal para ejecutar una instrucción SQL es[ExecuteStatement](#). La API de los datos admite los idiomas de programación compatibles con elAWSSDK. Para obtener más información al respecto, consulte[Herramientas para construirAWS](#).

Llamadas a la API de datos con la AWS CLI

Puede llamar a la API de datos utilizando la AWS CLI.

Los siguientes ejemplos utilizan lasAWS CLIpara llamar a la API de datos. Para ejecutar los ejemplos, edite los valores de los parámetros para que coincidan con su entorno. Estos ejemplos demuestran algunas de las operaciones de Data API. Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

Los comandos de los siguientes ejemplos se han dividido y formateado para mayor legibilidad.

Para ejecutar una instrucción SQL

Para ejecutar una instrucción SQL, utilice el comandoaws redshift-data execute-statement AWS CLIcommand.

Los siguientes ejemplos deAWS CLIejecuta una instrucción SQL y devuelve un identificador para obtener los resultados. En este ejemplo se utiliza elAWS Secrets ManagerMétodo de autenticación.

```
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
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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"
}
```

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL y devuelve un identificador para obtener los resultados. En este ejemplo se utiliza el método de autenticación de credenciales temporales.

```
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"
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "ClusterIdentifier": "mycluster-test",
  "CreatedAt": 1598306924.632,
  "Database": "dev",
  "DbUser": "myuser",
  "Id": "d9b6c0c9-0747-4bf4-b142-e8883122f766"
}
```

Para ejecutar una instrucción SQL con parámetros

Para ejecutar una instrucción SQL, utilice el comando `aws redshift-data execute-statement` AWS CLI command.

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL y devuelve un identificador para obtener los resultados. En este ejemplo se utiliza el AWS Secrets Manager Método de autenticación. El texto SQL tiene parámetros con nombre `colname` y `distance`. En este caso, el nombre de la columna de la tabla es `ratecode` y la distancia utilizada en el predicado es 5. Los valores de los parámetros con nombre asignado para la instrucción SQL se especifican en el cuadro de diálogo `parameters` opción.

```
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 :colname, COUNT(*) FROM demo_table WHERE trip_distance > :distance"
--parameters "[{\"name\": \"colname\", \"value\": \"ratecode\"}, {\"name\":
\"distance\", \"value\": \"5\"}]"
--database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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"
}
```

En el siguiente ejemplo se utiliza el `EVENT` de la base de datos de ejemplo. Para obtener más información, consulte [Tabla EVENT](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Si aún no tiene `event` en la base de datos, puede crear una usando la API de datos de la siguiente manera:

```
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)"
```

El siguiente comando inserta una fila en `event`Tabla de.

```
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\"}]"
```

El siguiente comando inserta una segunda fila en `event`Tabla de. Este ejemplo hace lo siguiente:

- El parámetro denominado `id` se utiliza cuatro veces en el texto SQL.
- La conversión de tipo implícita se aplica automáticamente al insertar parámetro `starttime`.
- La `venueid` es tipo de conversión al tipo de datos `SMALLINT`.
- Las cadenas de caracteres que representan el tipo de datos `DATE` se convierten implícitamente en el tipo de datos `TIMESTAMP`.
- Los comentarios se pueden usar dentro del texto SQL.

```
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\"}]"
```

A continuación se muestran las dos filas insertadas:

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

El siguiente comando utiliza un parámetro con nombre en una cláusula WHERE para recuperar la fila donde eventid es 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\"}]"
```

Ejecute el siguiente comando para obtener los resultados SQL de la instrucción SQL anterior:

```
aws redshift-data get-statement-result --id 7529ad05-b905-4d71-9ec6-8b333836eb5a
```

Proporciona los siguientes resultados:

```
{
  "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
}
```

Para enumerar metadatos acerca de las sentencias SQL

Para enumerar los metadatos acerca de las sentencias SQL, utilice la herramienta `aws redshift-data list-statements` AWS CLI command. La autorización para ejecutar este comando se basa en los permisos de IAM del autor de la llamada.

Los siguientes ejemplos de `AWS CLI` enumeran las sentencias SQL que se ejecutaron.

```
aws redshift-data list-statements
--region us-west-2
--status ALL
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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
    }
  ]
}
```

Para describir metadatos acerca de una instrucción SQL

Para obtener descripciones de los metadatos de una instrucción SQL, utilice la herramienta `aws redshift-data describe-statement` AWS CLI command. La autorización para ejecutar este comando se basa en los permisos de IAM del autor de la llamada.

Los siguientes ejemplos de AWS CLI: describe una instrucción SQL.

```
aws redshift-data describe-statement
--id d9b6c0c9-0747-4bf4-b142-e8883122f766
--region us-west-2
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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
}
```

Para obtener los resultados de una instrucción SQL

Para obtener el resultado de una instrucción SQL que se ejecutó, utilice el método `redshift-data get-statement-result` AWS CLI command. La autorización para ejecutar este comando se basa en los permisos de IAM del autor de la llamada.

```
aws redshift-data get-statement-result
--id d9b6c0c9-0747-4bf4-b142-e8883122f766
--region us-west-2
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "ColumnMetadata": [
    {
      "isCaseSensitive": false,
      "isCurrency": false,
      "isSigned": true,
      "label": "userid",
      "length": 0,
      "name": "userid",
      "nullable": 0,
      "precision": 10,
      "scale": 0,
      "schemaName": "",
      "tableName": "stl_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": "stll_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
}
```

Para describir una tabla

Para obtener metadatos que describen una tabla, utilice la herramienta `aws redshift-data describe-table` AWS CLI command.

Los siguientes ejemplos de `AWS CLI` ejecuta una instrucción SQL y devuelve metadatos que describen una tabla. En este ejemplo se utiliza el `AWS Secrets Manager` Método de autenticación.

```
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
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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"
    }
]
}
```

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL que describe una tabla. En este ejemplo se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data describe-table
--region us-west-2
--db-user myuser
--cluster-identifier mycluster-test
--database dev
--schema information_schema
--table sql_features
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "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"  
    }  
]  
}
```

Para mostrar las bases de datos de un clúster

Para enumerar las bases de datos de un clúster, utilice la herramienta `aws redshift-data list-databases` AWS CLI command.

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL para enumerar las bases de datos. En este ejemplo se utiliza el AWS Secrets Manager Método de autenticación.

```
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
```

A continuación se muestra un ejemplo de respuesta.

```
{  
  "Databases": [  
    "dev"  
  ]  
}
```

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL para enumerar las bases de datos. En este ejemplo se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-databases  
--region us-west-2  
--db-user myuser  
--cluster-identifier mycluster-test  
--database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{  
  "Databases": [  
    "dev"  
  ]  
}
```

Para enumerar los esquemas de una base de datos

Para enumerar los esquemas de una base de datos, utilice la herramienta `aws redshift-data list-schemas` AWS CLI command.

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL para enumerar esquemas en una base de datos. En este ejemplo se utiliza el AWS Secrets Manager Método de autenticación.

```
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
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

Los siguientes ejemplos deAWS CLLejecuta una instrucción SQL para enumerar esquemas en una base de datos. En este ejemplo se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-schemas
--region us-west-2
--db-user mysuser
--cluster-identifier mycluster-test
--database dev
```

A continuación se muestra un ejemplo de respuesta.

```
{
  "Schemas": [
    "information_schema",
    "pg_catalog",
    "pg_internal",
    "public"
  ]
}
```

Para mostrar las tablas de una base de datos

Para enumerar las tablas de una base de datos, utilice la herramientaaws redshift-data list-tables AWS CLIcommand.

Los siguientes ejemplos deAWS CLLejecuta una instrucción SQL para enumerar tablas en una base de datos. En este ejemplo se utiliza elAWS Secrets ManagerMétodo de autenticación.

```
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
```

A continuación se muestra un ejemplo de respuesta.

```
{
```

```
"Tables": [  
  {  
    "name": "sql_features",  
    "schema": "information_schema",  
    "type": "SYSTEM TABLE"  
  },  
  {  
    "name": "sql_implementation_info",  
    "schema": "information_schema",  
    "type": "SYSTEM TABLE"  
  }  
]
```

Los siguientes ejemplos de AWS CLI ejecuta una instrucción SQL para enumerar tablas en una base de datos. En este ejemplo se utiliza el método de autenticación de credenciales temporales.

```
aws redshift-data list-tables  
  --region us-west-2  
  --db-user myuser  
  --cluster-identifier mycluster-test  
  --database dev  
  --schema information_schema
```

A continuación se muestra un ejemplo de respuesta.

```
{  
  "Tables": [  
    {  
      "name": "sql_features",  
      "schema": "information_schema",  
      "type": "SYSTEM TABLE"  
    },  
    {  
      "name": "sql_implementation_info",  
      "schema": "information_schema",  
      "type": "SYSTEM TABLE"  
    }  
  ]  
}
```

Solución de problemas de la API de datos de Amazon Redshift

Use las siguientes secciones, tituladas con mensajes de error comunes, para ayudar a solucionar problemas que tenga con la API de datos.

Temas

- [El paquete de la consulta es demasiado grande \(p. 196\)](#)
- [Límite de tamaño superado de respuesta de base de datos \(p. 197\)](#)

El paquete de la consulta es demasiado grande

Si aparece un error que indica que el paquete de una consulta es demasiado grande, generalmente el conjunto de resultados devuelto para una fila es demasiado grande. El límite de tamaño de la API de datos es 64 KB por fila en el conjunto de resultados devuelto por la base de datos.

Para solventar este problema, asegúrese de que cada fila de un conjunto de resultados sea de 64 KB o menos.

Límite de tamaño superado de respuesta de base de datos

Si aparece un error que indica que la respuesta de la base de datos ha excedido el límite de tamaño, generalmente el tamaño del conjunto de resultados devuelto por la base de datos era demasiado grande. El límite de la API de datos es 100 MB en el conjunto de resultados devuelto por la base de datos.

Para resolver este problema, asegúrese de que las llamadas a la API de datos devuelvan 100 MB o menos. Si necesita devolver más de 100 MB, puede ejecutar varias llamadas a las instrucciones con el método `LIMIT` en su consulta.

Programación de las operaciones de la API de datos de Amazon Redshift con Amazon EventBridge

Amazon EventBridge le ayuda a responder a los cambios de estado de su AWS de AWS. Cuando cambia el estado de los recursos, estos envían automáticamente eventos a un flujo de eventos. Los eventos se envían a la cuenta que contiene la base de datos de Amazon Redshift. Puede crear reglas que coincidan con los eventos seleccionados en el flujo y los transfieran a destinos de para realizar alguna acción. También puede usar las reglas de para realizar alguna acción en una programación predeterminada. Para obtener más información, consulte la [guía del usuario de Amazon EventBridge](#).

Para programar operaciones de API de datos con EventBridge, el rol de IAM asociado debe confiar en el principal para CloudWatch Events (events.amazonaws.com). Este rol debe tener el equivalente de la directiva administrada `AmazonEventBridgeFullAccess` adjunto. También debería tener `AmazonRedshiftDataFullAccess` que son administrados por la API de datos. Puede crear un rol de IAM con estos permisos en la consola de IAM. Al crear un rol en la consola de IAM, elija la AWS entidad de confianza para CloudWatch Events. Para obtener más información sobre la creación de un rol de IAM, consulte [Creación de un rol para un AWS Servicio \(Consola\)](#) en la Guía del usuario de IAM.

En el siguiente ejemplo se utiliza la AWS CLI para crear una regla de EventBridge que se utiliza para ejecutar una instrucción SQL.

```
aws events put-rule
--name test-redshift-data
--schedule-expression "rate(1 minute)"
```

A continuación, se crea un destino de EventBridge para que se ejecute según la programación especificada en la regla.

```
aws events put-targets
--cli-input-json file://data.json
```

El archivo `data.json` de entrada es el siguiente.

```
{
  "Rule": "test-redshift-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-scheduler-statement",
        "WithEvent": true
    }
}
]
```

Supervisión de la API de datos

El monitoreo es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el desempeño de la API de datos y sus demás AWS Soluciones. AWS proporciona las siguientes herramientas de monitorización para controlar la API de datos, informar cuando algo no funciona y realizar acciones automáticas cuando proceda:

- Amazon EventBridge se puede utilizar para automatizar sus AWS Servicios de y responder automáticamente a eventos del sistema, como problemas de disponibilidad de aplicaciones o cambios de recursos. Eventos de AWS Los servicios de EventBridge se envían a casi en tiempo real. Puede crear reglas sencillas para indicar qué eventos le resultan de interés, así como qué acciones automatizadas se van a realizar cuando un evento cumple una de las reglas. Para obtener más información, consulte la [guía del usuario de Amazon EventBridge](#).
- AWS CloudTrail captura llamadas a la API de y los eventos relacionados realizados por su nombre o por su nombre AWS y entrega los archivos log al bucket de Amazon S3 que especifique. También pueden identificar qué usuarios y cuentas llamaron a AWS, la dirección IP de origen desde la que se realizaron las llamadas y el momento en que se efectuaron las llamadas. Para obtener más información, consulte la [AWS CloudTrail Guía del usuario de](#).

Temas

- [Supervisión de eventos para la API de datos de Amazon Redshift en Amazon EventBridge \(p. 198\)](#)
- [Registro de llamadas a la API de datos de Amazon Redshift con AWS CloudTrail \(p. 199\)](#)

Supervisión de eventos para la API de datos de Amazon Redshift en Amazon EventBridge

Puede monitorear los eventos de la API de datos en EventBridge, que proporciona un flujo de datos en tiempo real desde sus propias aplicaciones, aplicaciones de software como servicio (SaaS) y AWS Servicios de . EventBridge enruta esos datos a destinos como AWS Lambda y Amazon SNS. Estos eventos son los mismos que los que aparecen en Eventos de CloudWatch, que proporciona un flujo casi en tiempo real de eventos del sistema que describen cambios en AWS de AWS. Los eventos se envían a la cuenta que contiene la base de datos de Amazon Redshift. Por ejemplo, si asume un rol en otra cuenta, los eventos se envían a dicha cuenta. Para obtener más información, consulte [AWS Eventos](#) en la Guía del usuario de Amazon EventBridge.

Los eventos de API de datos se envían cuando el `ExecuteStatement` La operación de la API establece la `WithEvent` opción para `true`. La `state` El campo del evento contiene uno de los siguientes valores:

- FAILED — Error en la ejecución de la consulta.
- FINALIZADO — La consulta ha terminado de ejecutarse.

Los siguientes ejemplos muestran un evento para la API de datos cuando el `ExecuteStatement` Operación de la API finaliza.

Ejemplo de evento terminado de API de datos

En el siguiente evento de ejemplo, se utiliza una instrucción denominada `test.testtable` Terminó de funcionar.

```
{
  "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
  }
}
```

Registro de llamadas a la API de datos de Amazon Redshift conAWS CloudTrail

La API de datos de Amazon Redshift está integrada conAWS CloudTrail. CloudTrail es un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o unAWSEn la API de datos de Amazon Redshift. CloudTrail captura como eventos todas las llamadas a la API de datos de Amazon Redshift. Las llamadas capturadas incluyen las llamadas desde la consola de datos de Amazon Redshift y las llamadas desde el código a las operaciones de la API de datos de Amazon Redshift.

Si crea un registro de seguimiento de CloudTrail, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de la API de datos de Amazon Redshift. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar ciertas cosas. Estos incluyen la solicitud que se envió a la API de datos de Amazon Redshift, la dirección IP desde la que se realizó la solicitud, quién realizó la solicitud, cuándo se realizó y detalles adicionales.

Para obtener más información acerca de CloudTrail, consulte la [Guía del usuario de AWS CloudTrail](#).

Trabajar con información de API de datos en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en la API de datos de Amazon Redshift, dicha actividad se registra en un evento de CloudTrail junto con otrosAWS eventos de servicios enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte[Ver eventos con el historial de eventos de CloudTrail](#)en laAWS CloudTrailGuía del usuario.

Para obtener un registro continuo de los eventos de laAWS, incluidos los eventos de la API de datos de Amazon Redshift, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS. El registro de seguimiento consigna los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. También es posible configurar otros servicios de AWS

para analizar en profundidad y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte lo siguiente en la [AWS CloudTrail Guía del usuario](#):

- [Introducción a la creación de registros de seguimiento](#)
- [Consulte Servicios e integraciones compatibles con CloudTrail.](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas](#)

CloudTrail registra todas las acciones de la API de datos de Amazon Redshift y se documentan en [Referencia a la API de datos de Amazon Redshift](#). Por ejemplo, las llamadas `executeStatement`, `getStatementResults` y `cancelStatement` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte [Elemento `userIdentity` CloudTrail](#) en la [AWS CloudTrail Guía del usuario](#).

Descripción de las entradas del archivo de registro de la API de

El registro de seguimiento de la API de Amazon Redshift es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una solicitud específica realizada desde un origen y contiene información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que estas no aparecen en ningún orden específico.

En el ejemplo siguiente, se muestra una entrada de registro de CloudTrail que ilustra la acción `ExecuteStatement`.

```
{
  "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",
    "recipientAccountI": "123456789012"
  }
}
```

Enhanced VPC Routing

Cuando utiliza el enrutamiento de VPC mejorado de Amazon Redshift, Amazon Redshift obliga a todos los [COPY](#) y [DESCARGAR](#). Puesto que el tráfico entre el clúster y los repositorios de datos a través de la nube privada virtual (VPC) basada en el servicio de Amazon VPC. Mediante el uso de enrutamiento VPC mejorado, puede utilizar funciones de VPC estándar, como [VPC security groups](#), [Listas de control de acceso \(ACL\)](#), [Puntos de conexión de la VPC](#), [Políticas de punto de enlace de la VPC](#), [puertos de enlace a Internet](#), y [Sistema de nombres de dominio \(DNS\)](#), tal y como se describe en el [Guía del usuario de Amazon VPC](#). Puede utilizar estas características para administrar de forma precisa el flujo de datos entre el clúster de Amazon Redshift y otros recursos. Cuando utiliza el direccionamiento de VPC mejorado para direccionar el tráfico a través de la VPC, también puede utilizar [registros de flujo de VPC](#) para monitorear el tráfico COPY y UNLOAD.

Si Enhanced VPC Routing no está habilitado, Amazon Redshift dirige el tráfico a través de Internet, incluido el tráfico a otros servicios dentro de la [AWS Red](#).

Important

Puesto que Enhanced VPC Routing afecta la forma en la que Amazon Redshift accede a otros recursos, los comandos COPY y UNLOAD podrían fallar a menos que configure la VPC correctamente. Debe crear una ruta de acceso a la red específica entre la VPC del clúster y los recursos de datos, como se describe a continuación.

Cuando ejecuta un comando COPY o UNLOAD en un clúster que tiene Enhanced VPC Routing habilitado, la VPC dirige el tráfico al recurso especificado utilizando la ruta de red más estricta, o más específica, disponible.

Por ejemplo, puede configurar las siguientes rutas en la VPC:

- **Puntos de conexión de la VPC**— Para el tráfico a un bucket de Amazon S3 en la misma [AWS](#) En la región como clúster, puede crear un punto de enlace de la VPC para direccionar el tráfico al bucket de forma directa. Cuando utiliza los puntos de enlace de la VPC, puede adjuntar una política de puntos de enlace para administrar el acceso a Amazon S3. Para obtener más información acerca del uso de puntos de enlace con Amazon Redshift, consulte [Uso de los puntos de enlace de la VPC \(p. 203\)](#).
- **gateway NAT**— Puede conectarse a un bucket de Amazon S3 en otro [AWS](#) Region, y puede conectarse a otro servicio dentro de la [AWS](#) Red. También puede obtener acceso a una instancia de host fuera de [AWS](#) Red. Para ello, configure una [Gateway](#), tal y como se describe en la [Guía del usuario de Amazon VPC](#).
- **Gateway de Internet**— Para conectar a [AWS](#) fuera de su VPC, puede adjuntar un [gateway de Internet](#) a su subred VPC, tal y como se describe en la [Guía del usuario de Amazon VPC](#). Para utilizar un gateway de Internet, el clúster debe tener una IP pública para permitir a otros servicios comunicarse con el clúster.

Para obtener más información, consulte [Puntos de enlace de la VPC](#) de en la [Guía del usuario de Amazon VPC](#).

El uso de Enhanced VPC Routing no supone ningún cargo adicional. Es posible que incurra en cargos adicionales por transferencia de datos para determinadas operaciones. Entre ellas se incluyen operaciones como UNLOAD a Amazon S3 en [AWS](#) Región. COPY desde Amazon EMR o Secure Shell (SSH) con direcciones IP públicas. Para obtener más información acerca de los precios, consulte [Precios de Amazon EC2](#).

Temas

- [Uso de los puntos de enlace de la VPC \(p. 203\)](#)
- [Habilitación de Enhanced VPC Routing \(p. 203\)](#)

- [Uso de Amazon Redshift Spectrum con Enhanced VPC Routing \(p. 206\)](#)

Uso de los puntos de enlace de la VPC

Puede utilizar un punto de enlace de la VPC para crear una conexión administrada entre el clúster de Amazon Redshift de una VPC y Amazon Simple Storage Service (Amazon S3). Cuando lo haga, el tráfico COPY y UNLOAD entre el clúster y los datos de Amazon S3 permanecerá en la VPC de Amazon. Puede adjuntar una política de punto de enlace al punto de enlace para administrar con más precisión el acceso a los datos. Por ejemplo, puede añadir una política al punto de enlace de la VPC que permita la descarga de datos únicamente a un bucket específico de Amazon S3 en su cuenta.

Important

Actualmente, Amazon Redshift admite los puntos de enlace de la VPC únicamente para conectarse a Amazon S3. Cuando Amazon VPC agrega compatibilidad con otros AWS Para utilizar los puntos de enlace de la VPC, Amazon Redshift también admitirá esas conexiones de puntos de enlace de la VPC. Para conectarse a un bucket de Amazon S3 utilizando un punto de enlace de la VPC, el clúster de Amazon Redshift y el bucket de Amazon S3 deben estar en el mismo AWS Región .

Para utilizar los puntos de enlace de la VPC, cree un punto de enlace de la VPC para la VPC en la que está el clúster y luego habilite enhanced VPC routing en el clúster. Puede habilitar enhanced VPC routing cuando crea el clúster en una VPC o puede modificar un clúster en una VPC para que utilice enhanced VPC routing.

Un punto de enlace de la VPC utiliza tablas de ruteo para controlar el direccionamiento del tráfico entre un clúster de la VPC y Amazon S3. Todos los clústeres de subredes asociados a las tablas de ruteo especificadas utilizan automáticamente ese punto de enlace para acceder al servicio.

La VPC utiliza la ruta más específica, o más restrictiva, que coincida con el tráfico del clúster para determinar cómo direccionar el tráfico. Por ejemplo, supongamos que tiene una ruta en la tabla de ruteo para todo el tráfico de Internet (0.0/0/0) que apunta a una gateway de Internet y un punto de enlace de Amazon S3. En este caso, la ruta del punto de enlace tiene preferencia para todo el tráfico destinado a Amazon S3. Esto se debe a que rango de direcciones IP para el servicio de Amazon S3 es más específico que 0.0.0.0.0.0.0.0/0. En este ejemplo, el resto del tráfico de Internet se dirige a la gateway de Internet, incluido el tráfico destinado a los buckets de Amazon S3 en otras AWS Regiones.

Para obtener más información acerca de la creación de puntos de enlace, consulte [Puntos de enlace de la VPC](#) de la Guía del usuario de Amazon VPC.

Puede utilizar políticas de puntos de enlace para controlar el acceso desde el clúster a los buckets de Amazon S3 que almacenan los archivos de datos. De forma predeterminada, el asistente Create Endpoint asocia una política de puntos de enlace que no restringe aún más el acceso de cualquier usuario o servicio dentro de la VPC. Para tener un control más específico, de forma opcional, puede adjuntar una política de puntos de enlace personalizada. Para obtener más información, consulte [Uso de políticas de punto de enlace](#) en la Guía del usuario de Amazon VPC.

El uso de puntos de enlace no supone ningún cargo adicional. Se aplicará la tarifa estándar por la transferencia de datos y el uso de recursos. Para obtener más información acerca de los precios, consulte [Precios de Amazon EC2](#).

Habilitación de Enhanced VPC Routing

Puede habilitar Enhanced VPC Routing cuando crea un clúster o puede modificar un clúster existente para habilitar Enhanced VPC Routing.

Para trabajar con Enhanced VPC Routing, el clúster debe cumplir los siguientes requisitos y restricciones:

- El clúster debe estar en una VPC.

Si asocia un punto de enlace de la VPC de Amazon S3, el clúster utiliza el punto de enlace de la VPC únicamente para obtener acceso a los buckets de Amazon S3 en el mismo AWS Región. Para acceder a los depósitos en otro AWS Región (no utilizando el endpoint de VPC) o para acceder a otros AWS, haga que su clúster sea accesible públicamente o use un [Gateway](#). Para obtener más información, consulte [Creación de un clúster en una VPC \(p. 77\)](#).

- Debe habilitar la resolución del servicio de nombres de dominio (DNS) en la VPC. O bien, si está utilizando su propio servidor DNS, asegúrese de que las solicitudes de DNS a Amazon S3 se resuelven correctamente en las direcciones IP mantenidas por AWS. Para obtener más información, consulte [Utilización de DNS con su VPC](#) en la Guía del usuario de Amazon VPC.
- Los nombres de host de DNS deben estar habilitados en la VPC. Los nombres de host DNS están habilitados de forma predeterminada.
- Las políticas de puntos de enlace de la VPC deben permitir el acceso a cualquier bucket de Amazon S3 utilizado con llamadas a COPY, UNLOAD o CREATE LIBRARY en Amazon Redshift, incluido el acceso a cualquier archivo de manifiesto involucrado. Para utilizar COPY desde hosts remotos, las políticas de puntos de enlace deben permitir el acceso a cada máquina del host. Para obtener más información, consulte [Permisos de IAM para COPY, UNLOAD y CREATE LIBRARY](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear un clúster con enhanced VPC routing

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y Create cluster (Crear clúster) e introduzca las propiedades de Cluster details (Detalles del clúster).
3. Para mostrar la sección Additional configurations (Configuraciones adicionales), seleccione Use defaults (Usar valores predeterminados).
4. Para habilitar Enhanced VPC routing, seleccione Habilitado para forzar el tráfico del clúster a través de la VPC.
5. Seleccione Create cluster (Crear clúster) para crearlo. El clúster tardará varios minutos antes de estar listo para su uso.

Consola original

Puede crear un clúster con el enhanced VPC routing habilitado usando la AWS Management Console. Para ello, seleccione Yes (Sí) en la opción Enhanced VPC Routing de la sección Configure Networking Options (Configurar opciones de red) del asistente Launch Cluster, como se muestra a continuación. Para obtener más información, consulte [Creación de un clúster \(p. 47\)](#).

Configure Networking Options:

Choose a VPC The identifier of the VPC in which you want to create your cluster

Cluster Subnet Group Selected Cluster Subnet Group may limit the choice of Availability Zones

Publicly Accessible ☒ Yes ☐ No Select Yes if you want the cluster to have a public IP address that can be accessed from the public internet, select No if you want the cluster to have a private IP address that can only be accessed from within the VPC.

Choose a Public IP Address ☐ Yes ☒ No Select Yes if you want to select an elastic IP (EIP) address that you already have configured. Otherwise, select No to have Amazon Redshift create an EIP for your instance.

Enhanced VPC Routing ☒ Yes ☐ No  Additional VPC configuration might be required. [Learn more.](#)

Availability Zone The EC2 Availability Zone that the cluster will be created in.

Para modificar un clúster con el fin de habilitar Enhanced VPC Routing mediante la consola, seleccione el clúster. A continuación, elija Modify Cluster (Modificar clúster) y seleccione Yes (Sí) para la opción Enhanced VPC Routing en el cuadro de diálogo Modify Cluster (Modificar clúster). Para obtener más información, consulte [Modificación de un clúster \(p. 59\)](#).

Note

Cuando modifica un clúster para habilitar Enhanced VPC Routing, el clúster se reinicia automáticamente para aplicar el cambio.

Modify Cluster

Cluster Identifier: example-cluster

Cluster Parameter Group: default.redshift-1.0

Parameter Group Description: Default parameter group for redshift-1.0

VPC Security Groups: d-906736679c_controllers..., default (sg-af8223cb), launch-wizard-4 (sg-8c43f..., launch-wizard-5 (sg-5f46a...

Publicly Accessible: ☒ Yes ☐ No

Choose a Public IP Address: ☐ Yes ☒ No

Enhanced VPC Routing: ☒ Yes ☐ No

Master User Password:

Automated Snapshot Retention Period: 1 days

Maintenance Window Start: Start Day: Saturday, 03:30 UTC

Maintenance Window End: Start Day: Saturday, 04:00 UTC

Additional VPC configuration might be required. [Learn more.](#)

Cancel Modify

Puede utilizar las siguientesAWS Command Line Interface(AWS CLI) para Amazon Redshift para habilitar Enhanced VPC Routing:

- [create-cluster](#)
- [modify-cluster](#)

Puede utilizar las siguientes acciones de las API de Amazon Redshift para habilitar Enhanced VPC Routing:

- [CreateCluster](#)
- [ModifyCluster](#)

Uso de Amazon Redshift Spectrum con Enhanced VPC Routing

Enhanced VPC Routing enruta tráfico específico a través de la VPC. Todo el tráfico entre el clúster y los buckets de Amazon S3 queda obligado a pasar a través de la VPC de Amazon. Redshift Spectrum se ejecuta enAWS-recursos administrados que son propiedad de Amazon Redshift. Como estos recursos están fuera de la VPC, Redshift Spectrum no usa Enhanced VPC Routing.

Cuando el clúster está configurado para usar Enhanced VPC Routing, el tráfico entre Redshift Spectrum y Amazon S3 se enruta de forma segura a través de la AWS red privada, fuera de su VPC. El tráfico en tránsito se firma con el protocolo Signature Version 4 (SIGv4) de Amazon y se cifra mediante HTTPS. Este tráfico se basa en el rol de IAM que está asociado a su clúster de Amazon Redshift. Para administrar aún más el tráfico de Redshift Spectrum, puede modificar el rol IAM de su clúster y la política asociada al bucket de Amazon S3. Es posible que también deba configurar su VPC para permitir que su clúster acceda a AWS Glue o Athena, como se detalla a continuación.

Consideraciones para usar Enhanced VPC Routing para Redshift Spectrum

A continuación se incluyen las consideraciones que se deben tener en cuenta al usar Enhanced VPC Routing para Redshift Spectrum:

- [Políticas de acceso a buckets \(p. 207\)](#)
- [Rol de IAM de clúster \(p. 208\)](#)
- [Registro y auditoría del acceso a Amazon S3 \(p. 208\)](#)
- [Acceso a AWS Glue o Amazon Athena \(p. 209\)](#)

Políticas de acceso a buckets

Puede controlar el acceso a los datos en sus buckets de Amazon S3 utilizando una política de bucket asociada al bucket y un rol de IAM asociado al clúster.

Redshift Spectrum no puede obtener acceso a los datos almacenados en buckets de Amazon S3 que utilizan una política de bucket que restrinja el acceso únicamente a puntos de enlace especificados de la VPC. En su lugar, use una política de bucket que restrinja el acceso únicamente a entidades principales específicas, como a un AWS o usuarios específicos.

Para el rol de IAM al que se concede acceso al bucket, utilice una relación de confianza que permita que únicamente la entidad principal de servicio de Amazon Redshift pueda asumir el rol. Cuando se asocia a su clúster, el rol solo se puede usar en el contexto de Amazon Redshift y no se puede compartir fuera del clúster. Para obtener más información, consulte [Restricción de acceso a los roles de IAM \(p. 364\)](#).

Para utilizar Redshift Spectrum, no puede haber ninguna directiva de IAM que bloquee el uso de direcciones URL prefirmadas.

El siguiente ejemplo de política de bucket solo permite acceder al bucket especificado al tráfico originado por Redshift Spectrum propiedad de AWS account 123456789012.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "BucketPolicyForSpectrum",
      "Effect": "Allow",
      "Principal": { "AWS": [ "arn:aws:iam::123456789012:root" ] },
      "Action": [ "s3:GetObject", "s3:List*" ],
      "Resource": [ "arn:aws:s3:::examplebucket/*" ],
      "Condition": { "StringEquals": { "aws:UserAgent": "AWS Redshift/Spectrum" } }
    }
  ]
}
```

Rol de IAM de clúster

El rol asociado a su clúster debería tener una relación de confianza que solo permita que el rol sea asumido por el servicio de Amazon Redshift, tal como se muestra a continuación.

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

Puede agregar una política al rol del clúster que impida el acceso de COPY y UNLOAD a un bucket específico. La siguiente política solo permite tráfico al bucket especificado procedente de 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"}}
  }]
}
```

Para obtener más información, consulte [Políticas de IAM para Amazon Redshift Spectrum](#) en la [Amazon Redshift](#).

Registro y auditoría del acceso a Amazon S3

Una de las ventajas de usar Amazon Redshift VPC Routing es que todo el tráfico de COPY y UNLOAD queda registrado en los registros de flujo de la VPC. El tráfico originado desde Redshift Spectrum a Amazon S3 no pasa a través de la VPC, por lo que no queda registrado en el registro de flujo de la VPC. Cuando Redshift Spectrum accede a los datos en Amazon S3, realiza estas operaciones en el contexto de la AWS y los privilegios de rol respectivos. Puede registrar y auditar el acceso a Amazon S3 mediante el registro de acceso al servidor AWS CloudTrail Amazon S3.

AWS CloudTrail Registros

Para rastrear todo el acceso a objetos en Amazon S3, incluido el acceso a Redshift Spectrum, habilite el registro de CloudTrail para objetos de Amazon S3.

Puede utilizar CloudTrail para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en la AWS Infraestructura. Para obtener más información, consulte [Introducción a CloudTrail](#).

De manera predeterminada, CloudTrail solo registra acciones en el nivel de bucket. Para realizar un seguimiento de las acciones a nivel de objeto (como `GetObject`), habilite eventos de datos y administración para cada bucket registrado.

Registro de acceso al servidor de Amazon S3

El registro de acceso al servidor brinda registros detallados para las solicitudes realizadas a un bucket. La información del registro de acceso puede ser útil en auditorías de acceso y seguridad. Para obtener más

información, consulte [Cómo habilitar el registro de acceso al servidor](#) en la Amazon Simple Storage Service Developer Guide.

Para obtener más información, consulte la AWS Entrada en el blog de seguridad [Cómo utilizar las políticas de bucket y aplicar defensa en profundidad para proteger sus datos de Amazon S3](#).

Acceso a AWS Glueo Amazon Athena

Redshift Spectrum accede a su catálogo de datos en AWS Glueo Athena. Otra opción es utilizar un metaalmacén de Hive específico para su catálogo de datos.

Para habilitar el acceso a AWS Glueo Athena, configure su VPC con una gateway de Internet o una gateway NAT. Configure los grupos de seguridad de la VPC para permitir el tráfico saliente a los puntos de enlace públicos para AWS Gluey Athena. Alternativamente, puede configurar un punto de enlace de la VPC de la interfaz para que AWS Glue acceda a su AWS Glue Data Catalog. Cuando se utiliza un punto de enlace de interfaz VPC, la comunicación entre la VPC y AWS Glue se lleva a cabo dentro del AWS Red. Para obtener más información, consulte [Creación de un punto de enlace de interfaz](#).

Puede configurar las siguientes rutas en la VPC:

- Gateway de Internet: Para conectar a AWS fuera de su VPC, puede adjuntar un [gateway de Internet](#) a su subred VPC, tal y como se describe en la Guía del usuario de Amazon VPC. Para utilizar una gateway de Internet, el clúster debe tener una dirección IP pública para permitir a otros servicios comunicarse con el clúster.
- gateway NAT—Para conectar a un bucket de Amazon S3 en otra AWS Región o a otro servicio dentro de la AWS, configure una [Gateway](#), tal y como se describe en la Guía del usuario de Amazon VPC. Utilice esta configuración también para obtener acceso a una instancia de host fuera de AWS Red.

Para obtener más información, consulte [Enhanced VPC Routing](#) (p. 202).

Grupos de parámetros de Amazon Redshift

Overview

En Amazon Redshift, puede asociar un grupo de parámetros con cada clúster que cree. A Grupo de parámetros deEs un grupo de parámetros que se aplican a todas las bases de datos que crea en el clúster. Estos parámetros configuran los ajustes de la base de datos, como el tiempo de espera de consulta y el estilo de

Acerca de los grupos de parámetros

Cada grupo de parámetros tiene varios parámetros para la configuración de ajustes de la base de datos. La lista de parámetros disponibles depende de la familia de grupos de parámetros a la que el grupo de parámetros pertenece. La Familia de grupos de parámetrosEs la versión del motor de Amazon Redshift a la que se aplican los parámetros del grupo de parámetros. El formato del nombre de la familia de grupos de parámetros es `redshift-version`, donde *version* es la versión del motor. Por ejemplo, la versión actual del motor es `redshift-1.0`.

Amazon Redshift proporciona un grupo de parámetros predeterminado para cada familia de grupos de parámetros. El grupo de parámetros predeterminado tiene valores preestablecidos para cada uno de sus parámetros y no pueden modificarse. El formato del nombre del grupo de parámetros predeterminado es `default.parameter_group_family`, donde *parameter_group_family* es la versión del motor al que pertenece el grupo de parámetros. Por ejemplo, el grupo de parámetros predeterminado para la versión `redshift-1.0` se llama `default.redshift-1.0`.

Note

En este momento, `redshift-1.0` Es la única versión del motor de Amazon Redshift. Por lo tanto, `default.redshift-1.0` es el único grupo de parámetros predeterminado.

Si desea utilizar valores de parámetros diferentes a los del grupo de parámetros predeterminado, debe crear un grupo de parámetros personalizado y luego asociar el clúster a él. Inicialmente, los valores de los parámetros de un grupo de parámetros personalizado son los mismos que los de un grupo de parámetros predeterminado. El valor inicial de `source` para todos los parámetros es `engine-default`. Amazon Redshift establece previamente los valores. Luego de cambiar un valor de parámetro, el `source` cambia a `user` para indicar que su valor predeterminado se ha modificado.

Note

La consola de Amazon Redshift no muestra el `source` de cada parámetro. Para ello debe utilizar la API de Amazon Redshift, la AWS CLI o uno de los AWS SDK para ver el `source`.

Si se trata de grupos de parámetros creados por usted, puede modificar el valor de parámetro en cualquier momento o puede restablecer los valores de parámetros a sus valores predeterminados. También puede asociar un grupo de parámetros diferente a un clúster. En algunos casos, podrá modificar los valores del parámetro en un grupo de parámetros que ya está asociado a un clúster o asociar un grupo de parámetros diferentes a un clúster. En estos casos, quizás tenga que reiniciar el clúster para que se aplique los valores de los parámetros actualizados. Si el clúster falla y lo reinicia Amazon Redshift, los cambios se aplican en

ese momento. Si el clúster se reinicia durante el mantenimiento, no se aplican los cambios. Para obtener más información, consulte [Propiedades dinámicas y estáticas de WLM \(p. 213\)](#).

Valores de parámetros predeterminados

En la siguiente tabla se muestran los valores de parámetros predeterminados junto con enlaces a información más exhaustiva acerca de cada parámetro. Estos son los valores predeterminados para la familia de grupos de parámetros `redshift-1.0`.

Nombre del parámetro	Valor	Más información
<code>auto_analyze</code>	<code>true</code>	auto_analyze en la Guía para desarrolladores de bases de datos
<code>datestyle</code>	ISO, MDY	datestyle en la Guía para desarrolladores de bases de datos
<code>enable_case_sensitive_identifier</code>	<code>false</code>	enable_case_sensitive_identifier en la Guía para desarrolladores de bases de datos
<code>enable_user_activity_logging</code>	<code>false</code>	Registro de auditoría de bases de datos (p. 373) en esta guía
<code>extra_float_digits</code>	0	extra_float_digits en la Guía para desarrolladores de bases de datos
<code>max_concurrency_scaling_clusters</code>	1	max_concurrency_scaling_clusters en la Guía para desarrolladores de bases de datos
<code>query_group</code>	predeterminada	query_group en la Guía para desarrolladores de bases de datos
<code>require_ssl</code>	<code>false</code>	Configuración de las opciones de seguridad para las conexiones (p. 151) en esta guía
<code>search_path</code>	<code>\$user, public</code>	search_path en la Guía para desarrolladores de bases de datos
<code>statement_timeout</code>	0	statement_timeout en la Guía para desarrolladores de bases de datos
<code>wlm_json_configuration</code>	<code>[{"auto_wlm":true}]</code>	Configuración de la administración de cargas de trabajo (p. 213) en esta guía
<code>use_fips_ssl</code>	<code>false</code>	Habilite el modo SSL compatible con FIPS solo si el sistema debe ser compatible con FIPS.

Note

El parámetro `max_cursor_result_set_size` no está disponible. Para obtener más información acerca del tamaño de conjuntos de resultados de cursor, consulte [Restricciones del cursor](#) en la Guía para desarrolladores de bases de datos.

Puede anular un parámetro temporalmente utilizando el comando `SET` en la base de datos. El comando `SET` anula el parámetro solamente durante el tiempo de la sesión actual. Además de los parámetros mencionados en la tabla anterior, también puede ajustar de manera temporal el número de slots

estableciendo `wlm_query_slot_count` en la base de datos. El parámetro `wlm_query_slot_count` no está disponible para su configuración en grupos de parámetros. Para obtener más información acerca del ajuste del número de ranuras, consulte [wlm_query_slot_count](#) en la Guía para desarrolladores de bases de datos. Para obtener más información acerca de la anulación temporal de otros parámetros, consulte [Modificación de la configuración del servidor](#) en la Guía para desarrolladores de bases de datos.

Configuración de los valores de parámetros mediante la AWS CLI

Para configurar los parámetros de Amazon Redshift mediante el AWS CLI, utilice el comando `modify-cluster-parameter-group` para un grupo de parámetros específico. Especifique el grupo de parámetros a modificar en `parameter-group-name`. Utilice el parámetro `parameters` (para el comando `modify-cluster-parameter-group`) para especificar los pares de nombre/valor de cada parámetro que desea modificar en el grupo de parámetros.

Note

Existen consideraciones especiales cuando se configura el parámetro `wlm_json_configuration` mediante la AWS CLI. Los ejemplos de esta sección aplican a todos los parámetros, excepto `wlm_json_configuration`. Para obtener más información acerca de la configuración de `wlm_json_configuration` mediante la AWS CLI, consulte [Configuración de la administración de cargas de trabajo](#) (p. 213).

Luego de modificar los valores de parámetros, debe reiniciar cualquier clúster que esté asociado al grupo de parámetros modificado. El estado del clúster muestra `applying` para el `ParameterApplyStatus` durante la aplicación de los valores y `pending-reboot` después de que se han aplicado los valores. Luego de reiniciar, la base de datos del clúster comienza a utilizar los nuevos valores de parámetros. Para obtener más información acerca del reinicio de clústeres, consulte [Reinicio de un clúster](#) (p. 63).

Note

El parámetro `wlm_json_configuration` contiene algunas propiedades que son dinámicas y no requieren el reinicio de los clústeres asociados para que se apliquen los cambios. Para obtener más información acerca de las propiedades dinámicas y estáticas, consulte [Propiedades dinámicas y estáticas de WLM](#) (p. 213).

Sintaxis

La siguiente sintaxis muestra cómo utilizar el comando `modify-cluster-parameter-group` para configurar un parámetro. Especifique `parameter_group_name` y reemplace `parameter_name` y `parameter_value` por un parámetro real que desee modificar y un valor para ese parámetro. Si desea modificar más de un parámetro al mismo tiempo, separe con un espacio cada parámetro y valor establecido del siguiente.

```
aws redshift modify-cluster-parameter-group --parameter-group-name parameter_group_name --parameters ParameterName=parameter_name,ParameterValue=parameter_value
```

Ejemplo

En el siguiente ejemplo, se muestra cómo configurar los parámetros `statement_timeout` y `enable_user_activity_logging` para el grupo de parámetros `myclusterparametergroup`.

Note

Por fines de legibilidad, el ejemplo se muestra en varias líneas pero, en la AWS CLI real, se ve en una línea.

```
aws redshift modify-cluster-parameter-group
--parameter-group-name myclusterparametergroup
--parameters ParameterName=statement_timeout,ParameterValue=20000
ParameterName=enable_user_activity_logging,ParameterValue=true
```

Puede administrar los grupos de parámetros mediante la consola de. Para obtener más información, consulte [Administración de grupos de parámetros mediante la consola](#) (p. 223).

Configuración de la administración de cargas de trabajo

En Amazon Redshift, se utiliza la administración de cargas de trabajo (WLM, administración de cargas de trabajo) para definir el número de colas de consultas que están disponibles y cómo direccionar las consultas a esas colas para su procesamiento. WLM forma parte de la configuración de grupos de parámetros. Un clúster utiliza la configuración de WLM que se especifica en su grupo de parámetros asociados.

Cuando crea un grupo de parámetros, la configuración de WLM predeterminada contiene una cola que puede ejecutar hasta cinco consultas simultáneamente. Puede añadir colas adicionales y configurar las propiedades de WLM en cada una de ellas si desea tener más control en el procesamiento de consultas. Cada cola que añade tiene la misma configuración de WLM predeterminada hasta que configure sus propiedades.

Si añade otras colas, la última cola de la configuración será la cola predeterminada. A menos que la consulta se dirija a otra cola basada en criterios de la configuración de WLM, la consulta se procesa por la cola predeterminada. Puede especificar el modo y el nivel de simultaneidad (slots de consulta) de la cola predeterminada, pero no puede especificar grupos de usuarios ni grupos de consultas para dicha cola.

Como sucede con otros parámetros, usted no puede modificar la configuración de WLM en el grupo de parámetros predeterminado. Los clústeres asociados al grupo de parámetros predeterminado siempre utilizan la configuración de WLM predeterminada. Si desea modificar la configuración de WLM, cree un nuevo grupo de parámetros y asílo a cualquier clúster que requiera su configuración de WLM personalizada.

Propiedades dinámicas y estáticas de WLM

Las propiedades de configuración de WLM son dinámicas o estáticas. Puede aplicar propiedades dinámicas a la base de datos sin reiniciar el clúster, pero las propiedades estáticas requieren el reinicio del clúster para que los cambios surtan efecto. Para obtener más información sobre las propiedades estáticas y dinámicas, consulte [Propiedades de configuración dinámicas y estáticas de WLM](#).

Propiedades del parámetro `wlm_json_configuration`

Puede configurar WLM mediante la consola de Amazon Redshift, la AWS CLI, la API de Amazon Redshift o una de las AWS SDK de. La configuración de WLM usa diversas propiedades para definir el comportamiento de la cola, como la asignación de memoria entre colas, el número de consultas que se pueden ejecutar simultáneamente en una cola, etc.

Note

Las siguientes propiedades aparecen en las descripciones con los nombres de consola de Amazon Redshift y los nombres de las propiedades JSON correspondientes.

La tabla siguiente resume si una propiedad es aplicable a WLM automática o WLM manual.

Propiedad de WLM	WLM automática	WLM manual
Auto WLM (WLM automática)	Sí	Sí
Habilitar aceleración de consultas cortas	Sí	Sí
Tiempo máximo de ejecución de consultas cortas	Sí	Sí
Prioridad	Sí	No
Tipo de cola	Sí	Sí
Nombre de la cola	Sí	Sí
Modo de escalado de simultaneidad	Sí	Sí
Simultaneidad	No	Sí
Grupos de usuarios	Sí	Sí
Comodín de grupo de usuarios	Sí	Sí
Grupos de consultas	Sí	Sí
Comodín de grupo de consultas	Sí	Sí
Tiempo de espera	No	Obsoleto
Memoria	No	Sí
Reglas de monitorización de consultas	Sí	Sí

En la siguiente lista se describen las propiedades de WLM que puede configurar para cada cola.

Auto WLM (WLM automática)

Auto WLM (WLM automática) establecida en `true` habilita la WLM automática. WLM automático establece los valores de `Simultaneidad` en `principalMemory (%)` (Porcentaje de memoria) de `Auto`. Amazon Redshift gestiona la simultaneidad de consultas y la asignación de memoria. El valor predeterminado es `true`.

Propiedad JSON: `auto_wlm`

Habilitar aceleración de consultas cortas

La aceleración de consultas cortas (SQA) da prioridad a una serie de consultas seleccionadas que se ejecutan rápidamente frente a consultas que tardan más en ejecutarse. SQA ejecuta las consultas cortas en un espacio dedicado, de forma que estas consultas no tienen que esperar en las colas detrás de otras consultas más largas. Con SQA, las consultas cortas se ejecutan con mayor rapidez y los usuarios tardan menos en ver los resultados. Si habilita SQA, también puede especificar el tiempo máximo de ejecución de las consultas cortas. Para habilitar SQA, especifique `true`. El valor predeterminado es `false`.

Propiedad JSON: `short_query_queue`

Tiempo máximo de ejecución de consultas cortas

Si habilita SQA, también puede especificar 0 para permitir que WLM establezca de forma dinámica el tiempo máximo de ejecución de las consultas cortas. Por otro lado, también puede especificar un valor en milisegundos comprendido entre 1 y 20 segundos. El valor predeterminado es 0.

Propiedad JSON: `max_execution_time`

Prioridad

La prioridad establece la prioridad de las consultas que se ejecutan en una cola. Para establecer la prioridad, WLM mode (Modo de WLM) debe estar definido en Auto WLM (WLM automática); es decir, `auto_wlm` debe ser `true`. Los valores de prioridad pueden ser `highest`, `high`, `normal`, `low` y `lowest`. El valor predeterminado es `normal`.

Propiedad JSON: `priority`

Tipo de cola

El tipo de cola designa una cola tal como la utiliza Auto WLM (WLM automática) o Manual WLM (WLM manual). Establezca `queue_type` en `auto` o `manual`. Si no se especifica, el valor predeterminado es `manual`.

Propiedad JSON: `queue_type`

Nombre de la cola

El nombre de la cola. Puede establecer el nombre de la cola en función de las necesidades de su empresa. Los nombres de cola deben ser únicos dentro de una configuración WLM, tener hasta 64 caracteres alfanuméricos, guiones bajos o espacios y no pueden contener comillas. Por ejemplo, si tiene una cola para sus consultas ETL, podría denominarla `ETL_queue`. Este nombre se utiliza en métricas, valores de tabla del sistema y en la consola de Amazon Redshift para identificar la cola. Las consultas e informes que utilizan el nombre a partir de estas fuentes tienen que poder controlar los cambios del nombre. Anteriormente, Amazon Redshift generaba los nombres de cola. Los nombres predeterminados de las colas son `queue_1`, `queue_2`, hasta la última cola denominada `Default_queue`.

Important

Si cambia el nombre de una cola, también cambia el valor de la dimensión `QueueName` de las métricas de cola WLM (por ejemplo, `WLMQueueLength`, `WLMQueueWaitTime`, `WLMQueriesCompletedPerSecond`, `WLMQueryDuration`, `WLMRunningQueries`, etc.). Por lo tanto, si cambia el nombre de una cola, es posible que tenga que cambiar las alarmas de CloudWatch que haya configurado.

Propiedad JSON: `name`

Modo de escalado de simultaneidad

Para habilitar el escalado de simultaneidad en una cola, establezca `Concurrency Scaling mode` (Modo de escalado de simultaneidad) en `auto`. Cuando el número de consultas enviadas a una cola supera la simultaneidad configurada de la cola, las consultas que cumplen los requisitos se envían al clúster de escalado. Cuando hay slots disponibles, las consultas se ejecutan en el clúster principal. El valor predeterminado es `off`.

Propiedad JSON: `concurrency_scaling`

Simultaneidad

Número de consultas que pueden ejecutarse simultáneamente en una cola de WLM manual. Esta propiedad solo se aplica al WLM manual. Si el modo de escalado de simultaneidad está habilitado, las consultas que cumplen los requisitos se envían a un clúster de escalado cuando una cola alcanza el nivel de simultaneidad (slots de consulta). Si el escalado de simultaneidad no está habilitado, las consultas esperan en la cola hasta que haya un slot disponible. El rango está entre 1 y 50.

Propiedad JSON: `query_concurrency`

User Groups (Grupos de usuarios)

Una lista de nombres de grupos de usuarios separada por comas. Cuando los miembros del grupo de usuarios ejecutan consultas en la base de datos, estas se dirigen a la cola que está asociada a su grupo de usuarios.

Propiedad JSON: `user_group`

Carácter comodín de grupos de usuarios

Un valor booleano que indica si se habilitan comodines para los grupos de usuarios. Si el valor es 0, los comodines están desactivados y si el valor es 1, los comodines están habilitados. Si los caracteres comodín están habilitados, puede utilizar "*" o "?" para especificar varios grupos de usuarios al ejecutar consultas. Para obtener más información, consulte [Wildcards](#).

Propiedad JSON: `user_group_wild_card`

Grupos de consultas

Una lista de grupos de consultas separada por comas. Cuando los miembros del grupo de consultas ejecutan consultas en la base de datos, estas se dirigen a la cola que está asociada a su grupo de consultas.

Propiedad JSON: `query_group`

Carácter comodín de grupos de consultas

Un valor booleano que indica si se habilitan comodines para los grupos de consultas. Si el valor es 0, los comodines están desactivados y si el valor es 1, los comodines están habilitados. Si los caracteres comodín están habilitados, puede utilizar "*" o "?" para especificar varios grupos de consultas al ejecutar consultas. Para obtener más información, consulte [Wildcards](#).

Propiedad JSON: `query_group_wild_card`

Tiempo de espera (ms)

El tiempo de espera de WLM (`max_execution_time`) no está disponible. Si no está disponible cuando se utiliza WLM automática. En su lugar, cree una regla de monitorización de consultas (QMR) utilizando `query_execution_time` para limitar el tiempo de ejecución transcurrido de una consulta. Para obtener más información, consulte [Reglas de monitoreo de consultas de WLM](#).

El tiempo máximo, en milisegundos, en el que se pueden ejecutar las consultas antes de ser canceladas. En algunos casos, una consulta de solo lectura, como por ejemplo una instrucción SELECT, podría cancelarse debido al tiempo de espera de WLM. En estos casos, WLM intenta direccionarla a la siguiente cola coincidente en función de las reglas de asignación de colas de WLM. Si la consulta no coincide con ninguna otra definición de cola, esta no se asigna a la cola predeterminada, sino que se cancela. Para obtener más información, consulte [Salto de cola de consultas de WLM](#). El tiempo de espera de WLM no aplica a una consulta que haya alcanzado el estado `returning`. Para ver el estado de una consulta, diríjase a la tabla de sistema `STV_WLM_QUERY_STATE`.

Propiedad JSON: `max_execution_time`

Memory (%) (Porcentaje de memoria)

El porcentaje de memoria para asignar a la cola. Si especifica un porcentaje de memoria para al menos una de las colas, debe especificar un porcentaje para todas las otras colas hasta llegar a un total de 100 por ciento. Si la asignación de memoria es inferior al 100 por cien en todas las colas, el servicio administra la memoria sin asignar. El servicio puede entregar temporalmente esta memoria sin asignar a una cola que solicita memoria adicional para el procesamiento.

Propiedad JSON: `memory_percent_to_use`

Reglas de monitorización de consultas

Puede utilizar las reglas de monitorización de consultas de WLM para monitorear de forma continua las colas de WLM de consultas basadas en criterios o predicados que usted especificó. Por ejemplo, es posible que monitoree consultas que tiendan a consumir recursos excesivos del sistema y luego inicie una acción especificada cuando la consulta exceda los límites de rendimiento especificados.

Note

Si decide crear reglas mediante programación, recomendamos encarecidamente utilizar la consola para generar el JSON que incluirá en la definición del grupo de parámetros.

Asocie una regla de monitorización de consultas a una cola de consultas específica. Puede tener hasta 25 reglas por cola y el límite total para todas las colas es 25 reglas.

Propiedad JSON: `rules`

Jerarquía de propiedades JSON:

```
rules
  rule_name
  predicate
    metric_name
    operator
    value
  action
    value
```

Especifique las siguientes propiedades para cada regla:

- `rule_name` Los nombres de regla deben ser únicos en la configuración de WLM. Los nombres de reglas pueden tener un máximo de 32 caracteres alfanuméricos o guiones bajos y no pueden contener espacios ni comillas. Puede disponer de hasta ocho reglas por cola y el límite total para todas las colas es de ocho reglas.
- `predicate` Puede tener hasta tres predicados por regla. Especifique las siguientes propiedades para cada predicado:
 - `metric_name` Para ver una lista de métricas de, consulte [Métricas de monitoreo de consultas](#) en la Guía para desarrolladores de bases de datos.
 - `operator` Operaciones son: `=`, `<`, `>`.
 - `value` Valor de umbral para la métrica especificada que activa una acción.
- `action` Cada regla está asociada a una acción. Las acciones válidas son:
 - `log`
 - `hop` (solo disponible con WLM manual)
 - `abort`
 - `change_query_priority` (solo disponible con WLM automática)

En el siguiente ejemplo se muestra el JSON para una regla de monitorización de consultas de WLM denominada `rule_1`, con dos predicados y la acción `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"
  }
]
```

Para obtener más información acerca de cada una de estas propiedades y estrategias para la configuración de colas de consultas, consulte [Implementación de Workload Management](#) en la Guía para desarrolladores de bases de datos.

Configuración del parámetro wlm_json_configuration mediante la AWS CLI

Para configurar WLM, modifique el parámetro `wlm_json_configuration`. El tamaño máximo de `lawlm_json_configuration` valor de la propiedad es de 8000 caracteres. El valor tiene el formato de JavaScript Object Notation (JSON). Si configura WLM mediante el comando AWS CLI, la API de Amazon Redshift o una de las AWS SDK de, utilice el resto de esta sección para aprender a crear la estructura JSON para `lawlm_json_configuration` Parámetro.

Note

Si configura WLM mediante la consola de Amazon Redshift, no necesita comprender el formato JSON ya que la consola proporciona una forma sencilla de añadir colas y configurar sus propiedades. Para obtener más información acerca de la configuración de WLM mediante la consola, consulte [Modificación de un grupo de parámetros \(p. 225\)](#).

Ejemplo

En el siguiente ejemplo se muestra la configuración de WLM predeterminada, que define una cola con la WLM automática.

```
{
  "auto_wlm": true
}
```

Ejemplo

En el siguiente ejemplo, se muestra una configuración de WLM personalizada que define una cola de WLM manual con un nivel de simultaneidad (slots de consulta) de cinco.

```
{
  "query_concurrency": 5
}
```

Sintaxis

La configuración de WLM predeterminada es muy sencilla, tiene cola única y una propiedad. Puede añadir más colas y configurar varias propiedades para cada cola en la estructura JSON. La siguiente sintaxis representa la estructura JSON que se utiliza para configurar varias colas con varias propiedades:

```
[
  {
    "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",
      ...
    }
  ]"
]
```

En el ejemplo anterior, las propiedades representativas que comienzan con q1 son objetos de una matriz de la primera cola. Cada uno de estos objetos es un par de nombre/valor. name y value establecen juntos las propiedades de WLM para la primera cola. Las propiedades representativas que comienzan con q2 son objetos de una matriz de la segunda cola. Si necesita más colas, añada otra matriz para cada cola adicional y establezca las propiedades de cada objeto.

Cuando modifica la configuración de WLM, debe incluir toda la estructura para las colas, aunque solo desee cambiar una propiedad dentro de una cola. Esto se debe a que toda la estructura JSON se transfiere en forma de cadena como el valor para el parámetro wlm_json_configuration.

Formateo del comando de AWS CLI

El parámetro wlm_json_configuration requiere un formato específico cuando utiliza la AWS CLI. El formato que utilice depende del sistema operativo del cliente. Los sistemas operativos tienen formas diferentes de delimitar la estructura JSON para que se transfiera correctamente desde la línea de comando. Para ver detalles acerca de cómo construir el comando adecuado en los sistemas operativos de Windows, Mac OS X y Linux, consulte las siguientes secciones. Para obtener más información acerca de las diferencias en la delimitación de estructuras de datos JSON en la AWS CLI en general, ver [Citar cadenas](#) en la AWS Command Line Interface Guía del usuario.

Ejemplos

En el comando de ejemplo siguiente se configura WLM manual para un grupo de parámetros denominado example-parameter-group. La configuración permite la aceleración de las consultas cortas con un tiempo de ejecución máximo establecido en 0, lo que le indica a WLM que debe establecer el valor dinámicamente. El valor de ApplyType es dynamic. Esta opción significa que cualquier cambio que se realice en las propiedades dinámicas del parámetro se aplicarán de inmediato, a menos que se hayan realizado otros cambios estáticos en la configuración. La configuración define tres colas con lo siguiente:

- La primera cola permite a los usuarios especificar report como una etiqueta (como se especifica en la propiedad query_group) en sus consultas para ayudar a direccionar las consultas a esa cola. Se pueden realizar búsquedas con caracteres comodín de la etiqueta report*, por lo que no es necesario que la etiqueta sea exacta para que las consultas se direccionen a la cola. Por ejemplo, reports y reporting también coincidirán con este grupo de consultas. La cola tiene asignado el 25 por ciento del total de memoria entre todas las colas y puede ejecutar hasta cuatro consultas al mismo tiempo. Las consultas se limitan a un tiempo máximo de 20.000 milisegundos (ms). El modo se establece en automático, por tanto cuando los slots de consulta de la cola cumplen los requisitos las consultas se envían a un clúster de escalado.
- La segunda cola habilita a los usuarios miembros de grupos admin o dba en la base de datos a que sus consultas se direccionen a la cola para su procesamiento. Las búsquedas de comodín están desactivadas para los grupos de usuarios, por lo que los usuarios deben coincidir de forma exacta con los grupos de la base de datos para que sus consultas se direccionen a la cola. La cola tiene asignado

el 40 por ciento del total de memoria entre todas las colas y puede ejecutar hasta cinco consultas al mismo tiempo. El modo se establece como desactivado, de forma que todas las consultas enviadas por miembros del administrador o grupos de dba se ejecutan en el clúster principal.

- La última cola de la configuración es la cola predeterminada. A esta cola se le asigna el 35 por ciento del total de memoria entre todas las colas y puede procesar hasta cinco consultas a la vez. El modo se establece en automático.

Note

El ejemplo se muestra en varias líneas por fines ilustrativos. Los comandos reales no deben tener saltos de línea.

```
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,
    "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,
    "concurrency_scaling": "off",
    "queue_type": "manual"
  },
  {
    "query_concurrency": 5,
    "query_group": [],
    "query_group_wild_card": 0,
    "user_group": [],
    "user_group_wild_card": 0,
    "concurrency_scaling": "auto",
    "queue_type": "manual"
  },
  {"short_query_queue": true}
]'
```

A continuación se muestra un ejemplo de configuración de las reglas de monitorización de consultas de WLM para una configuración de WLM automática. El ejemplo crea un grupo de parámetros denominado `example-monitoring-rules`. La configuración define las tres mismas colas que las del ejemplo anterior, pero `query_concurrency` y `memory_percent_to_use` ya no se especifican. La configuración añade además las siguientes reglas y prioridades de consulta:

- La primera cola define una regla denominada `rule_1`. La regla tiene dos predicados: `query_cpu_time > 10000000` y `query_blocks_read > 1000`. La acción de la regla es `log`. La prioridad de esta cola es `Normal`.

- La segunda cola define una regla denominada `rule_2`. La regla tiene dos predicados: `query_execution_time > 600000000` y `scan_row_count > 1000000000`. La acción de la regla es `abort`. La prioridad de esta cola es `Highest`.
- La última cola de la configuración es la cola predeterminada. La prioridad de esta cola es `Low`.

Note

El ejemplo se muestra en varias líneas por fines ilustrativos. Los comandos reales no deben tener saltos de línea.

```
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,
  "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,
  "concurrency_scaling" : "off",
  "rules" : [ {
    "rule_name": "rule_2",
    "predicate": [
      { "metric_name": "query_execution_time",
        "operator": ">",
        "value": 600000000},
      { "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,
  "concurrency_scaling" : "auto",
  "priority": "low",
  "queue_type": "auto",
  "auto_wlm": true
}, {
  "short_query_queue" : true
```



```
} ]'
```

Configuración de WLM mediante la AWS CLI en la línea de comandos con un archivo JSON

Puede modificar el parámetro `wlm_json_configuration` utilizando la AWS CLI de AWS y pasarlo al valor del argumento `parameters` como un archivo JSON.

```
aws redshift modify-cluster-parameter-group --parameter-group-name myclusterparaametergroup  
--parameters file://modify_pg.json
```

Los argumentos de `--parameters` se almacenan en el archivo `modify_pg.json`: La ubicación del archivo se especifica en el formato del sistema operativo. Para obtener más información, consulte [Carga de parámetros desde un archivo](#). A continuación, se muestran ejemplos del contenido del archivo 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"  
  }  
]
```

Reglas para la configuración de WLM mediante la AWS CLI en la línea de comandos de los sistemas operativos Mac OS X y Linux

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas simples (') y corchetes ([]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).
- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Reglas para la configuración de WLM mediante la AWS CLI en Windows PowerShell para los sistemas operativos Microsoft Windows

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas simples (') y corchetes ([]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).
- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (") y su carácter de escape de barra oblicua inversa (\). Este requisito significa que utilizará tres barras inversas y una comilla doble para asegurarse de que las propiedades se transfieran correctamente (\\").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Reglas para la configuración de WLM mediante el símbolo del sistema en los sistemas operativos Windows

Siga estas reglas para ejecutar un comando de la AWS CLI con parámetros en una sola línea:

- Toda la estructura JSON debe estar separada por comillas dobles (") y corchetes ([]).
- Todos los nombres y valores de los parámetros deben estar separados por comillas dobles (").
- Dentro del valor `ParameterValue`, debe separar toda la estructura anidada por comillas dobles (") y corchetes ([]).
- Dentro de la estructura anidada, cada una de las propiedades y los valores para cada cola deben estar separados por llaves ({ }).
- Dentro de la estructura anidada, debe utilizar el carácter de escape de barra oblicua inversa (\) antes de cada comilla doble (") y su carácter de escape de barra oblicua inversa (\). Este requisito significa que utilizará tres barras inversas y una comilla doble para asegurarse de que las propiedades se transfieran correctamente (\\").
- Para los pares de nombre/valor, los dos puntos (:) separan cada propiedad de su valor.
- Cada par nombre/valor se separa del otro por una coma (,).
- Las colas múltiples se separan con una coma (,) entre el final de la llave de una cola (}) y el comienzo de la siguiente llave de la cola ({).

Administración de grupos de parámetros mediante la consola

Puede ver, crear, modificar y eliminar grupos de parámetros en la consola de Amazon Redshift.

Puede consultar cualquier grupo de parámetros de para ver un resumen de los valores de los parámetros y la configuración de administración de cargas de trabajo (WLM). Los grupos de parámetros se muestran en

la pestaña Parameters (Parámetros) y las colas de carga de trabajo se muestran en la pestaña Workload Management (Administración de cargas de trabajo).

Creación de un grupo de parámetros

Si desea establecer valores de parámetros diferentes a los del grupo de parámetros predeterminado, puede crear un grupo de parámetros personalizado.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

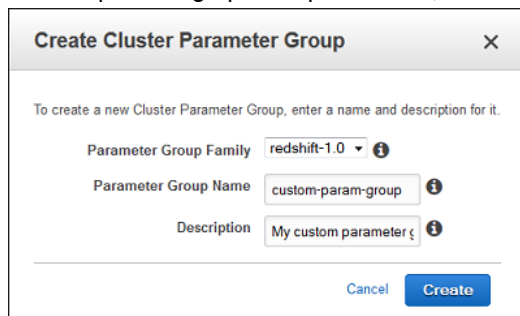
Para crear un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG y Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione Create (Crear) para mostrar la ventana de Create parameter group (Crear grupo de parámetros).
4. Introduzca un valor para Parameter group name (Nombre de grupo de parámetros) y Description (Descripción).
5. Haga clic en Create (Crear) para crear el grupo de parámetros,.

Consola original

Para crear un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Parameter Groups (Grupos de parámetros).
3. En la página Parameter Groups (Grupos de parámetros), seleccione Create Cluster Parameter Group (Crear grupo de parámetros de clúster).
4. En el cuadro de diálogo Create Cluster Parameter Group (Crear grupo de parámetros de clúster), elija una familia de grupos de parámetros. Luego introduzca un nombre de grupo de parámetros y una descripción del grupo de parámetros. Para obtener más información acerca de las restricciones de nombre para los grupos de parámetros, consulte [Cuotas y límites de Amazon Redshift \(p. 494\)](#).



5. Seleccione Create (Crear).

Modificación de un grupo de parámetros

Puede modificar parámetros para cambiar la configuración de los parámetros y las propiedades de la configuración de WLM.

Note

No puede modificar el grupo de parámetros predeterminado.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para modificar un grupo de parámetros

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG y Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Haga clic en la pestaña Parameters (Parámetros) para ver la configuración de parámetros actual.
5. Haga clic en Edit parameters (Editar parámetros) para permitir cambiar la configuración de estos parámetros:

- auto_analyze
- 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

Para obtener más información sobre estos parámetros, consulte [Grupos de parámetros de Amazon Redshift \(p. 210\)](#).

6. Introduzca sus cambios y luego haga clic en Save (Guardar) para actualizar el grupo de parámetros.

Para modificar la configuración de WLM en un grupo de parámetros

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG y Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).

3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Seleccione la pestaña Workload management (Administración de cargas de trabajo) para ver la configuración actual de WLM.
5. Para modificar la configuración de WLM, seleccione Edit workload queues (Editar colas de cargas de trabajo).
6. (Opcional) Seleccione Enable short query acceleration (Habilitar aceleración de consultas cortas, SQA) para habilitarlas.

Si se habilita SQA, Maximum run time for short queries (1 to 20 seconds) [Tiempo máximo de ejecución para consultas cortas (de 1 a 20 segundos)] se establece en Dynamic (Dinámico) de forma predeterminada. Para establecer el tiempo de ejecución máximo en un valor fijo, seleccione un valor comprendido entre 1 y 20.

7. Realice una o más de las siguientes acciones para modificar la configuración de la cola:
 - Elija Switch WLM mode (Cambiar modo de WLM) para elegir entre Auto WLM (WLM automática) y Manual WLM (WLM manual).

Con Auto WLM (WLM automática), los valores de Memory (Memoria) and Concurrency on main (Simultaneidad en principal) se establecen en auto (automático).

 - Para crear una cola, seleccione Edit workload queues (Editar colas de cargas de trabajo) y seleccione Add Queue (Añadir cola).
 - Para modificar una cola, cambie los valores de propiedad en la tabla. En función del tipo de cola, las propiedades pueden incluir las siguientes:
 - Queue name (Nombre de cola) no se puede cambiar.
 - Memory (%) (Porcentaje de memoria)
 - Concurrency on main cluster (Simultaneidad en clúster principal)
 - El valor de Concurrency Scaling mode (Modo de escalado de simultaneidad) puede ser off (desactivado) o auto (automático).
 - Tiempo de espera (ms)
 - Grupos de usuarios
 - Grupos de consultas

Para obtener más información sobre estas propiedades, consulte [Propiedades del parámetro wlm_json_configuration](#) (p. 213).

Important

Si cambia el nombre de una cola, también cambia el valor de la dimensión `QueueName` de las métricas de cola WLM (por ejemplo, `WLMQueueLength`, `WLMQueueWaitTime`, `WLMQueriesCompletedPerSecond`, `WLMQueryDuration`, `WLMRunningQueries`, etc.). Por lo tanto, si cambia el nombre de una cola, es posible que tenga que cambiar las alarmas de CloudWatch de que ha configurado.

- Para cambiar el orden de las colas, seleccione los botones de las flechas Up (Arriba) y Down (Abajo).
 - Para eliminar una cola, seleccione el botón Delete (Eliminar) en la fila de la cola de la tabla.
8. (Opcional) Seleccione Defer dynamic changes until reboot (Aplazar cambios dinámicos hasta reiniciar). para que se apliquen los cambios a los clústeres hasta el próximo reinicio.

Note

Algunos cambios requieren un reinicio del clúster independientemente de esta configuración. Para obtener más información, consulte [Propiedades dinámicas y estáticas de WLM](#) (p. 213).

9. Elija Save (Guardar).

Consola original

Para modificar parámetros en un grupo de parámetros

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.

En el panel de navegación, seleccione Parameter Groups (Grupos de parámetros).

2. En la página Parameter Groups (Grupos de parámetros) en la lista de grupos de parámetros, seleccione la fila del grupo de parámetros que desea modificar.
3. Para editar parámetros diferentes al parámetro de configuración de WLM, seleccione Edit Parameters (Editar parámetros).

La pestaña Parameters (Parámetros) se abre para que pueda actualizar los parámetros del grupo de parámetros. Puede actualizar los valores de los parámetros como:

- auto_analyze
 - datestyle
 - enable_user_activity_logging
 - extra_float_digits
 - force_acm
 - max_concurrency_scaling_clusters
 - query_group
 - require_ssl
 - search_path
 - statement_timeout
 - use_fips_ssl
4. En el cuadro Value (Valor) que corresponde al parámetro que desea modificar, escriba un nuevo valor. Para obtener más información sobre estos parámetros, consulte [Grupos de parámetros de Amazon Redshift \(p. 210\)](#).
 5. Elija Save changes (Guardar cambios).

Note

Si modifica estos parámetros en un grupo de parámetros que ya está asociado con un clúster, reinicie el clúster para que se apliquen los cambios. Para obtener más información, consulte [Reinicio de un clúster \(p. 63\)](#).

Para modificar la configuración de WLM en un grupo de parámetros

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Workload management (Administración de carga de trabajo).
3. En Parameter groups (Grupos de parámetros), seleccione el grupo de parámetros que desea modificar.

Note

No puede modificar el grupo de parámetros predeterminado.

4. Elija Edit

5. (Opcional) Seleccione Enable short query acceleration (Habilitar aceleración de consultas cortas, SQA) para habilitarlas.

Si se habilita SQA, Maximum run time for short queries (1 to 20 seconds) [Tiempo máximo de ejecución para consultas cortas (de 1 a 20 segundos)] se establece en Dynamic (Dinámico) de forma predeterminada. Para establecer el tiempo de ejecución máximo en un valor fijo, seleccione un valor comprendido entre 1 y 20.

6. Realice una o más de las siguientes acciones para modificar la configuración de la cola:

- Elija Switch WLM mode (Cambiar modo de WLM) para elegir entre Auto WLM (WLM automática) y Manual WLM (WLM manual).

Con Auto WLM (WLM automática), los valores de Memory (Memoria) and Concurrency on main (Simultaneidad en principal) se establecen en auto (automático).

- Para crear una cola, seleccione Add Queue (Añadir cola).
 - Para modificar el parámetro Máximo de clústeres de escalado de simultaneidad, elija Edit (Editar) junto al valor actual mostrado.
 - Para modificar una cola, cambie los valores de propiedad en la tabla. En función del tipo de cola, las propiedades pueden incluir las siguientes:
 - Memory (%) (Porcentaje de memoria)
 - Concurrency on main cluster (Simultaneidad en clúster principal)
 - El valor de Concurrency Scaling mode (Modo de escalado de simultaneidad) puede ser off (desactivado) o auto (automático).
 - Tiempo de espera (ms)
 - Grupos de usuarios
 - Grupos de consultas
 - Para cambiar el orden de las colas, seleccione los botones de las flechas Up (Arriba) y Down (Abajo) en la tabla.
 - Para eliminar una cola, seleccione el botón Delete (Eliminar) en la fila de la cola de la tabla.
7. (Opcional) Seleccione Defer dynamic changes until reboot (Aplazar cambios dinámicos hasta reiniciar). para que se apliquen los cambios a los clústeres hasta el próximo reinicio.

Note

Algunos cambios requieren un reinicio del clúster independientemente de esta configuración. Para obtener más información, consulte [Propiedades dinámicas y estáticas de WLM \(p. 213\)](#).

8. Elija Save (Guardar).

Creación o modificación de una regla de monitoreo de consultas mediante la consola

Puede usar la consola de Amazon Redshift para crear y modificar reglas de administración de consultas de WLM. Las reglas de monitorización de consultas forman parte del parámetro de configuración de WLM para un grupo de parámetros. Si modifica una regla de supervisión de consultas (QMR), el cambio se produce automáticamente sin necesidad de modificar el clúster. Para obtener más información, consulte [Reglas de monitoreo de consultas de WLM](#).

Cuando crea una regla, define el nombre de la regla, uno o más predicados y una acción.

Cuando guarda configuración de WLM que incluye una regla, puede ver el código JSON para la definición de la regla como parte del JSON para el parámetro de configuración de WLM.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una regla de monitorización de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG y Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. Seleccione el grupo de parámetros que desee modificar para mostrar la página de detalles con pestañas para Parameters (Parámetros) y Workload management (Administración de la carga de trabajo).
4. Seleccione la pestaña Workload management (Administrar cargas de trabajo) y seleccione Edit workload queues (Editar colas de cargas de trabajo) para editar la configuración de WLM.
5. Añada una nueva regla utilizando una plantilla predefinida o desde cero.

Para usar una plantilla predefinida, haga lo siguiente:

1. Seleccione Add rule from template (Añadir regla desde plantilla) en el grupo Query monitoring rules (Reglas de monitorización de consultas). Se muestra la lista de plantillas de regla.
2. Seleccione una o varias plantillas de regla. Cuando selecciona Save (Guardar), WLM crea una regla para cada plantilla que selecciona.
3. Introduzca o confirme los valores de la regla, incluyendo Rule names (Nombres de regla), Predicates (Predicados) y Actions (Acciones).
4. Elija Save (Guardar).

Para añadir una nueva regla desde cero, haga lo siguiente:

1. Para añadir predicados adicionales, seleccione Add predicate (Añadir predicado). Puede tener hasta tres predicados por regla. Si se cumplen todos los predicados, WLM desencadena la acción asociada.
2. Seleccione una acción en Action (Acción). Cada regla tiene una acción.
3. Elija Save (Guardar).

Amazon Redshift genera el parámetro de configuración de WLM en formato JSON y lo muestra en la lista de JSONsección.

Consola original

Para crear una regla de monitorización de consultas

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Workload management (Administración de carga de trabajo).
3. En Parameter groups (Grupos de parámetros), seleccione el grupo de parámetros que desea modificar.

Note

No puede modificar el grupo de parámetros predeterminado.

4. Para editar la configuración de WLM (para añadir una regla, elija Edit (Editar).
5. Para crear una nueva regla a través de una plantilla predefinida, en el grupo Rules for Queue 1 (Reglas de la cola 1), seleccione Add Rule from Templates (Añadir regla a partir de plantillas). Aparecerá el cuadro de diálogo Rule Templates (Plantillas de reglas), tal y como se muestra en la siguiente captura de pantalla.

Template Name	Predicate
☐ Nested loop join	Nested loop join row count (rows) > 100
☐ Query returns a high number of rows	Return row count (rows) > 1000000
☐ Join with a high number of rows	Rows joined (rows) > 1000000000
☐ High disk usage when writing intermediate results	Memory to disk (1 MB blocks) > 100000
☒ Long running query with high I/O skew	Segment execution time (seconds) > 120 And I/O skew (ratio) > 2

Cancel **Select**

6. Seleccione una o varias plantillas de regla. WLM crea una regla para cada plantilla que selecciona. En este ejemplo, seleccione Long running query with high I/O skew (Consulta de larga ejecución con un sesgo de E/S elevado) y haga clic en Select (Seleccionar).

Aparecerá una nueva regla con dos predicados, como se muestra en la siguiente captura de pantalla.

Queue 1 Done Editing Delete

Concurrency	User groups	Match wildcards	Query groups	Match wildcards	Timeout (ms)	Memory
5		☒		☐	0	

Rules for Queue 1 Add Rule from Templates | Add Custom Rule

Rule names	Predicates	Actions	Delete
	Segment execution time (seconds) > 120	log	X
	I/O skew (ratio) > 2		X

7. Introduzca un valor para Rule name (Nombre de regla). El nombre puede tener un máximo de 32 caracteres alfanuméricos y no debe contener espacios ni comillas. En este ejemplo, escriba **HighIOskew**.
8. (Opcional) Modificar los predicados de la regla.
9. Elija un valor para Action (Acción). Cada regla tiene una acción. En este ejemplo, seleccione **Hop**. El comando Hop termina la consulta y WLM envía la consulta a la próxima cola coincidente, si hay una disponible.
10. Elija Save (Guardar).

Collapse All

▼ Queue 1 Edit Delete

Concurrency ⓘ	User groups ⓘ	Match wildcards ⓘ	Query groups ⓘ	Match wildcards ⓘ	Timeout (ms) ⓘ	Memory(
5		☒		☐	0	

Rules for Queue 1

Rule names ⓘ	Predicates ⓘ	Actions ⓘ
HighIOskew	segment_execution_time > 120 and io_skew > 2	hop

- Para modificar las reglas de una cola, seleccione Edit (Editar).
- Para añadir una regla nueva desde cero, seleccione Add Custom Rule (Añadir regla personalizada). Puede tener un máximo de cinco reglas por cola, y un total de ocho reglas para todas las colas.
- Escriba un Rule name (Nombre de regla); por ejemplo, **NestedLoop**.
- Defina un valor de Predicate (Predicado). Seleccione un nombre de predicado, un operador y un valor. En este ejemplo, seleccione **Nested loop join count (rows)**. Establezca el operador en un valor superior a (>) y el tipo de valor en **1000**. En la siguiente captura de pantalla se muestra la nueva regla con un predicado.

Rules for Queue 1 Add Rule from Templates Add Custom Rule

Rule names ⓘ	Predicates ⓘ	Actions ⓘ	Delete
HighIOskew	Segment execution time (seconds) > 120	hop	✕
	I/O skew (ratio) > 2		✕
NestedLoop	Nested loop join row count (rows) > 1000	log	✕

- Para añadir predicados adicionales, seleccione el icono de añadir a la derecha de los predicados. Puede tener hasta tres predicados por regla. Si se cumplen todos los predicados, WLM desencadena la acción asociada.
- Seleccione una acción en Action (Acción). Cada regla tiene una acción. En este ejemplo, acepte la acción predeterminada: **Log**. La acción Log escribe un registro en la tabla de sistema **STL_WLM_RULE_ACTION** y deja la consulta ejecutándose en la cola.
- Seleccione Done Editing (Finalizar edición). Los detalles de la cola se contraen.
- Elija Save (Guardar).

Amazon Redshift genera el parámetro de configuración de WLM en formato JSON y muestra JSON en una ventana en la parte inferior de la pantalla, como se muestra en la siguiente captura de pantalla.



Eliminación de un grupo de parámetros

Puede eliminar un grupo de parámetros si ya no lo necesita y si no está asociado a clústeres. Solo puede eliminar grupos de parámetros personalizados.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para eliminar un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG y Workload management (Administración de la carga de trabajo) para mostrar la página de Workload management (Administración de la carga de trabajo).
3. En Parameter groups (Grupos de parámetros), seleccione el grupo de parámetros que desea modificar.

Note

No puede eliminar el grupo de parámetros predeterminado.

4. Seleccione Action (Acción) y confirme que desea eliminar el grupo de parámetros.

Consola original

Para eliminar un grupo de parámetros.

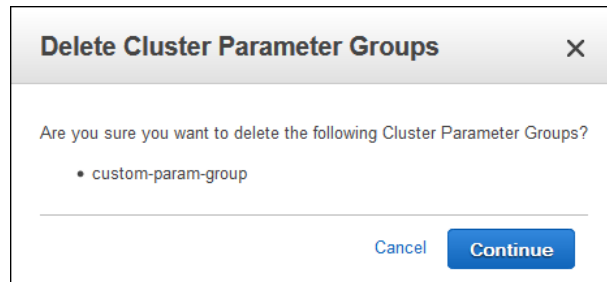
Para eliminar un grupo de parámetros

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Parameter Groups (Grupos de parámetros).
3. Seleccione la fila del grupo de parámetros que desea eliminar y haga clic en Delete (Eliminar).

Note

No puede eliminar el grupo de parámetros predeterminado.

4. En el cuadro de diálogo Delete Cluster Parameter Groups (Eliminar grupos de parámetros del clúster), seleccione Continue (Continuar).



Asociación de un grupo de parámetros con un clúster

Cuando lanza un clúster, debe asociarlo a un grupo de parámetros. Si desea cambiar el grupo de parámetros en otro momento, puede modificar el clúster y seleccionar un grupo de parámetros diferente. Para obtener más información, consulte [Creación de un clúster mediante un lanzamiento del clúster](#) (p. 50) y [Pasos para modificar un clúster](#) (p. 60).

Administración de grupos de parámetros mediante la herramienta AWS SDK for Java

En este ejemplo se muestran las siguientes tareas relacionadas con grupos de parámetros:

- Creación de un grupo de parámetros
- Modificación de un grupo de parámetros
- Asociación de un grupo de parámetros con un clúster
- Obtención de información acerca de grupos de parámetros

Este ejemplo crea un nuevo grupo de parámetros, `parametergroup1`, y realiza las siguientes actualizaciones:

- Cambia el parámetro `extra_float_digits` a 2 del valor predeterminado de 0.
- Reemplaza la configuración de la carga de trabajo existente (parámetro `wlm_json_configuration`) con el siguiente formato JSON que define una cola además de la cola predeterminada.

```
[
  {
    "user_group": [
      "example_user_group1"
    ],
    "query_group": [
      "example_query_group1"
    ],
    "query_concurrency": 7
  },
  {
    "query_concurrency": 5
  }
]
```

El JSON anterior es una matriz de dos objetos, uno para cada cola. El primer objeto define una cola con un grupo de usuarios y un grupo de consultas específicos. También establece el nivel de simultaneidad en 7.

```
{
  "user_group":[
    "example_user_group1"
  ],
  "query_group":[
    "example_query_group1"
  ],
  "query_concurrency":7
}
```

Dado que este ejemplo reemplaza la configuración WLM, esta configuración de JSON también define la cola predeterminada sin un grupo de usuarios o grupo de consultas específico. Establece la simultaneidad en el valor predeterminado: 5.

```
{
  "query_concurrency":5
}
```

Para obtener más información acerca de la administración de cargas de trabajo (WML), consulte [Implementación de Workload Management](#).

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Debe actualizar el código y proporcionar un identificador de clúster.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[CreateAndModifyClusterParameterGroup demonstrates how to
// create and modify an Amazon Redshift parameter group.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterParameterGroup]
// snippet-keyword:[DescribeClusterParameterGroups]
// snippet-keyword:[ModifyClusterParameterGroup]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyClusterParameterGroup.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

import com.amazonaws.services.redshift.model.*;
```

```
public class CreateAndModifyClusterParameterGroup {

    public static AmazonRedshift client;
    public static String clusterParameterGroupName = "parametergroup1";
    public static String clusterIdentifier = "****provide a cluster identifier****";
    public static String parameterGroupFamily = "redshift-1.0";

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            createClusterParameterGroup();
            modifyClusterParameterGroup();
            associateParameterGroupWithCluster();
            describeClusterParameterGroups();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createClusterParameterGroup() {
        CreateClusterParameterGroupRequest request = new
CreateClusterParameterGroupRequest()
            .withDescription("my cluster parameter group")
            .withParameterGroupName(clusterParameterGroupName)
            .withParameterGroupFamily(parameterGroupFamily);
        client.createClusterParameterGroup(request);
        System.out.println("Created cluster parameter group.");
    }

    private static void describeClusterParameterGroups() {
        DescribeClusterParameterGroupsResult result =
client.describeClusterParameterGroups();
        printResultClusterParameterGroups(result);
    }

    private static void modifyClusterParameterGroup() {
        List<Parameter> parameters = new ArrayList<Parameter>();
        parameters.add(new Parameter()
            .withParameterName("extra_float_digits")
            .withParameterValue("2"));
        // Replace WLM configuration. The new configuration defines a queue (in addition to
the default).
        parameters.add(new Parameter()
            .withParameterName("wlm_json_configuration")
            .withParameterValue("[{\"user_group\":\"example_user_group1\"}, {\"query_group\":
[\"example_query_group1\"}, {\"query_concurrency\":7}, {\"query_concurrency\":5}]}]"));

        ModifyClusterParameterGroupRequest request = new
ModifyClusterParameterGroupRequest()
            .withParameterGroupName(clusterParameterGroupName)
            .withParameters(parameters);
        client.modifyClusterParameterGroup(request);
    }

    private static void associateParameterGroupWithCluster() {
        ModifyClusterRequest request = new ModifyClusterRequest()
            .withClusterIdentifier(clusterIdentifier)
            .withClusterParameterGroupName(clusterParameterGroupName);
    }
}
```

```
Cluster result = client.modifyCluster(request);

System.out.format("Parameter Group %s is used for Cluster %s\n",
    clusterParameterGroupName,
    result.getClusterParameterGroups().get(0).getParameterGroupName());
}
private static void
printResultClusterParameterGroups(DescribeClusterParameterGroupsResult result)
{
    if (result == null)
    {
        System.out.println("\nDescribe cluster parameter groups result is null.");
        return;
    }

    System.out.println("\nPrinting parameter group results:\n");
    for (ClusterParameterGroup group : result.getParameterGroups()) {
        System.out.format("\nDescription: %s\n", group.getDescription());
        System.out.format("Group Family Name: %s\n", group.getParameterGroupFamily());
        System.out.format("Group Name: %s\n", group.getParameterGroupName());
        describeClusterParameters(group.getParameterGroupName());
    }
}

private static void describeClusterParameters(String parameterGroupName) {
    DescribeClusterParametersRequest request = new DescribeClusterParametersRequest()
        .withParameterGroupName(parameterGroupName);

    DescribeClusterParametersResult result = client.describeClusterParameters(request);
    printResultClusterParameters(result, parameterGroupName);
}

private static void printResultClusterParameters(DescribeClusterParametersResult
result, String parameterGroupName)
{
    if (result == null)
    {
        System.out.println("\nCluster parameters is null.");
        return;
    }

    System.out.format("\nPrinting cluster parameters for \"%s\"\n",
parameterGroupName);
    for (Parameter parameter : result.getParameters()) {
        System.out.println("  Name: " + parameter.getParameterName() + ", Value: " +
parameter.getParameterValue());
        System.out.println("  DataType: " + parameter.getDataType() + ",
MinEngineVersion: " + parameter.getMinimumEngineVersion());
        System.out.println("  AllowedValues: " + parameter.getAllowedValues() + ",
Source: " + parameter.getSource());
        System.out.println("  IsModifiable: " + parameter.getIsModifiable() + ",
Description: " + parameter.getDescription());
    }
}
}

// snippet-end:[redshift.java.CreateAndModifyClusterParameterGroup.complete]
```

Administración de grupos de parámetros mediante laAWS CLI/API de Amazon Redshift

Puede utilizar las siguientes operaciones de Amazon Redshift en laAWS CLIPara administrar los grupos de parámetros.

- [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](#)

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los grupos de parámetros.

- [CreateClusterParameterGroup](#)
- [DeleteClusterParameterGroup](#)
- [DescribeClusterParameters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeDefaultClusterParameters](#)
- [ModifyClusterParameterGroup](#)
- [ResetClusterParameterGroup](#)

Instantáneas de Amazon Redshift

Temas

- [Overview](#) (p. 238)
- [Instantáneas automatizadas](#) (p. 239)
- [Programación de instantáneas automatizadas](#) (p. 239)
- [Formato de la programación de instantáneas](#) (p. 239)
- [Instantáneas manuales](#) (p. 241)
- [Administración del almacenamiento de instantáneas](#) (p. 241)
- [Exclusión de tablas de instantáneas](#) (p. 242)
- [Copia de instantáneas en otroAWSRegión](#) (p. 242)
- [Restauración de un clúster desde una instantánea](#) (p. 243)
- [Restauración de una tabla a partir de una instantánea](#) (p. 245)
- [Uso compartido de instantáneas](#) (p. 248)
- [Administración de instantáneas mediante la consola](#) (p. 250)
- [Administración de instantáneas mediante la herramientaAWS SDK for Java](#) (p. 265)
- [Administración de instantáneas mediante laAWS CLIAmazon Redshift API y Amazon Redshift](#) (p. 268)

Overview

Las snapshots son backups de un momento determinado de un clúster. Existen dos tipos de instantáneas:AutomatizaciónyManual. Amazon Redshift almacena estas instantáneas internamente en Amazon S3 mediante una conexión de Capa de conexión segura (SSL).

Amazon Redshift realiza instantáneas incrementales automáticamente que hacen un seguimiento de los cambios realizados en el clúster desde la instantánea automatizada anterior. Las instantáneas automatizadas conservan todos los datos requeridos para restaurar un clúster a partir de una instantánea. Puede crear una programación de instantáneas para controlar cuándo se realizan las instantáneas automatizadas o realizar una instantánea manual en cualquier momento.

Cuando restaura a partir de una instantánea, Amazon Redshift crea un nuevo clúster y lo pone a disposición antes de que se carguen todos los datos, de modo que usted pueda empezar a consultar el nuevo clúster de inmediato. El clúster transmite datos bajo demanda desde la instantánea en respuesta a consultas activas, luego carga los datos restantes en un segundo plano.

Al lanzar un clúster, puede establecer el periodo de retención para las instantáneas automatizadas y manuales. Puede cambiar el período de retención predeterminado para las instantáneas automatizadas y manuales modificando el clúster. Puede cambiar el periodo de retención para una instantánea manual en el momento de crear la instantánea o modificando la instantánea.

Puede monitorizar el progreso de las instantáneas consultando los detalles de la propia instantánea en la AWS Management Console o llamando a [describe-cluster-snapshots](#) en la CLI o a la acción de API [DescribeClusterSnapshots](#). Para una instantánea en proceso, estos muestran información como el tamaño de la instantánea incremental, la tasa de transferencia, el tiempo transcurrido y el tiempo restante estimado.

Para garantizar que las copias de seguridad estén disponibles siempre para el clúster, Amazon Redshift almacena instantáneas en un bucket de Amazon S3 de gestión interna que administra Amazon Redshift. Para administrar los cargos de almacenamiento, evalúe la cantidad de días que necesita guardar instantáneas automatizadas y configure su periodo de retención en consecuencia. Elimine las instantáneas

manuales que ya no necesite. Para obtener más información acerca del costo del almacenamiento de backup, consulte la [Precios de Amazon Redshift](#) (Se ha creado el certificado).

Instantáneas automatizadas

Cuando las instantáneas automatizadas están habilitadas para un clúster, Amazon Redshift realiza instantáneas de ese clúster periódicamente. De forma predeterminada, Amazon Redshift realiza una instantánea cada ocho horas o después de cada cambio de datos de 5 GB por nodo, lo que ocurra primero. También puede crear una programación de instantáneas para controlar cuándo se realizan las instantáneas automatizadas. Las instantáneas automatizadas se habilitan de forma predeterminada cuando crea un clúster.

Las instantáneas automatizadas se eliminan cuando finaliza un periodo de retención. El periodo de retención predeterminado es de un día, pero puede modificarlo mediante la consola de Amazon Redshift o mediante programación utilizando la API o CLI de Amazon Redshift.

Para desactivar las instantáneas automatizadas, establezca el periodo de retención en cero. Si desactiva las instantáneas automatizadas, Amazon Redshift deja de tomar instantáneas y elimina cualquier instantánea automatizada ya existente para el clúster. No es posible desactivar las instantáneas automatizadas para tipos de nodos RA3. Puede establecer un periodo de retención automatizado de tipo de nodo RA3 de 1 a 35 días.

Sólo Amazon Redshift puede eliminar una instantánea automatizada; no puede eliminarla manualmente. Amazon Redshift elimina las instantáneas automatizadas al final del periodo de retención, cuando se deshabilitan las instantáneas automatizadas para el clúster o cuando se elimina el clúster. Amazon Redshift conserva la última instantánea automatizada hasta que deshabilite las instantáneas automatizadas o elimine el clúster.

Si desea conservar una instantánea automatizada por un periodo más extenso, puede crear una copia de esta como una instantánea manual. La instantánea automatizada se conserva hasta que expire el periodo de retención, pero la instantánea manual correspondiente se conservará hasta que el usuario la elimine manualmente o hasta el final del periodo de retención.

Programación de instantáneas automatizadas

Para controlar con precisión cuándo se realizan las instantáneas, puede crear una programación de instantáneas y asociarla a uno o varios clústeres. Cuando modifica una programación de instantáneas, esta se modifica para todos los clústeres asociados. Si un clúster no tiene una programación de instantáneas asociada, utiliza la programación de instantáneas automatizadas predeterminada.

Una programación de instantáneas es un conjunto de reglas de programación. Puede definir una regla de programación sencilla basada en un intervalo específico, como cada 8 horas o cada 12 horas. También puede añadir reglas para realizar instantáneas determinados días de la semana, a horas específicas o durante periodos específicos. Las reglas se pueden definir también con expresiones cron de tipo Linux.

Formato de la programación de instantáneas

En la consola de Amazon Redshift, puede crear una programación de instantáneas. A continuación, puede asociar una programación a un clúster para activar la creación de una instantánea del sistema. Una programación se puede asociar con varios clústeres y se pueden crear varias definiciones cron en una programación para activar una instantánea.

Puede definir una programación para sus instantáneas con la sintaxis cron. La definición de estas programaciones utiliza una [cron](#) Sintaxis de. La hora debe especificarse de acuerdo con el [Tiempo universal](#)

coordinado (UTC). Puede crear programaciones con una frecuencia máxima de una hora y una precisión mínima de un minuto.

Las expresiones cron modificadas de Amazon Redshift tienen tres campos obligatorios, que están separados por un espacio en blanco.

Sintaxis

```
cron(Minutes Hours Day-of-week)
```

Campos	Valores	Caracteres comodín
Minutos	0-59	
Hours	0-23	, - * /
Day-of-week	1-7 o SUN-SAT	, - * /

Wildcards

- El carácter comodín , (coma) incluye valores adicionales. En el campo `Day-of-week`, `MON, WED, FRI` incluiría lunes, miércoles y viernes. El total de valores está limitado a 24 por campo.
- El - (guion) especifica intervalos. En el navegador `Hour` campo, 1-15 incluiría las horas 1 a 15 del día especificado.
- El * (asterisco) incluye todos los valores del campo. En el campo `Hours`, * incluiría cada hora.
- El comodín / (barra inclinada) especifica incrementos. En el campo `Hours`, puede escribir `1/10` para especificar cada 10 horas, empezando por la primera hora del día (por ejemplo, 01:00, 11:00 y 21:00).

Limits

- No se admiten las programaciones de instantáneas que producen frecuencias de copia de seguridad de menos de una hora o de más de 24 horas. Si tiene programaciones solapadas que programan instantáneas en un periodo de una hora, se produce un error de validación.

Cuando cree una programación, puede utilizar las siguientes cadenas Cron de ejemplo.

Minutos	Hours	Día de la semana	Significado			
0	14-20/1	TUE	Cada hora entre las dos y las ocho de la tarde del martes.			
0	21	MON-FRI	Todas las noches a las 21:00 de lunes a viernes.			
30	0/6	SAT-SUN	Cada seis horas el sábado y el domingo empezando 30 minutos después de la medianoche (00:30) de ese día. Esto produce una instantánea a las			

Minutos	Hours	Día de la semana	Significado			
			[00:30, 06:30, 12:30 y 18:30] todos los días.			
30	12/4	*	Cada cuatro horas a partir de las 12:30 todos los días. Esto se resuelve en [12:30, 16:30, 20:30].			

Por ejemplo, para ejecutar una programación diaria cada dos horas empezando a las 15:15 (lo que se resuelve en [15:15, 17:15, 19:15, 21:15, 23:15]), especifique:

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

Puede crear varias definiciones de programación cron en una programación. Por ejemplo, el siguiente comando de la AWS CLI contiene dos programaciones cron en una sola programación.

```
create-snapshot-schedule --schedule-identifier "my-test" --schedule-definition "cron(0 17 SAT,SUN)" "cron(0 9,17 MON-FRI)"
```

Instantáneas manuales

También puede tomar una instantánea manual en cualquier momento. De forma predeterminada, las instantáneas manuales se conservarán de forma indefinida incluso después de que elimine el clúster. Puede especificar el periodo de retención en el momento de crear una instantánea manual o puede cambiar el periodo de retención modificando la instantánea. Para obtener más información acerca del cambio del periodo de retención, consulte [Cambiar el periodo de retención de instantáneas manuales](#) (p. 254).

Si se elimina una instantánea, no puede comenzar ninguna operación nueva que haga referencia a esa instantánea. Sin embargo, si hay una operación de restauración en proceso, esta se ejecutará hasta su finalización.

Amazon Redshift tiene una cuota que limita el número total de instantáneas manuales que el usuario puede crear; esta cuota se aplica porAWSPor cuentaAWSRegión . La cuota predeterminada se muestra en [Cuotas y límites de Amazon Redshift](#) (p. 494).

Administración del almacenamiento de instantáneas

Dado que las instantáneas acumulan cargos de almacenamiento, es importante que las elimine si ya no las necesita. Amazon Redshift elimina las instantáneas automatizadas y manuales al final de sus respectivos periodos de retención. También puede eliminar instantáneas manuales utilizando la herramientaAWS Management Consoleo con el [instantáneas por lotes eliminte-cluster-shots](#)Comando de la CLI.

Puede cambiar el periodo de retención para una instantánea manual modificando la configuración de la instantánea manual.

Para obtener información sobre la cantidad de almacenamiento que consumen las instantáneas, use la consola de Amazon Redshift o el [Describe-storage](#)Comando de la CLI.

Exclusión de tablas de instantáneas

De forma predeterminada, todas las tablas permanentes definidas por el usuario se incluyen en las instantáneas. Si no es necesario crear un backup para una tabla, como una tabla provisional, puede reducir de forma significativa el tiempo necesario para crear instantáneas y restaurar a partir de instantáneas. También se reduce el espacio de almacenamiento en Amazon S3 mediante el uso de una tabla sin backup. Para crear una tabla sin backup, incluya el parámetro `BACKUP NO` cuando cree la tabla. Para obtener más información, consulte [CREAR TABLAS](#) y [CREAR TABLAS COMO](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Copia de instantáneas en otroAWSRegión

Puede configurar Amazon Redshift para que copie automáticamente las instantáneas (manuales o automatizadas) de un clúster a otroAWSRegión. Cuando se crea una instantánea en el clúster principal deAWSRegión, se copia en unAWSRegión. Los dosAWSLas regiones se conocen respectivamente comoorigenAWSRegiónydestinationAWSRegión. Si almacena una copia de sus instantáneas en otroAWSEn la región, puede restaurar el clúster a partir de datos recientes si algo afecta laAWSRegión. Puede configurar el clúster para que copie las instantáneas únicamente en un destinoAWSRegión a la vez. Para obtener una lista de las regiones de Amazon Redshift, consulte [Regiones y puntos de enlace](#) en laReferencia general de Amazon Web Services.

Cuando habilita Amazon Redshift para copiar instantáneas automáticamente en otroAWSRegión, se especifica el destinoAWSRegión en la que se copiarán las instantáneas. Para las instantáneas automatizadas, también puede especificar el período de retención para mantenerlas en el destinoAWSRegión. Después de copiar una instantánea automatizada en el destinoAWSRegión y alcanza el periodo de retención allí, se elimina del destinoAWSRegión. De este modo, el uso de instantáneas se mantiene en niveles bajos. Para guardar las instantáneas durante un periodo más largo o más corto en el destinoAWSRegión, cambie este período de retención.

El período de retención que establezca para las instantáneas automatizadas que se copian en el destinoAWSLa región es independiente del período de retención para las instantáneas automatizadas en el origenAWSRegión. El período de retención predeterminado para las copias de instantáneas es de siete días. Ese período de siete días solo se aplica a las instantáneas automatizadas. Tanto en el origen como en el destino deAWSRegiones, instantáneas manuales se eliminan al final del periodo de retención o cuando se suprimen manualmente.

Puede desactivar la copia de instantánea automática de un clúster en cualquier momento. Cuando deshabilita esta función, las instantáneas dejarán de copiarse desde el origenAWSRegión hasta el destinoAWSRegión. Todas las instantáneas automatizadas copiadas en el destinoAWSLas regiones se eliminan cuando alcanzan el límite del periodo de retención, a menos que el usuario cree copias manuales de ellas. Estas instantáneas manuales y cualquier instantánea manual que se haya copiado desde el destinoAWSRegión, se mantienen en el destinoAWSRegistrar hasta que los elimine manualmente.

Para cambiar el destinoAWSRegión en la que copia las instantáneas, deshabilite primero la función de copia automática. Luego, habilítela de nuevo especificando el nuevo destinoAWSRegión.

Después de copiar una instantánea en el destinoAWSRegión, se activa y está disponible para fines de restauración.

Para copiar instantáneas deAWS KMS—clústeres cifrados en otroAWSRegión, cree una autorización para que Amazon Redshift pueda utilizar una clave maestra de cliente (CMK) de KMS en el destinoAWSRegión. A continuación, seleccione esa autorización cuando habilite la copia de instantáneas en el origenAWSRegión. Para obtener más información acerca de la configuración de autorizaciones para copiar instantáneas, consulte [CopiarAWS KMS—instantáneas cifradas en otroAWSRegión \(p. 287\)](#).

Restauración de un clúster desde una instantánea

Las instantáneas contienen datos de las bases de datos que se ejecutan en el clúster. También contienen información sobre el clúster, como el número de nodos, el tipo de nodos y el nombre de usuario maestro. Si restaura el clúster a partir de una instantánea, Amazon Redshift utilizará la información del clúster para crear otro nuevo. Después, restaurará todas las bases de datos a partir de la información de la instantánea.

En el clúster que se crea a partir de la instantánea original, puede seleccionar la configuración, como el tipo y el número de nodos. El clúster se restaura en el mismo AWS Región y una zona de disponibilidad elegida aleatoriamente por el sistema, a menos que el usuario especifique otra zona de disponibilidad en la solicitud. Cuando se restaura un clúster a partir de una instantánea, se puede elegir una pista de mantenimiento compatible para el nuevo clúster.

Note

Cuando se restaura una instantánea en un clúster con una configuración diferente, la instantánea debe haberse tomado de un clúster con la versión 1.0.10013 u otra posterior.

Cuando una restauración está en curso, los eventos se emiten normalmente en el siguiente orden:

1. `RESTORE_STARTED` — `REDSHIFT-EVENT-2008` enviado cuando comienza el proceso de restauración.
2. `RESTORE_SUCETIFIED` — `REDSHIFT-EVENT-3003` se envía cuando se ha creado el nuevo clúster.

El clúster está disponible para consultas.

3. `DATA_TRANSFER_COMPLETED` — `REDSHIFT-EVENT-3537` se envía cuando se completa la transferencia de datos.

Note

Los clústeres RA3 sólo emiten eventos `RESTORE_STARTED` y `RESTORE_SUCETIFIED`. No hay ninguna transferencia explícita de datos que se realice después de que un `RESTORE` tenga éxito, ya que los tipos de nodo RA3 almacenan datos en el almacenamiento gestionado de Amazon Redshift. Con los nodos RA3, los datos se transfieren continuamente entre los nodos RA3 y el almacenamiento gestionado por Amazon Redshift como parte del procesamiento normal de consultas. Los nodos RA3 almacenan en caché los datos calientes localmente y mantienen automáticamente los bloques consultados con menos frecuencia en el almacenamiento gestionado por Amazon Redshift.

Puede monitorizar el progreso de las restauraciones llamando a la acción [DescribeClusters](#) de la API o consultando los detalles del clúster en la AWS Management Console. Para una restauración en proceso, estos muestran información como el tamaño de los datos de la instantánea, la tasa de transferencia, el tiempo transcurrido y el tiempo restante estimado. Para ver una descripción de estas métricas, visite [RestoreStatus](#).

No puede utilizar una instantánea para que un clúster activo vuelva a un estado anterior.

Note

Cuando restaura una instantánea en un clúster nuevo, se usan los grupos de parámetros y de seguridad predeterminados, a menos que especifique valores diferentes.

Es posible que quiera restaurar una instantánea en un clúster con una configuración diferente por las siguientes razones:

- Si un clúster se compone de tipos de nodos más pequeños y desea consolidarlos en un tipo de nodo más grande para que tenga menos nodos.

- Si ha monitorizado la carga de trabajo y ha determinado que es necesario cambiar a un tipo de nodo con más CPU y más almacenamiento.
- Si desea medir el rendimiento de cargas de trabajo de prueba con diferentes tipos de nodos.

La restauración tiene las siguientes restricciones:

- La configuración del nuevo nodo debe tener suficiente almacenamiento para los datos existentes. Incluso cuando se añaden nodos, es posible que la nueva configuración no disponga de suficiente almacenamiento por la forma en que se han redistribuido los datos.
- La operación de restauración comprueba si la instantánea se creó en una versión de clúster compatible con la versión de clúster del nuevo clúster. Si el nuevo clúster tiene un nivel de versión demasiado pronto, se produce un error en la operación de restauración e informa más información en un mensaje de error.
- Las configuraciones posibles (número de nodos y tipo de nodo) a las que puede restaurar están determinadas por el número de nodos del clúster original y el tipo de nodo de destino del nuevo clúster. Para determinar las posibles configuraciones disponibles, puede usar la consola de Amazon Redshift o `aws redshift describe-node-configuration-options` AWS CLI Command con `action-type restore-cluster`. Para obtener más información acerca cómo restaurar mediante la consola de Amazon Redshift, consulte [Restauración de un clúster desde una instantánea \(p. 258\)](#).

En el siguiente procedimiento, se toma un clúster con muchos nodos y se consolida en un tipo de nodo mayor con menos nodos utilizando la AWS CLI. En este ejemplo, empezaremos con un clúster de origen de 24 nodos `ds2.xlarge`. En este caso, supongamos que ya se ha creado una instantánea de este clúster y que queremos restaurarlo en un tipo de nodo más grande.

1. Ejecute el siguiente comando para obtener los detalles de un clúster `ds2.xlarge` de 24 nodos.

```
aws redshift describe-clusters --region eu-west-1 --cluster-identifier
mycluster-123456789012
```

2. Ejecute el siguiente comando para obtener los detalles de una instantánea.

```
aws redshift describe-cluster-snapshots --region eu-west-1 --snapshot-identifier
mycluster-snapshot
```

3. Ejecute el siguiente comando para describir las opciones disponibles en esta instantánea.

```
aws redshift describe-node-configuration-options --snapshot-identifier mycluster-snapshot
--region eu-west-1 --action-type restore-cluster
```

Este comando devuelve una lista de opciones con recomendaciones sobre los tipos de nodos, el número de nodos y el uso de disco de cada opción. En este ejemplo, el comando anterior muestra las siguientes configuraciones de nodos posibles. Hemos decidido realizar la restauración en un clúster `ds2.8xlarge` de tres nodos.

```
{
  "NodeConfigurationOptionList": [
    {
      "EstimatedDiskUtilizationPercent": 65.26134808858235,
      "NodeType": "ds2.xlarge",
      "NumberOfNodes": 24
    },
    {
      "EstimatedDiskUtilizationPercent": 32.630674044291176,
      "NodeType": "ds2.xlarge",
      "NumberOfNodes": 48
    }
  ]
}
```

```
    },
    {
      "EstimatedDiskUtilizationPercent": 65.26134808858235,
      "NodeType": "ds2.8xlarge",
      "NumberOfNodes": 3
    },
    {
      "EstimatedDiskUtilizationPercent": 48.94601106643677,
      "NodeType": "ds2.8xlarge",
      "NumberOfNodes": 4
    },
    {
      "EstimatedDiskUtilizationPercent": 39.156808853149414,
      "NodeType": "ds2.8xlarge",
      "NumberOfNodes": 5
    },
    {
      "EstimatedDiskUtilizationPercent": 32.630674044291176,
      "NodeType": "ds2.8xlarge",
      "NumberOfNodes": 6
    }
  ]
}
```

4. Ejecute el comando siguiente para restaurar la instantánea con la configuración de clúster elegida. Una vez restaurado el clúster, tenemos el mismo contenido que el clúster de origen, pero los datos se han consolidado en tres nodos ds2.8xlarge.

```
aws redshift restore-from-cluster-snapshot --region eu-west-1 --snapshot-identifier
mycluster-snapshot --cluster-identifier mycluster-123456789012-x --node-type ds2.8xlarge
--number-of-nodes 3
```

Restauración de una tabla a partir de una instantánea

Puede restaurar una tabla individual a partir de una instantánea, en lugar de restaurar todo un clúster. Cuando restaure una tabla individual a partir de una instantánea, especifique la instantánea de origen, la base de datos, el esquema y el nombre de la tabla, como también, el clúster de destino, el esquema y un nuevo nombre de tabla para la tabla restaurada.

El nuevo nombre de la tabla no puede ser el nombre de una tabla ya existente. Para sustituir una tabla existente por una tabla restaurada a partir de una instantánea, cambie el nombre o elimine la tabla ya existente antes de restaurar la tabla desde la instantánea.

La tabla de destino se crea utilizando las definiciones de columnas, los atributos de tabla y los atributos de columna de la tabla de origen, a excepción de las claves externas. Para evitar conflictos de dependencias, la tabla de destino no hereda las claves externas de la tabla de origen. Cualquier dependencia, como vistas o permisos concedidos en la tabla de origen, no aplica a la tabla de destino.

Si el propietario de la tabla de origen existe, ese usuario es el propietario de la tabla restaurada, dado que el usuario tiene los permisos suficientes para volverse el propietario de una relación en la base de datos y el esquema especificados. De lo contrario, la tabla restaurada es propiedad del usuario maestro que se creó cuando se lanzó el clúster.

La tabla restaurada vuelve al estado en el que estaba en el momento que se realizó el backup. Esto incluye las reglas de visibilidad de transacciones definidas por la adhesión de Amazon Redshift [a aislamiento serializable](#), lo que significa que los datos estarán visibles de inmediato para las transacciones en tránsito que se inicien después de la copia de seguridad.

La restauración de una tabla a partir de una instantánea tiene las siguientes limitaciones:

- Puede restaurar una tabla únicamente para el clúster actual en ejecución activa y a partir de una instantánea que se haya tomado de ese clúster.
- Puede restaurar solo una tabla a la vez.
- No puede restaurar una tabla a partir de una instantánea de clúster que haya sido tomada antes de que se cambie el tamaño del clúster.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

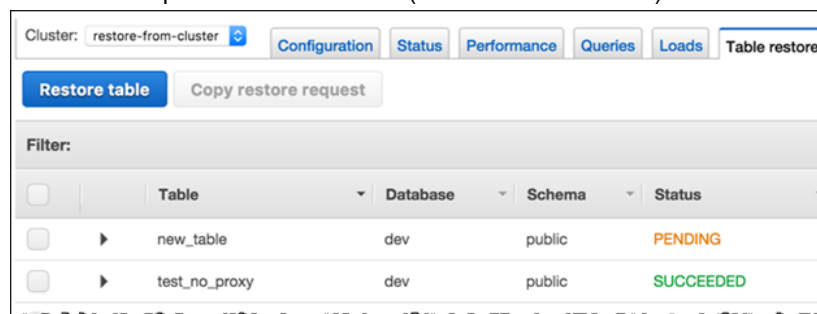
Restauración de una tabla a partir de una instantánea

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y seleccione el clúster que quiere utilizar para restaurar una tabla.
3. Para Actions (Acciones), seleccione Restore table (Restaurar tabla) para mostrar la página Restore table (Restaurar tabla).
4. Introduzca la información sobre qué instantánea, tabla de origen y tabla de destino usar, y luego seleccione Restore table (Restaurar tabla).

Consola original

Restauración de una tabla a partir de una instantánea con la consola de Amazon Redshift

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. Elija Cluster y seleccione un clúster.
3. Seleccione la pestaña Table restore (Restauración de tabla).



4. Seleccione Restore table (Restaurar tabla).
5. En el panel Table restore (Restauración de tabla), seleccione un intervalo de fechas que contenga la instantánea del clúster desde la que desea restaurar los datos. Por ejemplo, puede seleccionar Last 1 week para las instantáneas de clúster tomadas en la semana anterior.
6. Añada la información siguiente:

- A partir de snapshot— identificador de la instantánea del clúster que contiene la tabla desde la que se va a restaurar.
- Source table to restore from (Tabla de origen de la restauración)
 - Base de datos— nombre de la base de datos de la instantánea del clúster que contiene la tabla desde la que se va a restaurar.
 - Esquema— nombre del esquema de la base de datos de la instantánea del clúster que contiene la tabla desde la que se va a restaurar.
 - Tabla— nombre de la tabla de la instantánea del clúster desde la que se va a restaurar.
- Target table to restore to (Tabla de destino de la restauración)
 - Base de datos— nombre de la base de datos del clúster de destino en el que se va a restaurar la tabla.
 - Esquema— nombre del esquema de la base de datos del clúster de destino donde se va a restaurar la tabla.
 - Nombre nuevo de tabla— Nuevo nombre de la tabla restaurada. Este nombre no puede ser el nombre de una tabla ya existente en la base de datos de destino.

Table Level Restore X

Restore a table to cluster: restore-from-cluster

Select from snapshots in time range: Last 1 Week

From snapshot:* to-restore

Source table to restore from

Database:*

Schema:*

Table:*

Target table to restore to

Database:*

Schema:*

New table name: *

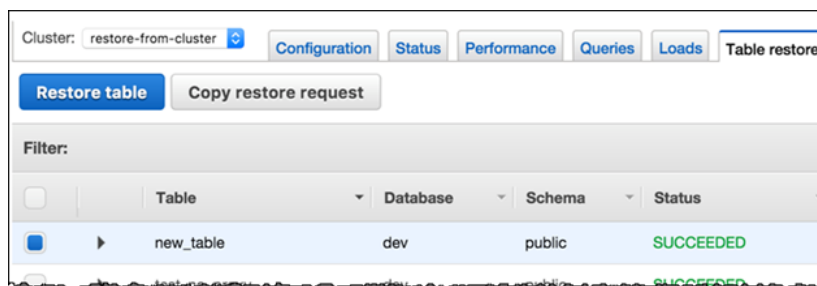
Cancel Restore

7. Seleccione Restore (Restaurar) para restaurar la tabla.

Si ha restaurado al menos una tabla a partir de una instantánea de clúster, puede copiar los valores de una solicitud de restauración de tabla anterior en la nueva solicitud de restauración de tabla. De esta forma, no tiene que volver a escribir valores que serán los mismos para varias operaciones de restauración de tablas.

Copia de una solicitud de restauración de tabla anterior a una nueva operación de restauración de tabla:

1. En la pestaña Table restore (Restauración de tabla), seleccione un estado de restauración de tabla existente.



2. Seleccione Copy restore request (Copiar solicitud de restauración).

Example Ejemplo: Restauración de una tabla a partir de una instantánea con laAWS CLI

En el siguiente ejemplo se utiliza el comando `restore-table-from-cluster-snapshot` de la AWS CLI para restaurar la tabla `my-source-table` desde el esquema `sample-database` en la `my-snapshot-id`. En el ejemplo se restaura la instantánea al clúster `mycluster-example` con un nombre de tabla nuevo de `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
--source-database-name sample-database
--source-table-name my-source-table
```

Uso compartido de instantáneas

Puede compartir una instantánea manual ya existente con otrosAWSAutorizando el acceso a la instantánea. Puede autorizar hasta el 20 de cada instantánea y el 100 de cada clave de AWS Key Management Service (AWS KMS). Es decir, si tiene 10 instantáneas que están cifradas con una sola clave de KMS, puede autorizar a 10AWSPara restaurar cada instantánea u otras combinaciones que sumen hasta 100 cuentas y no excedan las 20 cuentas por cada instantánea. Una persona que haya iniciado sesión como usuario en una de las cuentas autorizadas podrá describir la instantánea o restaurarla para crear un nuevo clúster de Amazon Redshift en su cuenta. Por ejemplo, si utiliza cuentas de clientes de AWS independientes para pruebas y producción, un usuario puede iniciar sesión con la cuenta de producción y compartir una instantánea con usuarios de la cuenta de pruebas. Alguien que haya iniciado sesión como usuario de la cuenta de pruebas puede restaurar la instantánea para crear un clúster nuevo que sea propiedad de la cuenta de pruebas para realizar pruebas y diagnósticos.

Una instantánea manual es propiedad permanente de la cuenta de cliente de AWS con la que fue creada. Solo los usuarios de la cuenta propietaria de la instantánea pueden autorizar a otras cuentas a obtener acceso a la instantánea o a revocar autorizaciones. Los usuarios de las cuentas autorizadas solo pueden describir o restaurar cualquier instantánea que se haya compartido con ellos; no pueden copiar o eliminar instantáneas que se hayan compartido con ellos. Una autorización permanece en vigor hasta que el propietario de la instantánea la revoque. Si se revoca una autorización, el usuario anteriormente autorizado pierde la visibilidad de la instantánea y no podrá lanzar ninguna acción nueva que haga referencia a la instantánea. Si la cuenta está en el proceso de restauración de la instantánea cuando se revoca el acceso, la restauración se ejecuta hasta finalizarse. No puede eliminar una instantánea mientras tenga autorizaciones activas, primero debe revocar todas las autorizaciones.

Las cuentas de clientes de AWS están autorizados de forma permanente a obtener acceso a las instantáneas propiedad de la cuenta. Los intentos de autorizar o revocar el acceso a la cuenta del

propietario recibirán un error. No puede restaurar o describir una instantánea que sea propiedad de una cuenta de cliente de AWS inactiva.

Después de haber autorizado el acceso a unAWS, ningún usuario de IAM de esa cuenta podrá realizar acciones en la instantánea a menos que tengan políticas de IAM que les permitan hacerlo.

- Los usuarios de IAM de la cuenta del propietario de la instantánea pueden autorizar y revocar el acceso a una instantánea solo si tienen una política de IAM que les permita realizar esas acciones con una especificación de recursos que incluya la instantánea. Por ejemplo, la siguiente política permite a un usuario de la cuenta 012345678912 de AWS autorizar a otras cuentas para que obtengan acceso a la instantánea `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"
      ]
    }
  ]
}
```

- Usuarios de IAM en unaAWSLa cuenta con la que se ha compartido una instantánea no puede realizar acciones en esa instantánea a menos que tengan políticas de IAM que lo permitan:
- Para enumerar o describir una instantánea, deben tener una política de IAM que permita la acción `DescribeClusterSnapshots`. En el siguiente código se muestra un ejemplo:

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

- Para restaurar una instantánea, los usuarios deben tener una política de IAM que permita la acción `RestoreFromClusterSnapshot` y tenga un elemento de recursos que abarque el clúster que están intentando crear y la instantánea. Por ejemplo, si un usuario de la cuenta 012345678912 ha compartido la instantánea `my-snapshot20130829` con la cuenta 219876543210, para crear un clúster mediante la restauración de la instantánea, un usuario de la cuenta 219876543210 debe tener una política como la siguiente:

```
{
  "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"
      ]
    }
  ]
}
```

- Después de revocar el acceso a una instantánea desde una cuenta AWS, ningún usuario de esa cuenta puede acceder a la instantánea. Esto es así incluso si tienen políticas de IAM que permiten acciones en el recurso de instantánea previamente compartido.

Administración de instantáneas mediante la consola

Amazon Redshift toma instantáneas automáticas e incrementales de los datos de forma periódica y las guarda en Amazon S3. Además, puede tomar snapshots manuales de sus datos cada vez que lo desee. En esta sección, se explica cómo administrar instantáneas desde la consola de Amazon Redshift. Para obtener más información acerca de las instantáneas, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

Todas las tareas de snapshots de la consola de Amazon Redshift parten de la lista de snapshots. Puede filtrar la lista utilizando un intervalo de tiempo, el tipo de instantánea y el clúster asociado con la instantánea. Además, puede ordenar la lista por fecha, tamaño y tipo de instantánea. Según el tipo de instantánea que haya seleccionado, puede que tenga diferentes opciones disponibles para trabajar con la instantánea.

Temas

- [Creación de una programación de instantáneas \(p. 250\)](#)
- [Creación de una instantánea manual \(p. 252\)](#)
- [Cambiar el periodo de retención de instantáneas manuales \(p. 254\)](#)
- [Eliminación de instantáneas manuales \(p. 255\)](#)
- [Copia de una instantánea automatizada \(p. 256\)](#)
- [Restauración de un clúster desde una instantánea \(p. 258\)](#)
- [Compartir una instantánea de un clúster \(p. 260\)](#)
- [Configuración de la copia de una instantánea entre regiones para un clúster no cifrado \(p. 262\)](#)
- [Configuración de la copia de una instantánea entre regiones para unAWS KMS—clúster cifrado \(p. 263\)](#)
- [Modificación del período de retención para una copia de instantáneas entre regiones \(p. 264\)](#)

Creación de una programación de instantáneas

Para controlar con precisión cuándo se realizan las instantáneas, puede crear una programación de instantáneas y asociarla a uno o varios clústeres. Puede asociar una programación cuando cree un clúster o modificando el clúster. Para obtener más información, consulte [Programación de instantáneas automatizadas \(p. 239\)](#).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una programación de instantáneas

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), y después seleccione la pestaña Snapshot schedules (Horarios de instantáneas). Se muestran los horarios de las instantáneas.
3. Seleccione Add schedule (Añadir horario) para mostrar la página para añadir un horario.
4. Introduzca las propiedades de la definición de programación, luego seleccione Add schedule (Añadir horario).
5. En la página que aparece, puede adjuntar clústeres a su nuevo horario de instantáneas, luego seleccione OK.

Consola original

Para crear una programación de instantáneas

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija Snapshot Schedules (Programaciones de instantáneas).
4. Elija Add Schedule (Añadir programación).
5. En When do you want to take automated snapshots? (¿Cuándo desea realizar instantáneas automatizadas?) elija Configure custom automated snapshot rules (Configurar reglas de instantáneas automatizadas personalizadas) y añada una o varias reglas. También puede elegir Take a snapshot every 8 hours (Realizar una instantánea cada 8 horas) y especificar el número de horas.
6. Elija Select a snapshot rule to add (Seleccionar la regla de instantánea que se va a añadir) y elija una plantilla de regla de la lista. Puede agregar varias reglas.
7. Modifique los campos de la plantilla para personalizar la programación.

When do you want the automated snapshots to be taken?

☐ Take a snapshot every hour(s)

☒ Configure custom automated snapshot rules

Automated snapshot rules

Select a snapshot rule to add

RULE:

SELECT THE DAYS TO TAKE A SNAPSHOT ON: ☒ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

SPECIFY HOW MANY SNAPSHOTS TO TAKE:

☐ Take one snapshot at : UTC Add another time

☒ Take a snapshot every hours from : to : UTC Add another time

8. Para ver la programación, elija Preview schedule for all rules (Vista previa de la programación de todas las reglas).
9. Elija Add Schedule (Añadir programación).

Creación de una instantánea manual

Puede crear una snapshot manual de un clúster desde la lista de snapshots de la siguiente manera. O bien puede tomar una snapshots de un clúster en el panel de configuración del clúster. Para obtener más información, consulte [Crear una instantánea de un clúster](#) (p. 69).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una instantánea manual

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), y después seleccione Create snapshot (Crear instantánea). Se muestra la página de instantáneas para crear una instantánea manual.
3. Introduzca las propiedades de la definición de instantánea, luego seleccione Create snapshot (Crear instantánea). La instantánea puede tardar un poco en estar disponible.

Consola original

Para crear una instantánea manual

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Elija Create Snapshot (Crear instantánea).
4. En el cuadro de diálogo Create Snapshot (Crear instantánea), haga lo siguiente:
 - a. En el cuadro Cluster Identifier (Identificador del clúster), seleccione el clúster del que desea realizar una instantánea.
 - b. En el cuadro Snapshot Identifier (Identificador de instantáneas), escriba un nombre para la instantánea.
 - c. Para Snapshot retention period (Periodo de retención de instantáneas), escriba el número de días para conservar la instantánea. Para conservar la instantánea de forma indefinida, escriba -1.

Create Snapshot

Choose a cluster and provide a snapshot identifier.

Cluster identifier example-cluster

Snapshot identifier*

Snapshot retention period days

Note: it may take several minutes for the newly created snapshot to appear on your account.

[Cancel](#) [Create](#)

5. Seleccione Create (Crear).

La snapshot podría tardar un tiempo en completarse. La nueva instantánea se muestra en la lista de instantáneas con su estado actual. En el siguiente ejemplo, se muestra que `snapshot-example` se está creando.

[Create Snapshot](#) [Actions](#)

Filter: Last 2 Weeks ▾ all ▾ All Clusters ▾

Sort by: Most recent ▾

☐	Snapshot Identifier ▾	Cluster Identifier ▾	Status ▾	Type ▾	Total Size
	snapshot-example	example-cluster	creating	manual	-1 MB

Snapshot Properties

Snapshot Identifier	snapshot-example
Snapshot Type	manual
Snapshot Status	creating
Snapshot Create Time	November 30, 2018 at 2:47:49 PM UTC-8
Encrypted	No

Cluster Details

Cluster identifier	example-cluster
Cluster version	1.0
Node Type	dc1.large
Number of nodes	2
Availability zone	us-west-2a
Master username	postgres
Cluster create time	August 28, 2018 at 12:08:52 PM UTC-8
VPC	

Access Configuration

Owner account ID	██████████ (this account)
Accounts With Restore Access	None

Backup Details

Total Backup Size	Unknown
Incremental Backup Size	Unknown
Progress	0%
Current Size	0.00 MB
Backup Rate	0.00 MB/s
Time taken	Unknown
Estimated Time to Completion	Unknown

Cambiar el periodo de retención de instantáneas manuales

Puede cambiar el periodo de retención para una instantánea manual modificando la configuración de la instantánea.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

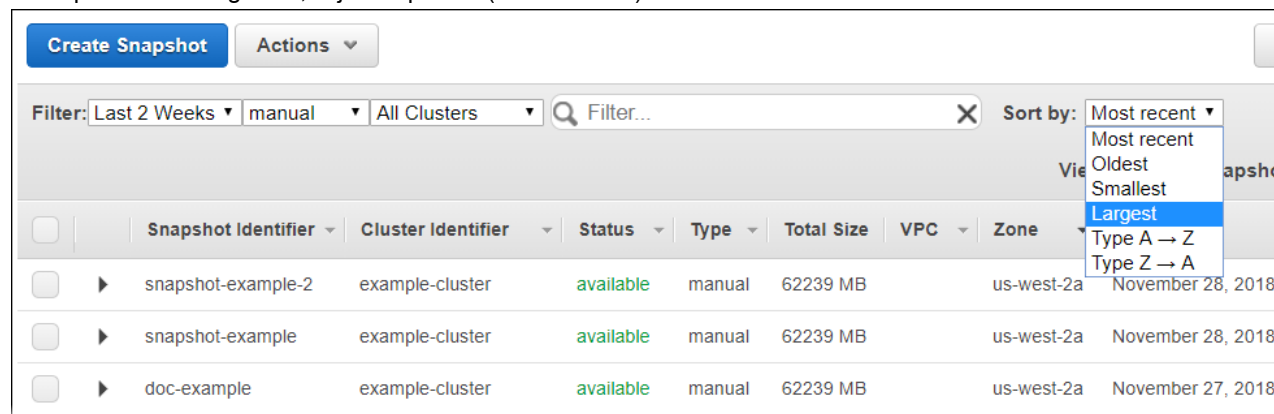
Para cambiar el periodo de retención de instantáneas manuales

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), luego seleccione la instantánea manual para cambiar.
3. Para Actions (Acciones), seleccione Manual snapshot settings (Configuración de instantáneas manuales) para mostrar las propiedades de la instantánea manual.
4. Introduzca las propiedades editadas de la definición de instantánea, luego seleccione Save (Guardar).

Consola original

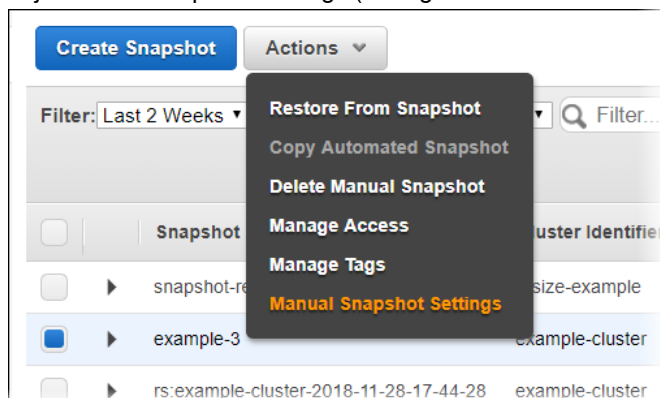
Para cambiar el periodo de retención de instantáneas manuales

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).

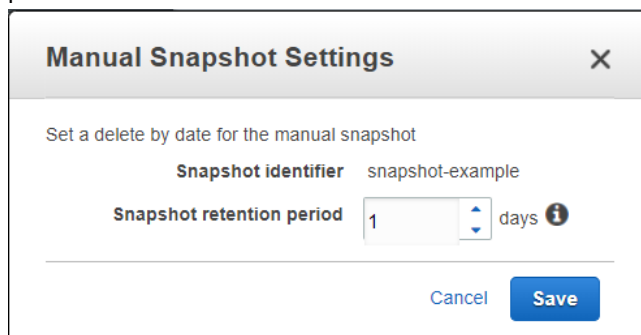


3. Para filtrar la lista con el fin de encontrar la instantánea que desea copiar, realice alguna de las acciones a continuación:
 - En el cuadro Time Range (Intervalo de tiempo), elija un intervalo de tiempo para acotar su búsqueda de forma adecuada.
 - En el cuadro Type (Tipo), elija manual.
 - En el cuadro Cluster, elija el nombre de un clúster para enumerar instantáneas para un único clúster, o elija All Clusters (Todos los clústeres) para enumerar instantáneas de todos los clústeres.

- En el campo Sort by (Ordenar por), elija cómo desea ordenar la lista.
4. En la lista de instantáneas, seleccione la instantánea que desea modificar.
 5. Elija Manual Snapshot Settings (Configuración de la instantánea manual).



6. Para Snapshot retention period (Periodo de retención de instantáneas), escriba el número de días para conservar la instantánea. Para conservar la instantánea de forma indefinida, escriba -1.



7. Elija Save (Guardar).

Eliminación de instantáneas manuales

Para eliminar instantáneas manuales, seleccione una o más instantáneas en la lista de instantáneas.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

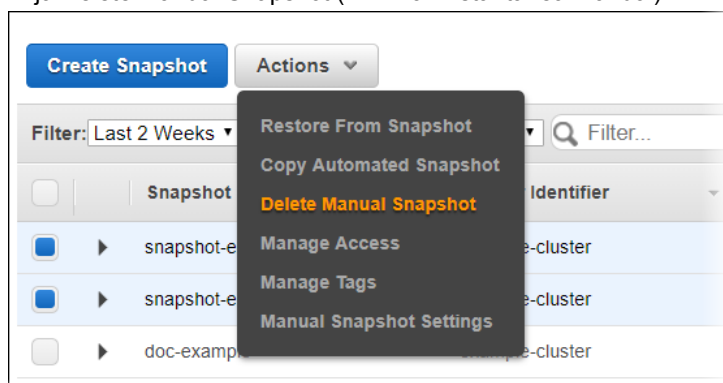
Pasos para eliminar una snapshot manual

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), y después seleccione la instantánea que desee borrar.
3. Para Actions (Acciones), seleccione Delete snapshot (Borrar instantánea) para borrar la instantánea.
4. Confirme la eliminación de las instantáneas enumeradas, luego seleccione Delete (Eliminar).

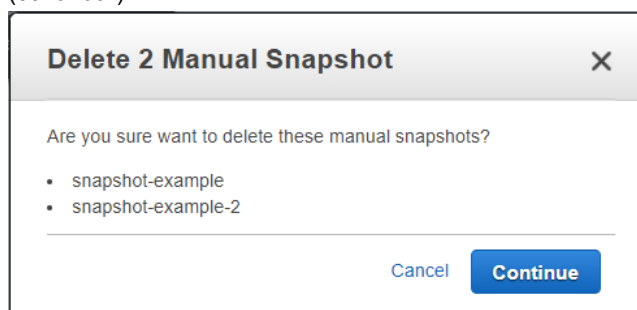
Consola original

Pasos para eliminar una snapshot manual

1. Inicie sesión en la en.AWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Para filtrar la lista, realice alguna de las acciones a continuación:
 - En el cuadro Time Range (Intervalo de tiempo), elija un intervalo de tiempo para acotar su búsqueda de forma adecuada.
 - En el cuadro Type (Tipo), elija manual.
 - En el cuadro Cluster, elija el nombre de un clúster para enumerar instantáneas para un único clúster, o elija All Clusters (Todos los clústeres) para enumerar instantáneas de todos los clústeres.
 - En el campo Sort by (Ordenar por), elija cómo desea ordenar la lista.
4. En la lista de instantáneas, seleccione las filas que contienen las instantáneas que desea eliminar.
5. Elija Delete Manual Snapshot (Eliminar instantánea manual).



6. En el cuadro de diálogo Delete Manual Snapshot (Eliminar instantánea manual), elija Continue (continuar).



Copia de una instantánea automatizada

Las snapshots automatizadas se eliminan de forma automática cuando expira el período de retención, cuando el usuario deshabilita la opción de snapshots automatizadas o cuando elimina un clúster. Si desea conservar una snapshot automatizada, puede copiarla a una snapshot manual.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

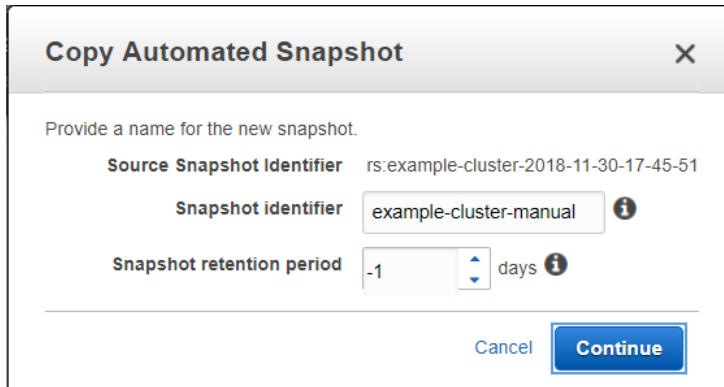
Pasos para copiar una snapshot automatizada

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), y después seleccione la instantánea que desee copiar.
3. Para Actions (Acciones), seleccione Copy automated snapshot (Copiar instantánea automática) para copiar la instantánea.
4. Actualice las propiedades de la nueva instantánea, luego seleccione Copy (Copiar).

Consola original

Pasos para copiar una snapshot automatizada

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Para filtrar la lista, realice alguna de las acciones a continuación:
 - En el cuadro Time Range (Intervalo de tiempo), elija un intervalo de tiempo para acotar su búsqueda de forma adecuada.
 - En el cuadro Type (Tipo), elija automated (automatizada).
 - En el cuadro Cluster, elija el nombre de un clúster para enumerar instantáneas para un único clúster, o elija All Clusters (Todos los clústeres) para enumerar instantáneas de todos los clústeres.
 - En el campo Sort by (Ordenar por), elija cómo desea ordenar la lista.
4. En la lista de instantáneas, seleccione la instantánea que desea copiar.
5. Elija Copy Automated Snapshot (Copiar instantánea automatizada).
6. En el cuadro Snapshot Identifier (Identificador de instantáneas) del cuadro de diálogo Copy Automated Snapshot (Copiar instantánea automatizada), escriba un nombre para la copia de la instantánea.
7. Para Snapshot retention period (Periodo de retención de instantáneas), escriba el número de días para conservar la instantánea. Para conservar la instantánea de forma indefinida, escriba **-1**.



Copy Automated Snapshot ✕

Provide a name for the new snapshot.

Source Snapshot Identifier rs:example-cluster-2018-11-30-17-45-51

Snapshot identifier example-cluster-manual ⓘ

Snapshot retention period -1 days ⓘ

Cancel Continue

8. Elija Continue.

Restauración de un clúster desde una instantánea

Cuando restaura un clúster desde una instantánea, Amazon Redshift crea un nuevo clúster con todos los datos de la instantánea del nuevo clúster.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Pasos para restaurar un clúster desde una snapshot

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), y después seleccione la instantánea que desee restaurar.
3. Seleccione Restore from snapshot (Restaurar desde instantánea) para ver los valores de la Cluster configuration (Configuración de clúster) y los Cluster details (Detalles de clúster) del nuevo clúster que se creará utilizando la información de la instantánea.
4. Actualice las propiedades del nuevo clúster, luego seleccione Restore cluster from snapshot (Restaurar clúster desde instantánea).

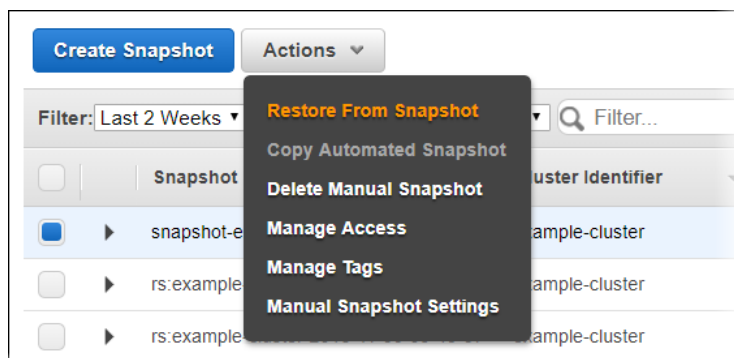
Consola original

Note

Puede utilizar estos pasos para cambiar la plataforma de un clúster de EC2-Classic a EC2-VPC y viceversa.

Pasos para restaurar un clúster desde una snapshot

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Para filtrar la lista, realice alguna de las acciones a continuación:
 - En el cuadro Time Range (Intervalo de tiempo), elija un intervalo de tiempo para acotar su búsqueda de forma adecuada.
 - En el cuadro Type (Tipo), elija manual o automated (automatizada).
 - En el cuadro Cluster, elija el nombre de un clúster para enumerar instantáneas para un único clúster, o elija All Clusters (Todos los clústeres) para enumerar instantáneas de todos los clústeres.
 - En el campo Sort by (Ordenar por), elija cómo desea ordenar la lista.
4. En la lista de instantáneas, elija la fila que contiene la instantánea que desea utilizar.
5. Elija Restore From Snapshot (Restaurar de instantánea).



6. En el cuadro de diálogo Restore Cluster from Snapshot (Restaurar clúster a partir de instantánea), haga lo siguiente:

- a. En el cuadro Cluster Identifier (Identificador del clúster), escriba un identificador para el clúster restaurado.

Los identificadores de clúster deben cumplir las condiciones a continuación:

- Deben tener de 1 a 255 caracteres alfanuméricos o guiones.
- Los caracteres alfanuméricos deben ir en minúscula.
- El primer carácter debe ser una letra.
- No pueden terminar con un guion ni tener dos guiones consecutivos.
- Deben ser únicos para todos los clústeres de una cuenta de AWS.

- b. En el cuadro Port (Puerto), acepte el puerto de la instantánea o cambie el valor, según corresponda.
- c. Seleccione Allow Version Upgrade (Permitir actualización de versiones), según corresponda.
- d. En el cuadro Cluster Subnet Group (Grupo de subredes del clúster), seleccione el grupo de subredes en el que desea restaurar el clúster.

Esta opción solo aparece si restaura el clúster hacia una plataforma EC2-VPC.

- e. En Publicly Accessible (Accesible públicamente), seleccione Yes (Sí) si desea que el clúster tenga una dirección IP pública a la que se pueda acceder desde una conexión pública a Internet. Seleccione No si desea que el clúster tenga una dirección IP privada a la que solamente se pueda acceder desde la VPC. Si las recetasAWSLa cuenta de le permite crear clústeres EC2-Classic, el valor predeterminado esNo. De lo contrario, el valor predeterminado esSí.

Esta opción solo aparece si restaura el clúster hacia una plataforma EC2-VPC.

- f. En Choose a Public IP Address (Seleccione una dirección IP pública), seleccione Yes (Sí) si desea seleccionar una dirección IP elástica (EIP) que ya haya configurado. De lo contrario, seleccioneNoPara que Amazon Redshift cree una EIP para su instancia.

Esta opción solo aparece si restaura el clúster hacia una plataforma EC2-VPC.

- g. En Elastic IP (IP elástica), seleccione una EIP para conectarse al clúster desde fuera de la VPC.

Esta opción solo aparece si restaura el clúster en la plataforma EC2-VPC y si selecciona Yes (Sí) en Choose a Public IP Address (Seleccione una dirección IP pública).

- h. En el cuadro Availability Zone (Zona de disponibilidad), acepte la zona de disponibilidad de la instantánea o cambie el valor, según corresponda.
- i. En Cluster Parameter Group (Grupo de parámetros del clúster), seleccione un grupo de parámetros para asociarlo al clúster.
- j. En Cluster Security Groups (Grupos de seguridad del clúster) o VPC Security Groups (Grupos de seguridad de VPC), seleccione un grupo de seguridad para asociarlo al clúster. Los tipos de

grupos de seguridad que se muestran aquí dependen de si está restaurando el clúster en una plataforma EC2-VPC o EC2-Classic.

La opción de seleccionar un grupo de seguridad de un clúster o un grupo de seguridad de una VPC depende de si está restaurando el clúster en la plataforma EC2-VPC o en la plataforma EC2-Classic.

- k. En Maintenance track (Pista de mantenimiento), se muestra el valor de la pista de mantenimiento. En Change maintenance track to (Cambiar pista de mantenimiento a), puede elegir restaurar el clúster con una de las pistas de mantenimiento que se muestran.

A continuación, tenemos un ejemplo de una restauración de una snapshot en un clúster que utiliza la plataforma EC2-VPC.

The screenshot shows the 'Restore Cluster From Snapshot' dialog box. It contains the following fields and options:

- Snapshot Identifier:** rs:examplecluster-2015-03-16-17-03-49
- Node Type:** ds2.xlarge
- Cluster Identifier:** examplecluster-target
- Duplicate CloudWatch alarms:** Yes (selected)
- Port:** 5439
- Allow Version Upgrade:** Yes (selected)
- Cluster Subnet Group:** default
- Publicly Accessible:** Yes (selected)
- Choose a Public IP Address:** No
- Availability Zone:** us-east-1b
- Cluster Parameter Group:** default.redshift-1.0
- VPC Security Groups:** default-elasticmapreduce-1

A continuación, tenemos un ejemplo de una restauración de una snapshot en un clúster que utiliza la plataforma EC2-Classic.

The screenshot shows the 'Restore Cluster From Snapshot' dialog box for EC2-Classic. It contains the following fields and options:

- Snapshot Identifier:** rs:examplecluster - 2015-03-18-20-32-31
- Node Type:** ds2.xlarge
- Cluster Identifier:** examplecluster-target
- Duplicate CloudWatch alarms:** Yes (selected)
- Port:** 5439
- Allow Version Upgrade:** Yes (selected)
- Availability Zone:** us-east-1a
- Cluster Parameter Group:** default.redshift-1.0
- Cluster Security Groups:** default, securitygroup1

- 7. Elija Restore.

Compartir una instantánea de un clúster

Puede autorizar a otros usuarios a obtener acceso a una snapshot manual de su propiedad o puede revocar ese acceso más adelante cuando ya no sea necesario.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

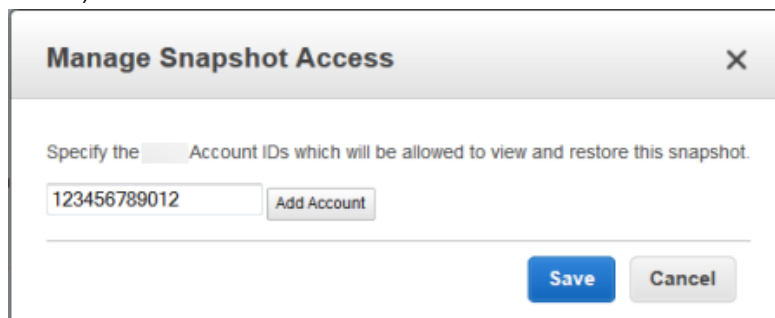
Para compartir una instantánea con otra cuenta

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES), Snapshots (Instantáneas), luego seleccione la instantánea manual para compartir.
3. Para Actions (Acciones), seleccione Manual snapshot settings (Configuración de instantáneas manuales) para mostrar las propiedades de la instantánea manual.
4. Introduzca la cuenta o cuentas para compartir en la sección Manage access (Administrar acceso), luego seleccione Save (Guardar).

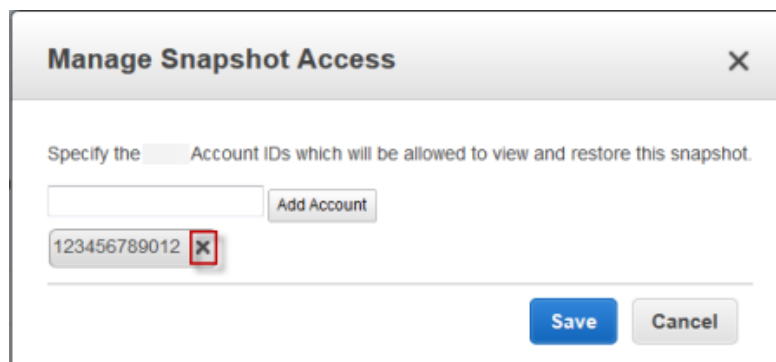
Consola original

Pasos para compartir una snapshot de un clúster

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Snapshots (Instantáneas).
3. Si necesita filtrar la lista para poder encontrar la snapshot que desea compartir, realice alguna de las acciones a continuación:
 - En el cuadro Time Range (Intervalo de tiempo), elija un intervalo de tiempo para acotar su búsqueda de forma adecuada.
 - En el cuadro Cluster (Clúster), elija el clúster cuya instantánea desea compartir.
4. En la lista de instantáneas, elija la fila que contiene la instantánea que desea utilizar.
5. Elija Manage Access (Administrar acceso).
6. En el cuadro de diálogo Manage Snapshot Access (Administrar acceso a instantánea), puede autorizar a un usuario para que obtenga acceso a la instantánea, o bien puede revocar cualquier acceso que haya autorizado previamente.
 - Si desea autorizar a un usuario para que obtenga acceso a la instantánea, escriba en el cuadro el ID de 12 dígitos de la cuenta de AWS de ese usuario (omite los guiones) y elija Add Account (Añadir cuenta).



- Para revocar la autorización de un usuario, seleccione X al lado de ese usuario AWSID de la cuenta de.



7. Elija Save (Guardar) para guardar los cambios o Cancel (Cancelar) para revertir los cambios.

Configuración de la copia de una instantánea entre regiones para un clúster no cifrado

Puede configurar Amazon Redshift para que copie las instantáneas de un clúster a otroAWSRegión . Para configurar una copia de snapshots entre regiones, debe habilitar esta función de copia para cada clúster y, luego, configurar dónde desea copiar las snapshots y por cuánto tiempo desea conservar las snapshots automatizadas o manuales copiadas en el destino de destinoAWSRegión . Cuando se habilita una copia de un clúster entre regiones, se copian todas las instantáneas manuales y automáticas en el clúster especificadoAWSRegión . Los nombres de las instantáneas que se copian tienen el prefijo **copy** .

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para configurar instantáneas entre regiones

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y elija el clúster del que desee mover las instantáneas.
3. ParaActions, elijaConfigurar instantáneas entre regiones.

Aparecerá el cuadro de diálogo Configure entre regiones.
4. ParaCopia de instantáneas, elijaSí.
5. EnDestinoAWSRegión, elija la opciónAWSRegión en la que desea copiar las instantáneas.
6. EnPeriodo de retención de instantáneas (días), seleccione la cantidad de días que desea conservar las instantáneas automatizadas en el destino de destinoAWSRegión antes de que se eliminen.
7. EnPeriodo de retención de instantáneas, seleccione el valor que representa la cantidad de días que desea conservar las instantáneas manuales en el destinoAWSRegión antes de que se eliminen. Si eligeValor personalizado, el período de retención debe estar entre 1 y 3653 días.
8. Elija Save (Guardar).

Consola original

Para configurar la copia de una instantánea entre regiones para un clúster no cifrado

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Elija Backup (copia de seguridad) y, luego, elija Configure Cross-Region Snapshots (Configurar instantáneas entre regiones).
4. En el cuadro de diálogo Configure Cross-Region Snapshots (Configurar instantáneas entre regiones), en Copy Snapshots (Copiar instantáneas), seleccione Yes (Sí).
5. En Región de destino, elija la opciónAWSRegión en la que desea copiar las instantáneas.
6. EnPeriodo de retención (días), seleccione la cantidad de días que desea conservar las instantáneas automatizadas en el destino de destinoAWSRegión antes de que se eliminen.
7. Elija Save (Guardar).

Configuración de la copia de una instantánea entre regiones para unAWS KMS—clúster cifrado

Cuando lance un clúster de Amazon Redshift, puede elegir cifrarlo con una clave maestra desde la lista deAWS Key Management Service(AWS KMS).AWS KMSLas claves de son específicas de unaAWSRegión . Si desea habilitar la copia de una instantánea entre regiones para un servicio deAWS KMS, debe configurar un clúster cifradoconcesión de copia de instantáneaspara una clave maestra en el destinoAWSRegión . Al hacer esto, habilita a Amazon Redshift para que realice operaciones de cifrado en el destino deAWSRegión .

En el siguiente procedimiento, se describe el proceso para habilitar la copia de instantáneas entre regiones para un clúster cifrado en AWS KMS. Para obtener más información acerca del cifrado de Amazon Redshift y las autorizaciones de copia de instantáneas, consulte[CopiarAWS KMS—instantáneas cifradas en otroAWSRegión](#) (p. 287).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para configurar instantáneas entre regiones para un servicio deAWS KMS—clúster cifrado

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y elija el clúster del que desee mover las instantáneas.
3. ParaActions, elijaConfigurar instantáneas entre regiones.

Aparecerá el cuadro de diálogo Configure entre regiones.
4. ParaCopia de instantáneas, elijaSí.
5. EnDestinoAWSRegión, elija la opciónAWSRegión en la que desea copiar las instantáneas.
6. EnPeriodo de retención de instantáneas (días), seleccione la cantidad de días que desea conservar las instantáneas automatizadas en el destino de destinoAWSRegión antes de que se eliminen.

7. En **Período de retención de instantáneas**, seleccione el valor que representa la cantidad de días que desea conservar las instantáneas manuales en el destino **AWSRegión** antes de que se eliminen. Si elige **Valor personalizado**, el período de retención debe estar entre 1 y 3653 días.
8. Elija **Save (Guardar)**.

Consola original

Para configurar una copia de instantáneas entre regiones para un clúster cifrado en AWS KMS

1. Abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija **Clusters (Clústeres)**.
3. En la lista de clústeres, seleccione el nombre de un clúster para abrir la vista **Configuration (Configuración)** del clúster.
4. Elija **Backup (copia de seguridad)** y, luego, elija **Configure Cross-Region Snapshots (Configurar instantáneas entre regiones)**.
5. En el cuadro de diálogo **Configure Cross-Region Snapshots (Configurar instantáneas entre regiones)**, en **Copy Snapshots (Copiar instantáneas)**, seleccione **Yes (Sí)**.
6. En **Región de destino**, elija la opción **AWSRegión** en la que desea copiar las instantáneas.
7. En **Período de retención (días)**, seleccione la cantidad de días que desea conservar las instantáneas automatizadas en el destino de destino **AWSRegión** antes de que se eliminen.
8. En **Existing Snapshot Copy Grant (Concesión de copia de instantánea existente)**, realice una de las siguientes operaciones:
 - a. Seleccione **No** para crear una nueva autorización de copia de instantáneas. En **KMS Key**, seleccione la clave de AWS KMS para la que desea crear la autorización y escriba un nombre en **Snapshot Copy Grant Name (Nombre de concesión de copia de instantánea)**.
 - b. Seleccione **Sí** para seleccionar una autorización de copia de instantáneas existente en el destino de destino **AWSRegión**. A continuación, seleccione una autorización desde **Snapshot Copy Grant (Concesión de copia de instantánea)**.
9. Elija **Save (Guardar)**.

Modificación del período de retención para una copia de instantáneas entre regiones

Después de configurar la copia de instantáneas entre regiones, es posible que desee cambiar la configuración. Puede cambiar el período de retención fácilmente si selecciona otra cantidad de días y guarda los cambios.

Warning

No se puede modificar el destino de **AWSRegión** después de que se haya configurado la copia de una instantánea entre regiones.

Si desea copiar instantáneas a una **AWSRegión**, primero desactive la copia de una instantánea entre regiones. Luego, vuelva a habilitarlo con un nuevo destino. **AWSPeríodo de retención de región**. Las instantáneas automáticas copiadas se eliminan después de deshabilitar la copia de la instantánea entre regiones. Por lo tanto, debe determinar si desea conservar alguna y copiarlas en instantáneas manuales antes de deshabilitar la copia de instantáneas entre regiones.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de **New console (Nueva consola)** o **Original console (Consola original)** en función de la consola que utilice. Las instrucciones de **New console (Nueva consola)** están abiertas de forma predeterminada.

New console

Para modificar instantáneas entre regiones

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y elija el clúster de cual desee modificar las instantáneas.
3. En Actions (Acciones), elija Configure cross-region snapshot (Configurar instantánea entre regiones) para mostrar las propiedades de la instantánea.
4. Introduzca las propiedades editadas de la definición de instantánea, luego seleccione Save (Guardar).

Consola original

Pasos para modificar el período de retención para las snapshots copiadas a un clúster de destino

1. Inicie sesión en la en.AWS Management Console y abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Elija Backup (copia de seguridad) y, luego, elija Configure Cross-Region Snapshots (Configurar instantáneas entre regiones).
4. En el navegadorPeríodo de retenciónSeleccione la nueva cantidad de días que desea conservar las instantáneas automatizadas en el destino de destinoAWSRegión .

Si selecciona una cantidad de días para conservar las instantáneas en el destinoAWSEn la región se eliminan todas las instantáneas automatizadas que se tomaron antes del nuevo período de retención. Si selecciona una cantidad de días para conservar las instantáneas en el destinoAWSEn la región, se prolongará el período de retención de las instantáneas automatizadas existentes. Se alarga por la diferencia entre el valor antiguo y el nuevo valor.

5. Elija Save Configuration (Guardar configuración).

Administración de instantáneas mediante la herramientaAWS SDK for Java

En el siguiente ejemplo, se muestran estas operaciones frecuentes relacionadas con snapshots:

- Creación de una snapshot manual de un clúster
- Visualización de información de todas las snapshots de un clúster
- Eliminación de snapshots manuales de un clúster

En este ejemplo, se inicia una snapshot del clúster. Cuando una snapshot se crea correctamente, se eliminan todas las snapshots manuales del clúster que fueron creadas antes que la snapshot nueva. Cuando se inicia la creación de una snapshot manual, la snapshot no está disponible inmediatamente. Por lo tanto, en este ejemplo se utiliza un bucle para sondear el estado de la snapshot mediante el método `describeClusterSnapshot`. Por lo general, toma algún tiempo hasta que una snapshot está disponible después de su inicialización. Para obtener más información acerca de las instantáneas, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#).

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Debe actualizar el código y proporcionar un identificador de clúster.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[CreateAndDescribeSnapshot demonstrates how to create an
// Amazon Redshift cluster snapshot and describe existing snapshots.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterSnapshot]
// snippet-keyword:[DeleteClusterSnapshot]
// snippet-keyword:[DescribeClusterSnapshots]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-30]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndDescribeSnapshot.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
import java.text.SimpleDateFormat;
import java.util.Date;

import com.amazonaws.services.redshift.model.*;

public class CreateAndDescribeSnapshot {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "****provide a cluster identifier****";
    public static long sleepTime = 20;

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
        com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            // Unique snapshot identifier
            String snapshotId = "my-snapshot-" + (new SimpleDateFormat("yyyy-MM-dd-HH-mm-ss")).format(new Date());

            Date createDate = createManualSnapshot(snapshotId);
            waitForSnapshotAvailable(snapshotId);
            describeSnapshots();
            deleteManualSnapshotsBefore(createDate);
            describeSnapshots();

        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }
}
```

```
private static Date createManualSnapshot(String snapshotId) {

    CreateClusterSnapshotRequest request = new CreateClusterSnapshotRequest()
        .withClusterIdentifier(clusterIdentifier)
        .withSnapshotIdentifier(snapshotId);
    Snapshot snapshot = client.createClusterSnapshot(request);
    System.out.format("Created cluster snapshot: %s\n", snapshotId);
    return snapshot.getSnapshotCreateTime();
}

private static void describeSnapshots() {

    DescribeClusterSnapshotsRequest request = new DescribeClusterSnapshotsRequest()
        .withClusterIdentifier(clusterIdentifier);
    DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(request);

    printResultSnapshots(result);
}

private static void deleteManualSnapshotsBefore(Date creationDate) {

    DescribeClusterSnapshotsRequest request = new DescribeClusterSnapshotsRequest()
        .withEndTime(creationDate)
        .withClusterIdentifier(clusterIdentifier)
        .withSnapshotType("manual");

    DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(request);

    for (Snapshot s : result.getSnapshots()) {
        DeleteClusterSnapshotRequest deleteRequest = new DeleteClusterSnapshotRequest()
            .withSnapshotIdentifier(s.getSnapshotIdentifier());
        Snapshot deleteResult = client.deleteClusterSnapshot(deleteRequest);
        System.out.format("Deleted snapshot %s\n",
deleteResult.getSnapshotIdentifier());
    }
}

private static void printResultSnapshots(DescribeClusterSnapshotsResult result) {
    System.out.println("\nSnapshot listing:");
    for (Snapshot snapshot : result.getSnapshots()) {
        System.out.format("Identifier: %s\n", snapshot.getSnapshotIdentifier());
        System.out.format("Snapshot type: %s\n", snapshot.getSnapshotType());
        System.out.format("Snapshot create time: %s\n",
snapshot.getSnapshotCreateTime());
        System.out.format("Snapshot status: %s\n\n", snapshot.getStatus());
    }
}

private static Boolean waitForSnapshotAvailable(String snapshotId) throws
InterruptedException {
    Boolean snapshotAvailable = false;
    System.out.println("Waiting for snapshot to become available.");
    while (!snapshotAvailable) {
        DescribeClusterSnapshotsResult result = client.describeClusterSnapshots(new
DescribeClusterSnapshotsRequest()
            .withSnapshotIdentifier(snapshotId));
        String status = (result.getSnapshots().get(0).getStatus());
        if (status.equalsIgnoreCase("available")) {
            snapshotAvailable = true;
        }
        else {
            System.out.print(".");
            Thread.sleep(sleepTime*1000);
        }
    }
}
```

```
        return snapshotAvailable;
    }
}
// snippet-end:[redshift.java.CreateAndDescribeSnapshot.complete]
```

Administración de instantáneas mediante laAWS CLIAmazon Redshift API y Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar las instantáneas.

- [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](#)

Puede utilizar las siguientes acciones de la API de Amazon Redshift para administrar las instantáneas.

- [AuthorizeSnapshotAccess](#)
- [CopyClusterSnapshot](#)
- [CreateClusterSnapshot](#)
- [DeleteClusterSnapshot](#)
- [DescribeClusterSnapshots](#)
- [DisableSnapshotCopy](#)
- [EnableSnapshotCopy](#)
- [ModifySnapshotCopyRetentionPeriod](#)
- [RestoreFromClusterSnapshot](#)
- [RevokeSnapshotAccess](#)

Para obtener más información acerca de las instantáneas de Amazon Redshift, consulte [Instantáneas de Amazon Redshift](#) (p. 238).

Integración de Amazon Redshift con un AWS Socio

Al trabajar con Amazon Redshift, puede integrarse con AWS socios de la Detalles de clúster en la consola de Amazon Redshift. Desde la Detalles de clúster, puede acelerar la incorporación de datos en su almacén de datos de Amazon Redshift con AWS Aplicaciones de socios. También puede unir y analizar datos de diferentes orígenes junto con los datos existentes en el clúster. Los siguientes ejemplos de AWS Los partners pueden integrarse con Amazon Redshift:

- [Datacoral](#)
- [Etleap](#)
- [Cinvetran](#)
- [Informatica](#)
- [SnapLogic](#)
- [Matillion \(vista previa\)](#)
- [Sisense \(vista previa\)](#)
- [Puntada \(vista previa\)](#)

AWS Los partners pueden integrarse con Amazon Redshift mediante el AWS CLI o las operaciones de la API de Amazon Redshift. Para obtener más información, consulte la AWS CLI Referencia de los comandos de la API de Amazon Redshift.

Integración con una AWS asociado que utiliza la consola de Amazon Redshift

Utilice el siguiente procedimiento para integrar un clúster con una AWS- Un socio.

Para integrar un clúster de Amazon Redshift con una AWS Socio

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione CLÚSTERES DE.
3. Elija el clúster que desea integrar.
4. Seleccione Integración con socios. La Elija socios se abre con detalles sobre el AWS partners
5. Elija un AWS Socio, luego elija Siguiente.

Más detalles sobre el elegido AWS aparecerá el socio, junto con detalles sobre el clúster que está integrando. La Detalles de clúster incluye la información que proporciona en la sección AWS Sitio web de socios, como el identificador de clúster, Punto de enlace, Nombre de base de datos, y User name (Nombre de usuario): (que es un nombre de usuario de base de datos). Esta información se envía al socio que eligió.

6. Seleccione Agregar socios para abrir AWS Sitio web del socio.
7. Configure la integración con su clúster de Amazon Redshift en el sitio web del socio. En el sitio web del socio, puede seleccionar y configurar las fuentes de datos que se cargan en el clúster de Amazon Redshift. También puede definir transformaciones adicionales de extracción, carga y transformación

(ELT) para procesar los datos empresariales, unirlos a otros conjuntos de datos y crear vistas consolidadas para el análisis y la generación de informes.

Puede ver y administrarAWSIntegraciones de socios desde los detalles del clústerPropiedadesPestaña. LaIntegracionesmuestra la secciónSocioque puede utilizar para vincular a laAWSsitio web del socio, elEstadode la integración, elBase de datosque recibe los datos, y elÚltima conexión correctaque podría haber actualizado el clúster.

Los valores posibles son los siguientes:

- Activo:AWSEl socio puede conectarse al clúster y completar las tareas configuradas.
- Inactive:AWSLa integración con socios no existe.
- Error en tiempo de ejecución: elAWSEl socio puede conectarse al clúster, pero no puede completar las tareas configuradas.
- Error de conexión: elAWSEl socio no puede conectarse al clúster.

Después de eliminar unAWSIntegración de partners de Amazon Redshift, los datos siguen fluyendo en su clúster. Complete la eliminación en el sitio web del socio.

Compra de nodos reservados de Amazon Redshift

Overview

En AWS, los cargos incurridos por usar Amazon Redshift se basan en los nodos de computación. Cada nodo de computación se factura según una tarifa por hora. La tarifa por hora varía según factores como región, tipo de nodo y si el nodo recibe precio de nodo bajo pedido o precio de nodo reservado.

Precios de nodos bajo demanda es la opción más costosa, pero también la más flexible de Amazon Redshift. Con tarifas bajo pedido, se le facturan únicamente los nodos de computación que tenga en un clúster en ejecución. Si cierra o elimina un clúster, ya no se le cobrará por los nodos de computación que estaban en ese clúster. Solo se le factura por los nodos de computación que utilice, no más. La tarifa por hora que se le cobra por cada nodo de computación varía según factores como región y tipo de nodo.

El precio de nodo reservado es menos costoso que el precio bajo pedido, ya que los nodos de computación se facturan a un precio por hora con descuento. No obstante, para recibir estas tarifas con descuento, debe comprar ofertas de nodos reservados. Cuando compra una oferta, hace una reserva. La reserva establece una tarifa con descuento para cada nodo que reserve por la duración de la reserva. La tarifa con descuento en una oferta varía según factores como región, tipo de nodo, duración y opción de pago.

Puede designar un nodo como nodo reservado llamando a la operación `PurchaseReservedNodeOffering` de la API o eligiendo Comprar nodos reservados en la consola de Amazon Redshift. Al comprar un nodo reservado, debe especificar un `AWSRegión`, tipo de nodo, término, cantidad de nodos y tipo de oferta para el tipo de nodo reservado aplicable. El nodo reservado solo puede utilizarse en el `AWSRegión`.

En este tema, se analiza qué son las ofertas de nodo reservado y cómo puede adquirirlas para reducir el costo de ejecución de los clústeres de Amazon Redshift. En este tema, se analizan las tarifas en términos generales, por ejemplo bajo pedido o con descuento, para que pueda comprender los conceptos de precios y cómo estos afectan la facturación. Para obtener más información sobre tarifas específicas, visite [Precios de Amazon Redshift](#).

Consideraciones sobre ofertas de nodos reservados

Si desea que el clúster de Amazon Redshift se siga ejecutando continuamente durante un período prolongado, considere adquirir ofertas de nodo reservado. Estas ofertas ofrecen ahorros importantes sobre el precio bajo pedido, pero requieren que reserve nodos de computación y se comprometa a pagar por esos nodos durante un año o tres años.

Los nodos reservados son un concepto de facturación que se utiliza estrictamente para determinar la tarifa de facturación por los nodos. Reservar un nodo, en realidad, no crea ningún nodo para usted. Se le cobra por los nodos reservados independientemente del uso, lo que significa que debe pagar por cada nodo que reserve por la duración de la reserva, tenga o no nodos en un clúster en ejecución al que se aplique la tarifa con descuento.

En la fase de evaluación del proyecto o cuando desarrolla una prueba de concepto, el precio bajo demanda le brinda flexibilidad para pagar por uso, solo por lo que use, y dejar de pagar en cualquier momento al cerrar o eliminar clústeres. Después de establecer las necesidades del entorno de producción y comenzar la fase de implementación, debe considerar reservar nodos de computación al adquirir una o más ofertas.

Una oferta puede aplicarse a uno o más nodos de computación. Usted especifica la cantidad de nodos de computación que reservará cuando adquiere la oferta. Puede elegir adquirir una oferta para distintos nodos de computación o puede elegir adquirir varias ofertas y especificar una determinada cantidad de nodos de computación en cada oferta.

Por ejemplo, cualquiera de las siguientes son formas válidas de adquirir una oferta para tres nodos de computación:

- Adquirir una oferta y especificar tres nodos de computación.
- Adquirir dos ofertas y especificar un nodo de computación para la primera oferta y dos nodos de computación para la segunda oferta.
- Adquirir tres ofertas y especificar un nodo de computación para cada una.

Comparación del precio entre ofertas de nodos reservados

Amazon Redshift ofrece distintas opciones de pago para las ofertas. La opción de pago que elija afectará el cronograma de pagos y la tarifa con descuento que se le cobre por la reserva. Mientras más pague inicialmente por la reserva, mayor será el ahorro general que obtenga.

Las siguientes opciones de pago están disponibles para las ofertas. Las ofertas se indican en orden de menor a mayor ahorro sobre tarifas bajo pedido.

Note

Se le cobra la tarifa por hora aplicable por cada hora en la duración especificada de la reserva, independientemente de si usa el nodo reservado o no. La opción de pago solamente determina la frecuencia de los pagos y el descuento que se aplicará. Para obtener más información, consulte [Consideraciones sobre ofertas de nodos reservados \(p. 271\)](#).

Comparación de ofertas de nodos reservados

Opción de pago	Cronograma de pagos	Comparación de ahorros	Duración	Cargos iniciales	Cargos mensuales recurrentes
Sin pago inicial	Cuotas mensuales para la duración de la reserva. Sin pagos iniciales.	Aproximadamente, un 20% de descuento sobre tarifas bajo pedido.	Término de un año	Ninguna	Sí
Pago inicial parcial	Pago inicial parcial y cuotas mensuales por la duración de la reserva.	Hasta un 41% a un 73% de descuento según la duración.	Término de un año o tres años	Sí	Sí
Pago inicial total	Pago inicial completo para la reserva. Sin cargos mensuales.	Hasta un 42% a un 76% de descuento según la duración.	Término de un año o tres años	Sí	Ninguna

Note

Si ya compraste `Usos intensos` para Amazon Redshift, la oferta comparable es la `Pago inicial parcial`.

Cómo funcionan los nodos reservados

Con ofertas de nodo reservado, usted paga según los términos de pago, como se indicó en la sección anterior. De esta manera, debe pagar ya sea que tenga un clúster en ejecución o que lance un clúster después de una reserva.

Cuando compra una oferta, la reserva tiene el estado `payment-pending` (pendiente de pago) hasta que se procesa. Si la reserva no se puede procesar, el estado es `payment-failed` (error al pagar) y puede intentar el proceso nuevamente. Cuando la reserva se procesa con éxito, el estado cambia a `active` (activa). La tarifa con descuento aplicable a la reserva no se hace efectiva en la factura hasta que el estado cambia a `active` (activa). Una vez que transcurre la duración de la reserva, el estado cambia a `retired` (retirada), pero puede seguir obteniendo acceso a la información relacionada con la reserva para consultar el historial. Cuando el estado de una reserva es `retired` (retirada), los clústeres continúan ejecutándose, pero es posible que se apliquen los precios bajo pedido, a menos que tenga otra reserva que aplique un precio con descuento a los nodos.

Los nodos reservados son específicos de la región en la cual compra la oferta. Si adquiere una oferta mediante la consola de Amazon Redshift, seleccione la casilla `AWSEn la que desea comprar una oferta` y, luego, complete el proceso de reserva. Si compra una oferta de manera programática, la región se determina por el punto de enlace de Amazon Redshift al que se conecta. Para obtener más información sobre las regiones de Amazon Redshift, consulte [Regiones y puntos de enlace](#) de la Referencia general de Amazon Web Services.

Para asegurarse de que se aplique la tarifa con descuento a todos los nodos cuando lanza un clúster, asegúrese de que la región, el tipo de nodo y la cantidad de nodos que seleccione coincidan con una o más reservas activas. De lo contrario, se le cobrará una tarifa bajo demanda por los nodos que no coincidan con una reserva activa.

En un clúster en ejecución, si supera la cantidad de nodos que tiene reservados, comienza a acumular cargos por esos nodos adicionales a una tarifa bajo pedido. Esta acumulación significa que es posible que se le cobren tarifas variables por los nodos de un mismo clúster, según la cantidad de nodos que haya reservado. Puede adquirir otra oferta para cubrir esos nodos adicionales y la tarifa con descuento se aplicará a esos nodos en lo que reste de la duración una vez que el estado de la reserva sea `active` (activa).

Si redimensiona el clúster en un tipo de nodo diferente y no tiene nodos reservados de ese tipo, se le cobrará la tarifa bajo pedido. Puede comprar otra oferta con el tipo de nodo nuevo para el que desea recibir tarifas con descuento para su clúster redimensionado. Sin embargo, también continúa pagando por la reserva original hasta que transcurra su duración. Si necesita cambiar las reservas antes de que finalice el plazo, cree un caso de soporte a través de la [AWS Consola](#).

Nodos reservados y facturación unificada

Los beneficios de precio de nodos reservados se comparten cuando la cuenta de adquisición es parte de un conjunto de cuentas facturadas en una sola cuenta del pagador de facturación consolidada. El uso por hora entre todas las subcuentas se acumula mensualmente en la cuenta del pagador. Por lo general, esta modalidad es útil para empresas en las que hay diferentes equipos o grupos funcionales; de este modo, se aplica la lógica normal de nodos reservados para calcular la factura. Para obtener más información, consulte [Facturación unificada](#) en la [AWS Billing and Cost Management Guía del usuario](#) de .

Ejemplos de nodos reservados

En los escenarios de esta sección, se demuestra de qué manera los nodos acumulan cargos según tarifas bajo pedido o con descuento utilizando los siguientes detalles de reserva:

- Región : US West (Oregon)

- Tipo de nodo: ds2.xlarge
- Opción de pago: Sin pago inicial
- Duración: un año
- Cantidad de nodos reservados: 16

Ejemplo 1

Tiene un clúster ds2.xlarge en la región EE. UU. Oeste (Oregón) con 20 nodos.

En este escenario, 16 de los nodos reciben la tarifa con descuento de la reserva, pero los 4 nodos adicionales en el clúster se facturan a una tarifa bajo pedido.

Ejemplo 2

Tiene un clúster ds2.xlarge en la región EE. UU. Oeste (Oregón) con 12 nodos.

En este escenario, los 12 nodos del clúster reciben la tarifa con descuento de la reserva. No obstante, también paga por los nodos reservados restantes en la reserva, aunque actualmente no tenga un clúster en ejecución donde aplicarlos.

Ejemplo 3

Tiene un clúster ds2.xlarge en la región EE. UU. Oeste (Oregón) con 12 nodos. Usted ejecuta el clúster durante varios meses con esta configuración y, luego, necesita añadir nodos al clúster. Redimensiona el clúster, elige el mismo tipo de nodo y especifica un total de 16 nodos.

En este escenario, se le factura la tarifa con descuento por los 16 nodos. Los cargos permanecen iguales durante todo el año de duración porque la cantidad de nodos que tiene en el clúster es igual a la cantidad de nodos que tiene reservados.

Ejemplo 4

Tiene un clúster ds2.xlarge en la región EE. UU. Oeste (Oregón) con 16 nodos. Usted ejecuta el clúster durante varios meses con esta configuración y, luego, necesita añadir nodos. Redimensiona el clúster, elige el mismo tipo de nodo y especifica un total de 20 nodos.

En este escenario, se le factura la tarifa con descuento por todos los nodos antes del redimensionamiento. Luego del redimensionamiento, se le factura la tarifa con descuento por 16 de los nodos para el resto del año, y se le factura una tarifa bajo pedido para los 4 nodos adicionales que añadió al clúster.

Ejemplo 5

Tiene dos clústeres ds2.xlarge en la región EE. UU. Oeste (Oregón). Uno de los clústeres tiene 6 nodos y el otro, 10 nodos.

En este escenario, se le factura tarifa con descuento para todos los nodos porque la cantidad total de nodos en ambos clústeres es igual a la cantidad de nodos que tiene reservados.

Ejemplo 6

Tiene dos clústeres ds2.xlarge en la región EE. UU. Oeste (Oregón). Uno de los clústeres tiene 4 nodos y el otro, 6 nodos.

En este escenario, se le factura la tarifa con descuento para los 10 nodos que tiene en clústeres en ejecución y también paga la tarifa con descuento para los 6 nodos adicionales que tiene reservados, aunque actualmente no los aplique a ningún clúster en ejecución.

Adquisición de una oferta de nodo reservado con la consola de Amazon Redshift

Utilice la **Nodos reservados** En la consola de Amazon Redshift para adquirir ofertas de nodos reservados y ver las reservas pasadas y actuales.

Después de adquirir una oferta, en la lista Reserved Node (Nodo reservado) se muestran las reservas y los detalles de cada una, como el tipo de nodo, la cantidad de nodos y el estado del proceso de reserva. Para obtener más información acerca de los detalles de las reservas, consulte [Cómo funcionan los nodos reservados](#) (p. 273).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para adquirir un nodo reservado

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (Clústeres) y a continuación seleccione Reserved nodes (Nodos reservados) para mostrar la lista de nodos reservados.
3. Seleccione Purchase reserved nodes (Adquirir nodos reservados) para mostrar la página para seleccionar las propiedades del nodo que quiere adquirir.
4. Entre en las propiedades del nodo y seleccione Purchase reserved nodes (Comprar nodos reservados)

Consola original

Adquisición de una oferta de nodo reservada

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Reserved Nodes (Nodos reservados).
3. Seleccione Purchase Reserved Nodes (Adquirir nodos reservados)
4. En el asistente Purchase Reserved Nodes (Adquirir nodos reservados), seleccione Node Type (Tipo de nodo), Term (Periodo) y Offering Type (Tipo de oferta).

Purchase Reserved Nodes

Select from the options below, then enter the Number of Nodes you wish to reserve with this order. When you are done, click the Continue button to review your order.

Node Type: ds2.xlarge
Term: 3 years
Offering Type: Partial Upfront

One-time Payment: \$3,000.00 (per node)
Number of Nodes: 1
Total One-time Payment*: \$3,000.00 (Due Now)
*Additional taxes may apply

Usage Charges*: \$0.11 (Hourly) (per node)
Charges for your usage will appear on your monthly bill.
*Additional taxes may apply

Cancel Continue

5. En Number of Nodes (Número de nodos), escriba el número de nodos que desea reservar.
6. Elija Continue.
7. Revise los detalles de la oferta y seleccione Purchase (Comprar).

Purchase Reserved Nodes

You are about to purchase Reserved Node(s) with the following information.

Region: US East (N. Virginia)
Node Type: ds2.xlarge
Offering Type: Partial Upfront
Term: 3 years
Quantity: 1
Price Per Node: \$3,000.00
Total Payment Due Now: \$3,000.00

Purchasing these Reserved Nodes will charge \$3,000.00 the payment method associated with this Amazon Web Services account.

Are you sure you would like to proceed?

Purchase

Back Cancel

8. En la página Reserved Nodes (Nodos reservados), la reserva se muestra en la lista de reservas con el estado payment-pending (pendiente de pago).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para actualizar un nodo reservado, utilice la Original Console (Consola original) o la AWS CLI.

Consola original

Actualizar un nodo reservado de DC1 a DC2

Puede actualizar sin costo alguno los nodos reservados DC1 a nodos DC2 durante el resto de la oferta actual. El nodo DC2 está diseñado para cargas de trabajo de almacenamiento de datos exigentes que requieren una latencia baja y un nivel de procesamiento elevado.

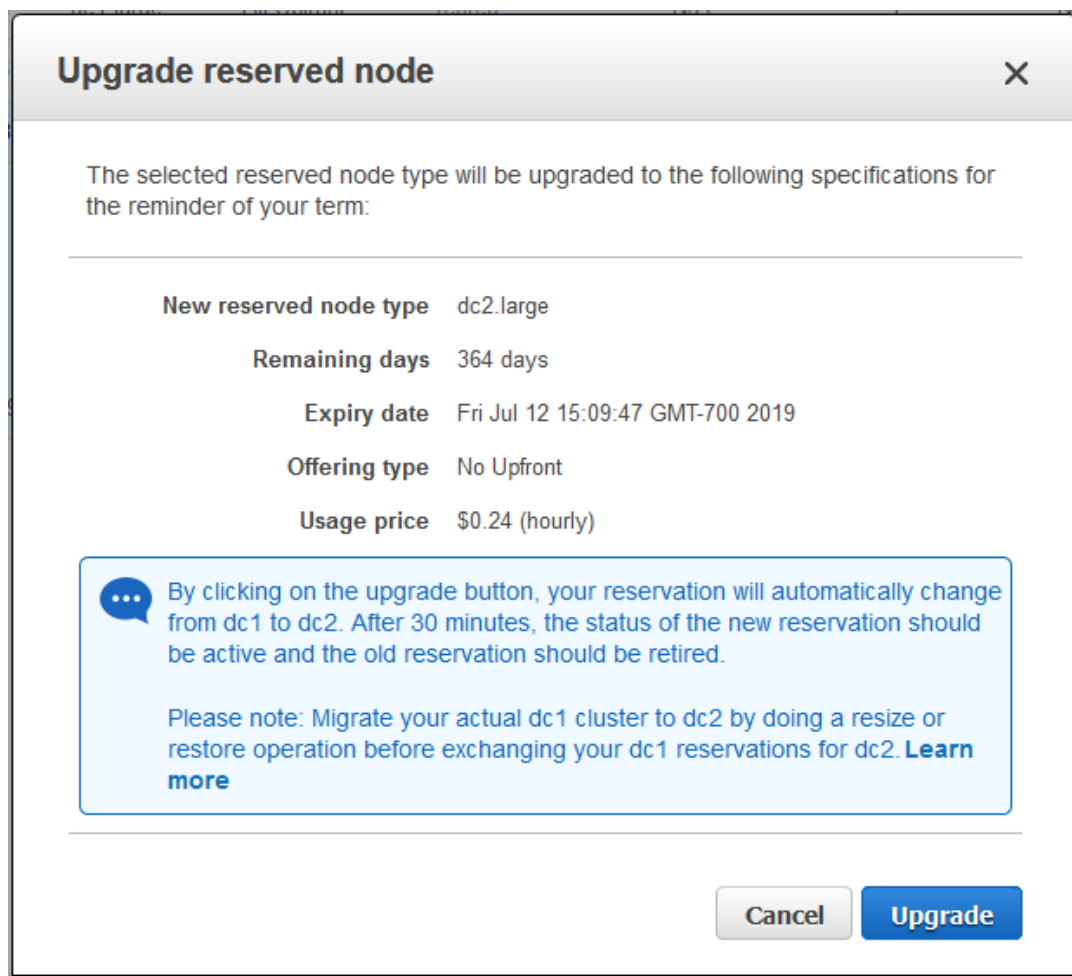
Requisitos previos

Migre el clúster que incluye el nodo que tiene previsto actualizar antes de actualizar los nodos reservados. Si desea migrar el clúster DC1 a DC2, use la operación de ajuste de tamaño o restauración. Si el clúster es de tipo DC1.large, puede restaurarlo en un nuevo clúster DC2.large a partir de una instantánea existente. Si su clúster es de tipo DC1.8xlarge, puede cambiar el tamaño para que sea un clúster DC2.8xlarge. Compruebe que el clúster DC1 esté cerrado antes de actualizar los nodos reservados. El clúster DC2 incrementará los precios bajo demanda hasta que actualice los nodos reservados DC1.

Para obtener más información acerca de la restauración desde una instantánea, consulte [Instantáneas de Amazon Redshift \(p. 238\)](#). Para obtener más información acerca de cómo cambiar el tamaño de un clúster, consulte [Cambio de tamaño de los clústeres de Amazon Redshift \(p. 23\)](#).

Para actualizar una reserva de nodo reservado

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Reserved Nodes (Nodos reservados).
3. Seleccione el nodo reservado DC1 que quiere actualizar.
4. Revise los detalles en el cuadro de diálogo Upgrade reserved node (Actualizar nodo reservado) y seleccione Upgrade (Actualizar).



Actualizar nodos reservados con AWS CLI

Para actualizar una reserva de nodo reservado con AWS CLI

1. Obtenga una lista de ReservedNodeOfferingID de ofertas que cumplan los requisitos de tipo de pago, plazo y cargos. El ejemplo siguiente ilustra este paso.

```
aws redshift get-reserved-node-exchange-offerings --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx
{
  "ReservedNodeOfferings": [
    {
      "Duration": 31536000,
      "ReservedNodeOfferingId": "yyyyyyyy-yyy-yyy-yyyy-yyyyyyyyyyyy",
      "UsagePrice": 0.0,
      "NodeType": "dc2.large",
      "RecurringCharges": [
        {
          "RecurringChargeFrequency": "Hourly",
          "RecurringChargeAmount": 0.2
        }
      ],
      "CurrencyCode": "USD",
    }
  ]
}
```

```

    "OfferingType": "No Upfront",
    "ReservedNodeOfferingType": "Regular",
    "FixedPrice": 0.0
  }
]
}

```

2. Llame a `accept-reserved-node-exchange` y proporcione el ID del nodo reservado DC1 que quiere intercambiar junto con el `ReservedNodeOfferingID` que ha obtenido en el paso anterior.

El ejemplo siguiente ilustra este paso.

```
aws redshift accept-reserved-node-exchange --reserved-node-id xxxxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx --target-reserved-node-offering-id yyyyyyy-yyy-yyy-yyy-yyy-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": "yyyyyy-yyy-yyy-yyy-yyy-yyyyyyyyyyyy",
    "Duration": 31536000
  }
}
```

Puede confirmar que el intercambio se ha completado llamando a `describe-reserved-nodes` y comprobando el valor de `Node type`.

Adquisición de una oferta de nodo reservado mediante laAWS SDK for Java

En el siguiente ejemplo se muestra cómo usar laAWS SDK for Javapuede hacer lo siguiente:

- Enumerar nodos reservados ya existentes.
- Buscar una nueva oferta de nodo reservado basada en criterios de nodos especificados.
- Adquirir un nodo reservado.

Este ejemplo, primero selecciona todas las ofertas de nodos reservados que coincidan con un tipo de nodo especificado y un valor fijado. Luego, pasa por cada oferta encontrada y le permite adquirir la oferta.

Important

Si ejecuta este ejemplo y acepta la oferta para adquirir un nodo reservado, le cobraremos por la oferta.

Para obtener instrucciones paso a paso para ejecutar este ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Para obtener información acerca de un tipo de nodo y un precio fijo diferente a los que se muestran, actualice el código y proporcione ese tipo de nodo y precio fijado.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[ListAndPurchaseReservedNodeOffering demonstrates how to list
// and purchase Amazon Redshift reserved node offerings.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[DescribeReservedNodeOfferings]
// snippet-keyword:[PurchaseReservedNodeOffering]
// snippet-keyword:[ReservedNode]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-31]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ListAndPurchaseReservedNodeOffering.complete]

package com.amazonaws.services.redshift;

import java.io.DataInput;
import java.io.DataInputStream;
import java.io.IOException;
import java.util.ArrayList;

import com.amazonaws.services.redshift.model.*;

public class ListAndPurchaseReservedNodeOffering {

    public static AmazonRedshift client;
    public static String nodeTypeToPurchase = "dc2.large";
    public static Double fixedPriceLimit = 10000.00;
    public static ArrayList<ReservedNodeOffering> matchingNodes = new
    ArrayList<ReservedNodeOffering>();

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
        com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
```

```
        listReservedNodes();
        findReservedNodeOffer();
        purchaseReservedNodeOffer();

    } catch (Exception e) {
        System.err.println("Operation failed: " + e.getMessage());
    }
}

private static void listReservedNodes() {
    DescribeReservedNodesResult result = client.describeReservedNodes();
    System.out.println("Listing nodes already purchased.");
    for (ReservedNode node : result.getReservedNodes()) {
        printReservedNodeDetails(node);
    }
}

private static void findReservedNodeOffer()
{
    DescribeReservedNodeOfferingsRequest request = new
DescribeReservedNodeOfferingsRequest();
    DescribeReservedNodeOfferingsResult result =
client.describeReservedNodeOfferings(request);
    Integer count = 0;

    System.out.println("\nFinding nodes to purchase.");
    for (ReservedNodeOffering offering : result.getReservedNodeOfferings())
    {
        if (offering.getNodeType().equals(nodeTypeToPurchase)){

            if (offering.getFixedPrice() < fixedPriceLimit) {
                matchingNodes.add(offering);
                printOfferingDetails(offering);
                count +=1;
            }
        }
    }
    if (count == 0) {
        System.out.println("\nNo reserved node offering matches found.");
    } else {
        System.out.println("\nFound " + count + " matches.");
    }
}

private static void purchaseReservedNodeOffer() throws IOException {
    if (matchingNodes.size() == 0) {
        return;
    } else {
        System.out.println("\nPurchasing nodes.");

        for (ReservedNodeOffering offering : matchingNodes) {
            printOfferingDetails(offering);
            System.out.println("WARNING: purchasing this offering will incur costs.");
            System.out.println("Purchase this offering [Y or N]?");
            DataInput in = new DataInputStream(System.in);
            String purchaseOpt = in.readLine();
            if (purchaseOpt.equalsIgnoreCase("y")){

                try {
                    PurchaseReservedNodeOfferingRequest request = new
PurchaseReservedNodeOfferingRequest()

.withReservedNodeOfferingId(offering.getReservedNodeOfferingId());
                    ReservedNode reservedNode =
client.purchaseReservedNodeOffering(request);
                    printReservedNodeDetails(reservedNode);
                }
            }
        }
    }
}
```

```
        }
        catch (ReservedNodeAlreadyExistsException ex1){
        }
        catch (ReservedNodeOfferingNotFoundException ex2){
        }
        catch (ReservedNodeQuotaExceededException ex3){
        }
        catch (Exception ex4){
        }
    }
}
System.out.println("Finished.");

}

private static void printOfferingDetails(
    ReservedNodeOffering offering) {
    System.out.println("\nOffering Match:");
    System.out.format("Id: %s\n", offering.getReservedNodeOfferingId());
    System.out.format("Node Type: %s\n", offering.getNodeType());
    System.out.format("Fixed Price: %s\n", offering.getFixedPrice());
    System.out.format("Offering Type: %s\n", offering.getOfferingType());
    System.out.format("Duration: %s\n", offering.getDuration());
}

private static void printReservedNodeDetails(ReservedNode node) {
    System.out.println("\nPurchased Node Details:");
    System.out.format("Id: %s\n", node.getReservedNodeOfferingId());
    System.out.format("State: %s\n", node.getState());
    System.out.format("Node Type: %s\n", node.getNodeType());
    System.out.format("Start Time: %s\n", node.getStartTime());
    System.out.format("Fixed Price: %s\n", node.getFixedPrice());
    System.out.format("Offering Type: %s\n", node.getOfferingType());
    System.out.format("Duration: %s\n", node.getDuration());
}
}
// snippet-end:[redshift.java.ListAndPurchaseReservedNodeOffering.complete]
```

Adquisición de una oferta de nodo reservado mediante la AWS CLI y la API de Amazon Redshift

Puede utilizar las siguientes operaciones de AWS CLI para adquirir las ofertas de nodos reservados.

- [purchase-reserved-node-offering](#)
- [describe-reserved-node-offerings](#)
- [describe-orderable-cluster-options](#)

Puede utilizar las siguientes operaciones la API de Amazon Redshift para adquirir las ofertas de nodos reservados.

- [PurchaseReservedNodeOffering](#)
- [DescribeReservedNodeOfferings](#)
- [DescribeOrderableClusterOptions](#)

Seguridad en Amazon Redshift

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube—AWS es responsable de proteger la infraestructura en la que se ejecutan los servicios de AWS. La nube de AWS también le proporciona servicios que puede utilizar de forma segura. Auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información acerca de los programas de conformidad que se aplican a Amazon Redshift, consulte [AWS Servicios de en el ámbito del programa de conformidad](#).
- Seguridad en la nube— Su responsabilidad está determinada por el AWS que utilice. Usted también es responsable de otros factores incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

El acceso a los recursos de Amazon Redshift se controla en cuatro niveles:

- Administración de clústeres La capacidad para crear, configurar y eliminar clústeres se controla mediante los permisos que se conceden al usuario o la cuenta de IAM asociados a las credenciales de seguridad. Los usuarios de IAM con los permisos adecuados pueden utilizar el AWS Management Console, AWS Command Line Interface (CLI) o la interfaz de programación de aplicaciones (API, Interfaz de programación de aplicaciones) de Amazon Redshift para administrar sus clústeres. Este acceso se administra al usar políticas de IAM. Para obtener más información, consulte [Administración de identidades y accesos en Amazon Redshift](#) (p. 304).
- Conectividad de clústeres Los grupos de seguridad de Amazon Redshift especifican las instancias de que tienen autorización para conectarse a un clúster de Amazon Redshift en formato CIDR (Enrutamiento entre dominios sin clases). Para obtener más información acerca de cómo crear grupos de seguridad de Amazon Redshift, Amazon EC2 y Amazon VPC y cómo asociarlos a clústeres, consulte [Grupos de seguridad de clúster de Amazon Redshift](#) (p. 390).
- Acceso a la base de datos La capacidad para obtener acceso a objetos de la base de datos, como tablas y vistas, se controla mediante las cuentas de usuario de la base de datos de Amazon Redshift. Los usuarios solo pueden obtener acceso a los recursos de la base de datos para los cuales sus cuentas de usuario han recibido permiso. Puede crear estas cuentas de usuario de Amazon Redshift y administrar los permisos de mediante la [CREAR USUARIO](#), [CREAR GRUPO](#), [CONCESIÓN](#), y [REVOCAR](#) Instrucción SQL. Para obtener más información, consulte [Administración de la seguridad de bases de datos](#) En la Guía de desarrollador de base de datos de Amazon Redshift.
- Credenciales temporales de bases de datos e inicio de sesión único —Además de crear y administrar usuarios de base de datos mediante comandos SQL, como CREATE USER y ALTER USER, puede configurar el cliente SQL con controladores JDBC u ODBC de personalizados de Amazon Redshift. Estos controladores administran el proceso de creación de usuarios de bases de datos y contraseñas temporales como parte del proceso de inicio de sesión en la base de datos.

Los controladores autentican a los usuarios de la base de datos en función de la autenticación de AWS Identity and Access Management (IAM). Si ya gestiona identidades de usuario fuera de AWS Puede utilizar un proveedor de identidad compatible con SAML 2.0 para administrar el acceso a los recursos de Amazon Redshift. Utilice un rol de IAM para configurar su IdP y AWS Para permitir que los usuarios federados generen credenciales de base de datos temporales e inicien sesión en bases de datos de

Amazon Redshift. Para obtener más información, consulte [Uso de la autenticación de IAM para generar credenciales de usuario de base de datos](#) (p. 324).

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Amazon Redshift. En los siguientes temas, se le mostrará cómo configurar Amazon Redshift para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros AWS Servicios de Amazon Redshift que le ayudan a supervisar y proteger sus recursos de Amazon Redshift.

Temas

- [Protección de datos en Amazon Redshift](#) (p. 284)
- [Administración de identidades y accesos en Amazon Redshift](#) (p. 304)
- [Registro y monitoreo en Amazon Redshift](#) (p. 373)
- [Validación de la conformidad para Amazon Redshift](#) (p. 388)
- [Resiliencia en Amazon Redshift](#) (p. 388)
- [Seguridad de la infraestructura en Amazon Redshift](#) (p. 389)
- [Configuración y análisis de vulnerabilidades en Amazon Redshift](#) (p. 409)

Protección de datos en Amazon Redshift

La [AWS Modelo de responsabilidad compartida](#) se aplica a la protección de datos en Amazon Redshift. Tal como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Este contenido incluye la configuración de seguridad y las tareas de administración de los servicios de AWS que usted utiliza. Para obtener más información acerca de la privacidad de los datos, consulte las [Preguntas frecuentes sobre la privacidad de datos](#). Para obtener información acerca de la protección de datos en Europa, consulte la publicación de blog [The AWS Shared Responsibility Model and GDPR](#) en el Blog de seguridad de AWS.

Para fines de protección de datos, le recomendamos proteger las credenciales de la cuenta de AWS y configurar cuentas de usuario individuales con AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También le recomendamos proteger sus datos de las siguientes formas:

- Utilice Multi-Factor Authentication (MFA) con cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Le recomendamos TLS 1.2 o una versión posterior.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de AWS.
- Utilice avanzados servicios de seguridad administrados, como Amazon Macie, que le ayuden a detectar y proteger los datos personales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de enlace de FIPS. Para obtener más información acerca de los puntos de enlace de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-2](#).

Le recomendamos encarecidamente que no incluya nunca información de identificación confidencial (por ejemplo, direcciones de correo electrónico de sus clientes) en etiquetas o campos de formato libre, como un Nombre. Esto incluye cuando trabaje con Amazon Redshift u otros AWS utilizando la consola, API, AWS CLI, o bien AWS SDK de. Los datos que introduzca en etiquetas o campos de formato libre utilizados para

los nombres se pueden utilizar para los registros de facturación o de diagnóstico. Cuando proporcione una URL a un servidor externo, no incluya información de credenciales en la URL para validar la solicitud para ese servidor.

AQUA (Advanced Query Accelerator) es un servicio multitenant que se ejecuta en servidores independientes del clúster de Amazon Redshift. AQUA admite la autenticación, el cifrado, el aislamiento y el cumplimiento normativo para mantener sus datos en reposo y los datos en tránsito seguros. Los mismos permisos para acceder a Amazon Redshift se utilizan para AQUA. Las consultas procesadas en servidores AQUA se ejecutan en procesos aislados para garantizar la protección de datos.

Cifrado de datos

La protección de datos se refiere a salvaguardarlos en tránsito (al desplazarse desde y hacia Amazon Redshift en reposo (almacenado en discos en centros de datos de Amazon Redshift). Los datos en tránsito se pueden proteger mediante el uso de SSL o cifrado del lado del cliente. Dispone de las siguientes opciones para proteger datos en reposo en Amazon Redshift.

- Uso del cifrado en el servidor: solicita a Amazon Redshift que cifre sus datos antes de guardarlos en discos de sus centros de datos y los descifre al descargarlo.
- Uso del cifrado del lado del cliente: Puede cifrar datos en el cliente y cargar los datos cifrados en Amazon Redshift. En este caso, administra el proceso de cifrado, las claves de cifrado y las herramientas relacionadas.

Cifrado en reposo

El cifrado del lado del servidor se aplica a los datos en reposo, es decir, Amazon Redshift cifra opcionalmente sus datos a medida que escribe en ellos en sus centros de datos y los descifra cuando usted accede a ellos. Siempre que autentique su solicitud y tenga permiso de acceso, no existe diferencia alguna en la forma de obtener acceso a datos cifrados o sin cifrar.

Amazon Redshift protege los datos en reposo a través del cifrado. De forma opcional, puede proteger todos los datos almacenados en discos en un clúster y todas las copias de seguridad en Amazon S3 con Advanced Encryption Standard AES-256.

Para gestionar las claves que se utilizan para cifrar y descifrar los recursos de Amazon Redshift, debe utilizar [AWS Key Management Service \(AWS KMS\)](#). AWS KMS combina hardware y software seguros de alta disponibilidad para ofrecer un sistema de administración de claves adaptado a la nube. Si utiliza AWS KMS, puede crear claves de cifrado y definir las políticas que controlan cómo se pueden utilizar dichas claves. AWS KMS es compatible con AWS CloudTrail, lo que permite auditar el uso de claves para comprobar que las claves se utilizan de forma adecuada. Puede usar su AWS KMS en combinación con Amazon Redshift y compatibles AWS Servicios de.. Para obtener una lista de los servicios compatibles con AWS KMS, consulte [Cómo de AWS Uso de los servicios AWS KMS](#) en la [AWS Key Management Service Guía para desarrolladores](#).

AQUA (Advanced Query Accelerator) recibe y utiliza las mismas claves de cifrado de base de datos (DEK) utilizadas por Amazon Redshift para almacenar las instantáneas de datos en Amazon S3. Amazon Redshift utiliza el cifrado de sobres, lo que significa que puede rotar claves sin tener que volver a cifrar los bloques de datos. Si el clúster de Amazon Redshift no está cifrado, AQUA utiliza sus propias claves administradas para cifrar los datos. Para obtener más información, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

En algunos casos, puede revocar AWS KMS acceso a un rol de IAM asociado a un clúster. Si es así, una vez completadas las consultas en vuelo, no es posible acceder más a los datos almacenados en caché en AQUA. Esto se debe a que AQUA no persiste claves más allá de un solo escaneo presionado hacia abajo o operación agregada. Esta falta de persistencia también significa que no se puede acceder a ningún metadato sobre esos bloques.

Temas

- [Cifrado de base de datos de Amazon \(p. 286\)](#)

Cifrado de base de datos de Amazon

En Amazon Redshift, puede habilitar el cifrado de base de datos en sus clústeres para proteger los datos en reposo. Cuando habilita el cifrado para un clúster, se cifran los bloques de datos y metadatos del sistema para el clúster y sus instantáneas.

Puede habilitar el cifrado al lanzar el clúster o puede modificar un clúster sin cifrar para que utilice el cifrado AWS Key Management Service (AWS KMS). Para ello, puede usar una AWS o una clave administrada por el cliente (CMK). Cuando modifica el clúster para habilitar el cifrado de KMS, Amazon Redshift migra automáticamente sus datos a un nuevo clúster cifrado. Las instantáneas creadas a partir del clúster cifrado también se cifran. También puede migrar un clúster cifrado a un clúster sin cifrar modificando el clúster y cambiando la opción Encrypt database (Cifrar base de datos). Para obtener más información, consulte [Cambio del cifrado del clúster \(p. 290\)](#).

Aunque el cifrado es un ajuste opcional en Amazon Redshift, recomendamos habilitarlo para los clústeres que contienen información confidencial. Además, es posible que sea obligatorio utilizar cifrado según las directrices o regulaciones que rigen los datos. Por ejemplo, el Estándar de seguridad de datos (Data Security Standard, DSS) del sector de tarjetas de pago (Payment Card Industry, PCI), la Ley de Sarbanes-Oxley (SOX), la Ley de Portabilidad y Responsabilidad de Seguros Médicos (Health Insurance Portability and Accountability Act, HIPAA) y otras regulaciones similares proporcionan directrices para el manejo de tipos específicos de datos.

Amazon Redshift utiliza una jerarquía de claves de cifrado para cifrar la base de datos de. Puede usar AWS Key Management Service (AWS KMS) o un módulo de seguridad por hardware (HSM) para administrar las claves de cifrado de nivel superior en esta jerarquía. El proceso que utiliza Amazon Redshift para el cifrado varía según la manera en que administra las claves. Amazon Redshift se integra automáticamente con AWS KMS pero no con un HSM. Cuando utiliza un HSM, debe utilizar certificados de cliente y servidor para configurar una conexión segura entre Amazon Redshift y el HSM.

Temas

- [Cifrado de base de datos de Amazon Redshift mediante AWS KMS \(p. 286\)](#)
- [Cifrado para Amazon Redshift mediante módulos de seguridad de hardware \(p. 288\)](#)
- [Rotación de claves de cifrado en Amazon Redshift \(p. 289\)](#)
- [Cambio del cifrado del clúster \(p. 290\)](#)
- [Configuración del cifrado de la base de datos mediante la consola \(p. 294\)](#)
- [Configuración del cifrado de la base de datos mediante la API de Amazon Redshift y la de AWS CLI \(p. 300\)](#)

Cifrado de base de datos de Amazon Redshift mediante AWS KMS

Cuando elige AWS KMS para gestionar las claves de Amazon Redshift, hay una jerarquía de cuatro niveles de claves de cifrado. Estas claves, en orden jerárquico, son la clave maestra, una clave de cifrado de clúster (CEK), una clave de cifrado de base de datos (DEK) y claves de cifrado de datos.

Cuando se lanza el clúster, Amazon Redshift devuelve una lista de las claves maestras de cliente (CMK) que la AWS ha creado o tiene permiso para usar en AWS KMS. Seleccione una CMK para utilizar como la clave maestra en la jerarquía de cifrado.

De forma predeterminada, Amazon Redshift selecciona la clave predeterminada como la clave maestra. La clave de predeterminada es una AWS que se crea para su AWS para usar en Amazon Redshift. AWS KMS crea esta clave la primera vez que inicia un clúster cifrado en un AWS Región y elija la clave predeterminada.

Si no desea utilizar la clave predeterminada, debe tener (o crear) otra CMK administrada por el cliente en AWS KMS antes de iniciar el clúster en Amazon Redshift. Las CMK administradas por el cliente le ofrecen una mayor flexibilidad, incluida la opción de crear, rotar, desactivar, definir los controles de acceso y auditar las claves de cifrado utilizadas para proteger los datos. Para obtener más información acerca de la creación de CMK, consulte [Creación de claves](#) en la AWS Key Management Service Guía para desarrolladores.

Si desea usar un tipo de propiedad AWS KMS clave de otra AWS En Amazon Redshift, debe tener permiso para utilizar la clave y especificar su nombre de recurso de Amazon (ARN). Para obtener más información acerca del acceso a claves en AWS KMS, consulte [Control del acceso a las claves](#) en la AWS Key Management Service Guía para desarrolladores.

Después de elegir una clave maestra, Amazon Redshift solicita que AWS KMS Genere una clave de datos y cifrarla mediante la clave maestra seleccionada. Esta clave de datos se utiliza como CEK en Amazon Redshift. AWS KMS exporta la CEK cifrada a Amazon Redshift, donde se almacena internamente en el disco en una red separada del clúster junto con la autorización de la CMK y el contexto de cifrado de la CEK. Solo se exporta el CEK cifrado a Amazon Redshift; el CMK permanece en AWS KMS. Amazon Redshift también transfiere la CEK cifrada a través de un canal seguro al clúster y la carga en la memoria. A continuación, Amazon Redshift llama a AWS KMS para descifrar la CEK y cargar la CEK descifrada en la memoria. Para obtener más información acerca de concesiones, contexto de cifrado y otros AWS KMS conceptos relacionados, consulte [Conceptos](#) en la AWS Key Management Service Guía para desarrolladores.

A continuación, Amazon Redshift genera aleatoriamente una clave para utilizarla como la DEK y la carga en la memoria del clúster. El CEK descifrado se utiliza para cifrar la DEK, que luego se pasa a través de un canal seguro desde el clúster para ser almacenada internamente por Amazon Redshift en el disco, en una red separada del clúster. Como sucede con la CEK, ambas versiones cifradas y descifradas de la DEK se cargan en la memoria del clúster. La versión descifrada de la DEK se utiliza posteriormente para cifrar las claves de cifrado individuales que se generan aleatoriamente para cada bloque de datos de la base de datos.

Cuando se reinicia el clúster, Amazon Redshift arranca con las versiones cifradas almacenadas internamente de la CEK y la DEK, las vuelve a cargar en la memoria y ejecuta AWS KMS para descifrar el CEK con el CMK de nuevo para que pueda cargarse en la memoria. La CEK descifrada se utiliza posteriormente para descifrar la DEK nuevamente, y la DEK descifrada se carga en la memoria y se utiliza para cifrar y descifrar las claves de bloque de datos según sea necesario.

Para obtener más información acerca de la creación de clústeres de Amazon Redshift cifrados con AWS KMS claves, consulte [Creación de un clúster](#) (p. 47) y [Administración de clústeres a través de la AWS CLI API de Amazon Redshift](#) (p. 72).

[Copiar AWS KMS—instantáneas cifradas en otro AWS Región](#)

AWS KMS Las claves de son específicas de AWS Región . Si habilita la copia de instantáneas de Amazon Redshift a otro AWS Región, y el clúster de origen y sus instantáneas se cifran mediante una clave maestra de AWS KMS, debe configurar una concesión para que Amazon Redshift utilice una clave maestra en el destino AWS Región . Esta autorización permite a Amazon Redshift cifrar instantáneas en el destino AWS Región . Para obtener más información acerca de la copia de instantáneas entre regiones, consulte [Copia de instantáneas en otro AWS Región](#) (p. 242).

Note

Si habilita la copia de instantáneas desde un clúster cifrado y utiliza AWS KMS como la clave maestra, no puede cambiar el nombre del clúster ya que el nombre del clúster es parte del contexto de cifrado. Si debe cambiarle el nombre al clúster, puede deshabilitar la copia de instantáneas en la AWS Pasos para cambiar el nombre del clúster y, luego, configurar y habilitar la copia de instantáneas nuevamente.

A continuación se detalla el proceso para configurar la autorización para la copia de instantáneas.

1. En destinoAWSRegión, cree una autorización de copia de instantáneas a través de las siguientes acciones:
 - Si no dispone de una clave de AWS KMS, cree una. Para obtener más información acerca de la creación deAWS KMSclaves, consulte[Creación de claves](#)en laAWS Key Management ServiceGuía para desarrolladores.
 - Especifique un nombre para la autorización de copia de instantáneas. Este nombre debe ser único enAWSRegión para suAWSaccount.
 - Especifique el ID de la clave de AWS KMS para la que crea la autorización. Si no especifica un ID de clave, la autorización se aplica a la clave predeterminada.
2. En la fuenteAWSRegión, habilite la copia de instantáneas y especifique el nombre de la autorización de copia de instantáneas que creó en el destinoAWSRegión .

Este proceso anterior sólo es necesario si habilita la copia de instantáneas mediante laAWS CLI, la API de Amazon Redshift o los SDK. Si utiliza la consola, Amazon Redshift proporciona el flujo de trabajo adecuado para configurar la autorización cuando habilita la copia de instantáneas entre regiones. Para obtener más información acerca de la configuración para copiar instantáneas entre regiones con clústeres cifrados por AWS KMS mediante la consola, consulte [Configuración de la copia de una instantánea entre regiones para unAWS KMS—clúster cifrado](#) (p. 263).

Antes de copiar la instantánea en el destinoAWSRegión, Amazon Redshift descifra la instantánea mediante la clave maestra del origenAWSRegione y lo vuelve a cifrar temporalmente utilizando una clave RSA generada aleatoriamente que Amazon Redshift gestiona internamente. A continuación, Amazon Redshift copia la instantánea a través de un canal seguro en el destinoAWSRegión, descifra la instantánea mediante la clave RSA administrada internamente y, a continuación, vuelve a cifrar la instantánea mediante la clave maestra en elAWSRegión .

Para obtener más información acerca de la configuración de autorizaciones para copiar instantáneas de clústeres cifrados con AWS KMS, consulte [Configuración de Amazon Redshift para utilizarAWS KMSmediante la API de Amazon RedshiftAWS CLI](#) (p. 300).

Cifrado para Amazon Redshift mediante módulos de seguridad de hardware

Si no usaAWS KMSPara la administración de claves, puede utilizar un módulo de seguridad por hardware (HSM) para administrar las claves con Amazon Redshift.

Important

No se admite el cifrado de HSM para los tipos de nodos DC2 y RA3.

Los HSM son dispositivos que proporcionan control directo de la generación y administración de claves. Ofrecen una mayor seguridad, ya que separan la administración de claves de las capas de aplicación y base de datos. Amazon Redshift admiteAWS CloudHSMClásico para la administración de claves. El proceso de cifrado es diferente cuando usa HSM para administrar las claves de cifrado en lugar de AWS KMS.

Important

Amazon RedshiftAWS CloudHSMClassic. No se admite la versión más reciente deAWS CloudHSMServicio de.

AWS CloudHSMClassic está cerrado a nuevos clientes. Para obtener más información, consulte[Precios de CloudHSM Classic](#).AWS CloudHSM Clásico no está disponible en todos losAWSRegiones de. Para obtener más información acerca deAWSRegiones, consulte[AWSTabla de regiones](#).

Cuando configura el clúster para utilizar un HSM, Amazon Redshift envía una solicitud al HSM para generar y almacenar una clave para utilizar como la CEK. Sin embargo, a diferencia deAWS KMS, el HSM no exporta la CEK a Amazon Redshift. En cambio, Amazon Redshift genera aleatoriamente la DEK en el clúster y la pasa al HSM para ser cifrada por la CEK. El HSM devuelve la DEK cifrada a Amazon Redshift, donde se cifra aún más utilizando una clave maestra interna generada de forma aleatoria que se guarda

internamente en el disco, en una red separada del clúster. Amazon Redshift también carga la versión descifrada de la DEK en la memoria del clúster para que puede utilizarse para cifrar y descifrar las claves concretas de los bloques de datos.

Si se reinicia el clúster, Amazon Redshift descifra la DEK con doble cifrado almacenada internamente a través de la clave maestra interna para devolver la DEK almacenada internamente al estado cifrado por CEK. A continuación, la DEK cifrada por CEK se pasa al HSM para descifrarse y pasarse nuevamente a Amazon Redshift, donde se puede cargar en la memoria nuevamente para utilizarla con las claves de bloque de datos individuales.

Configuración de una conexión segura entre Amazon Redshift y un HSM

Cuando elige utilizar un HSM para la administración de la clave del clúster, necesita configurar un enlace de red segura entre Amazon Redshift y el HSM. Para hacerlo, necesita configurar los certificados de cliente y servidor. La conexión segura se utiliza para pasar las claves de cifrado entre el HSM y Amazon Redshift durante las operaciones de cifrado y descifrado.

Amazon Redshift crea un certificado de cliente público desde un key pair privadas y públicas generado aleatoriamente. Estas se cifran y almacenan internamente. Descargue y registre el certificado de cliente público en el HSM, y asígnelo a la partición de HSM aplicable.

Puede proporcionar a Amazon Redshift la dirección IP de HSM, el nombre de partición de HSM, la contraseña de partición de HSM y un certificado de servidor de HSM público, que se cifra utilizando una clave maestra interna. Amazon Redshift completa el proceso de configuración y verifica que pueda conectarse al HSM. Si no puede conectarse, el clúster se coloca en el estado INCOMPATIBLE_HSM y no se crea. En este caso, debe eliminar el clúster incompleto y volver a intentarlo.

Important

Cuando modifica el clúster para utilizar una partición de HSM diferente, Amazon Redshift verifica que puede conectarse a la nueva partición, pero no verifica si existe una clave cifrada válida. Antes de usar la nueva partición, debe replicar las claves en la nueva partición. Si el clúster se reinicia y Amazon Redshift no puede encontrar una clave válida, el reinicio produce un error. Para obtener más información, consulte [Replicación de claves en varios HSM](#).

Para obtener más información acerca de cómo configurar Amazon Redshift para que utilice un HSM, consulte [Configuración de Amazon Redshift para utilizar un HSM mediante la consola de Amazon Redshift \(p. 294\)](#) y [Configuración de Amazon Redshift para utilizar un HSM mediante la API de Amazon Redshift y AWS CLI \(p. 301\)](#).

Después de la configuración inicial, si Amazon Redshift no puede conectarse al HSM, se registra un evento. Para obtener más información acerca de estos eventos, consulte [Notificaciones de eventos de Amazon Redshift](#).

Rotación de claves de cifrado en Amazon Redshift

En Amazon Redshift puede cambiar las claves de cifrado para los clústeres cifrados. Cuando se inicia el proceso de rotación de claves, Amazon Redshift cambia la CEK del clúster especificado y de cualquier instantánea automatizada o manual de dicho clúster. Amazon Redshift también cambia la DEK del clúster especificado, pero no puede cambiar la DEK de las instantáneas mientras están almacenadas internamente en Amazon Simple Storage Service (Amazon S3) y permanecen cifradas con la DEK existente.

Mientras la rotación está en curso, el clúster entra en el estado ROTATING_KEYS hasta que finaliza el proceso, momento en el que vuelve al estado AVAILABLE. Amazon Redshift gestiona el descifrado y el re-cifrado durante el proceso de rotación de claves.

Note

No puede cambiar claves para instantáneas que no tienen un clúster de origen. Antes de eliminar un clúster, verifique si sus instantáneas dependen de una rotación de claves.

Debido a que el clúster no está disponible momentáneamente durante el proceso de rotación de claves, debe cambiar las claves solo cuando lo requieran los datos o cuando sospeche que las claves están en riesgo. Como práctica recomendada, debe revisar el tipo de datos que almacena y planificar la frecuencia con la que cambia las claves que cifran esos datos. La frecuencia de la rotación de claves varía según las políticas corporativas de seguridad de datos y cualquier estándar que se refiera a información confidencial y conformidad normativa. Asegúrese de que el plan equilibre las necesidades de seguridad con las consideraciones de disponibilidad para el clúster.

Para obtener más información acerca de rotación de claves, consulte [Rotación de las claves de cifrado mediante la consola de Amazon Redshift](#) (p. 299) y [Rotación de las claves de cifrado mediante la API de Amazon Redshift y la deAWS CLI](#) (p. 301).

Cambio del cifrado del clúster

Puede modificar un clúster no cifrado para utilizarAWS Key Management Service(AWS KMS), utilizando unAWS o una clave administrada por el cliente (CMK). Cuando modifica el clúster para habilitar el cifrado de KMS, Amazon Redshift migra automáticamente sus datos a un nuevo clúster cifrado. También puede migrar un clúster no cifrado a un clúster cifrado modificando el clúster.

Durante la operación de migración, el clúster se encuentra disponible en modo de solo lectura y su estado es resizing (cambiando tamaño).

Si el clúster está configurado para habilitarAWSCopia de instantáneas de región, debe deshabilitarla antes de cambiar el cifrado. Para obtener más información, consulte [Copia de instantáneas en otroAWSRegión](#) (p. 242) y [Configuración de la copia de una instantánea entre regiones para unAWS KMS—clúster cifrado](#) (p. 263). No puede habilitar el cifrado de Hardware Security Module (HSM, Módulo de seguridad de hardware) modificando el clúster. En lugar de ello, debe crear un nuevo clúster cifrado con HSM y migrar los datos al nuevo clúster. Para obtener más información, consulte [Migración a un clúster cifrado con HSM](#) (p. 292) .

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para modificar el cifrado de la base de datos en un clúster

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, elijaCLÚSTERES DEy, luego, seleccione el clúster que desea modificar el cifrado.
3. Seleccione Properties (Propiedades).
4. En el navegadorConfiguración de las bases, elijaEditary, después, elijaEditar cifrado.
5. Elija una de las opciones de cifrado y elijaGuardar cambios.

Consola original

Para cambiar el cifrado de un clúster mediante la consola

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Clusters (Clústeres) y elija el clúster que desee modificar.
3. Elija Cluster y, a continuación, seleccione Modify (Modificar).

4. En Encrypt database (Cifrar base de datos), elija KMS para habilitar el cifrado o elija None (Ninguno) para deshabilitar el cifrado.
5. Para utilizar una clave administrada por el cliente, para Master Key (Clave principal) elija Enter a key ARN (Escriba el ARN de clave) y escriba el ARN en el campo ARN.

Modify cluster

Cluster settings
Maintenance settings

Cluster identifier ⓘ

Cluster parameter group ⓘ

Parameter group description Default parameter group for redshift-1.0 ⓘ

Encrypt database ☐ None ☒ KMS ☐ HSM

Master key

Description Default master key that protects my Redshift clus

Account This account (555555555555)

KMS key ID arn:aws:kms:us-east-1:123456789012:key:12345678-1234-1234-1234-123456789012

Cluster security groups ⓘ

Master user password ⓘ

Automated snapshot retention period days ⓘ

6. Elija Modify.

Para cambiar el cifrado de un clúster mediante la CLI

Para modificar su clúster sin cifrar para usar KMS, ejecute el comando de la CLI `modify-cluster` y especifique `--encrypted`, tal como se muestra a continuación. De forma predeterminada, se utiliza la clave de KMS predeterminada. Para especificar una clave administrada por el cliente, incluya la opción `--kms-key-id`.

```
aws redshift modify-cluster --cluster-identifier <value> --encrypted --kms-key-id <value>
```

Para quitar el cifrado de su clúster, ejecute el siguiente comando de la CLI.

```
aws redshift modify-cluster --cluster-identifier <value> --no-encrypted
```

Migración a un clúster cifrado con HSM

Para migrar un clúster sin cifrar a un clúster cifrado mediante un módulo de seguridad de hardware (HSM), debe crear un nuevo clúster cifrado y trasladar los datos al nuevo clúster. No puede realizar una migración a un clúster cifrado con HSM modificando el clúster.

Para migrar de un clúster sin cifrar a un clúster cifrado con HSM, primero debe descargar los datos del clúster de origen existente. A continuación, vuelva a cargar los datos en un clúster nuevo, o clúster de destino, con la configuración de cifrado que desee. Para obtener más información sobre cómo lanzar un clúster cifrado, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

Durante el proceso de migración, el clúster de origen está disponible para consultas de solo lectura hasta el último paso. El último paso consiste en cambiar el nombre de los clústeres de destino y de origen, lo que cambia los puntos de enlace para que todo el tráfico se dirija al nuevo clúster de destino. El clúster de destino no está disponible hasta que se reinicia después de cambiarle el nombre. Suspenda todas las cargas de datos y otras operaciones de escritura en el clúster de origen mientras durante la transferencia de los datos.

Para preparar la migración

1. Identifique todos los sistemas dependientes que interactúan con Amazon Redshift, por ejemplo, las herramientas de inteligencia empresarial (BI) y los sistemas de extracción, transformación y carga (ETL).
2. Identifique las consultas de validación que permiten probar la migración.

Por ejemplo, puede utilizar la consulta siguiente para buscar el número de tablas definidas por el usuario.

```
select count(*)
from pg_table_def
where schemaname != 'pg_catalog';
```

La consulta siguiente devuelve una lista de todas las tablas definidas por el usuario y el número de filas de cada tabla.

```
select "table", tbl_rows
from svv_table_info;
```

3. Elija un buen momento para la migración. Para encontrar un momento en el que el uso del clúster sea mínimo, monitoree las métricas del clúster, como la utilización de la CPU y el número de conexiones a la base de datos. Para obtener más información, consulte [Visualización de datos de rendimiento del clúster \(p. 431\)](#).
4. Elimine las tablas que no se utilicen.

Para crear una lista de tablas con el número de veces que se ha consultado cada tabla, ejecute la consulta siguiente.

```
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. Lance un clúster cifrado nuevo.

Utilice el mismo número de puerto para el clúster de destino que para el clúster de origen. Para obtener más información sobre cómo lanzar un clúster cifrado, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

6. Configure el proceso de descarga y carga.

Puede utilizar la [utilidad Unload/Copy de Amazon Redshift](#) para facilitar la migración de datos entre clústeres. La utilidad exporta los datos del clúster de origen a una ubicación en Amazon S3. Los datos se cifran con AWS KMS. A continuación, la utilidad importa automáticamente los datos en el clúster de destino. También puede utilizar la utilidad para limpiar Amazon S3 una vez finalizada la migración.

7. Ejecute una prueba para verificar el proceso y estimar durante cuánto tiempo deben suspenderse las operaciones de escritura.

Durante las operaciones de descarga y carga, mantenga la consistencia de los datos suspendiendo las cargas de datos y otras operaciones de escritura. Ejecute el proceso de descarga y carga usando una de sus tablas más grandes para realizar una estimación del tiempo.

8. Cree los objetos de base de datos, como esquemas, vistas y tablas. Para ayudarlo a generar las instrucciones de lenguaje de definición de datos (DDL) necesarias, puede utilizar las secuencias de comandos en [AdminViews](#) en la AWS Repositorio de GitHub.

Para migrar el clúster

1. Detenga todos los procesos ETL en el clúster de origen.

Para confirmar que no hay operaciones de escritura en proceso, utilice la consola de administración de Amazon Redshift para monitorizar las IOPS de escritura. Para obtener más información, consulte [Visualización de datos de rendimiento del clúster \(p. 431\)](#).

2. Ejecute las consultas de validación que identificó anteriormente para recopilar información sobre el clúster de origen sin cifrar antes de la migración.
3. (Opcional) Cree una cola de administración de cargas de trabajo (WLM) para utilizar el máximo de recursos disponibles, tanto en el clúster de origen como en el de destino. Por ejemplo, cree una cola denominada `data_migrate` y configúrela con una memoria del 95 por ciento y una simultaneidad de 4. Para obtener más información, consulte [Direccionamiento de consultas a las colas en función de los grupos de usuarios y de consultas](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.
4. Ejecute `UnloadCopyUtility` utilizando la cola `data_migrate`.

Monitoree el proceso de UNLOAD y COPY mediante la consola de Amazon Redshift.

5. Vuelva a ejecutar las consultas de validación y verifique que los resultados coinciden con los del clúster de origen.
6. Cambie el nombre de los clústeres de origen y de destino para intercambiar los puntos de enlace. Para evitar interrupciones, realice esta operación fuera del horario normal de trabajo.
7. Compruebe que puede conectarse al clúster de destino utilizando todos sus clientes SQL, como las herramientas de ETL y de generación de informes.
8. Cierre el clúster de origen sin cifrar.

Configuración del cifrado de la base de datos mediante la consola

Puede utilizar la consola de Amazon Redshift para configurar Amazon Redshift a fin de utilizar un HSM y rotar las claves de cifrado. Para obtener información acerca de cómo crear clústeres con AWS KMS claves de cifrado, consulte [Creación de un clúster](#) (p. 47) y [Administración de clústeres a través de la AWS CLI API de Amazon Redshift](#) (p. 72).

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para modificar el cifrado de la base de datos en un clúster

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y elija el clúster del que desee mover las instantáneas.
3. En Actions (Acciones), seleccione Modify (Modificar) para mostrar la página de configuración.
4. En la sección de Database configuration (Configuración de la base de datos), elija la configuración de Encryption (Cifrado) y luego seleccione Modify cluster (Modificar clúster).

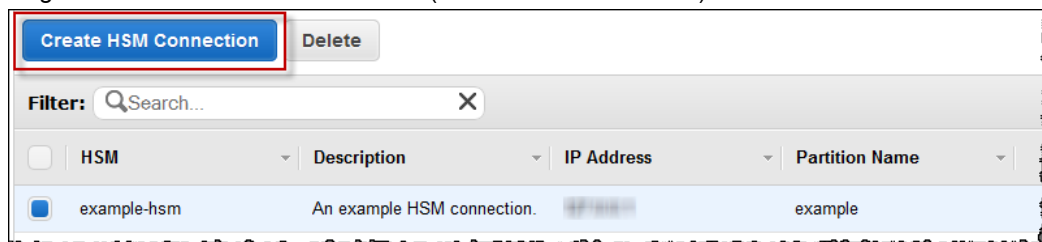
Consola original

Configuración de Amazon Redshift para utilizar un HSM mediante la consola de Amazon Redshift

Puede utilizar los siguientes procedimientos para especificar información sobre la conexión y la configuración de un HSM en Amazon Redshift a través de la consola de Amazon Redshift.

Para crear una conexión de HSM

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, haga clic en Security (Seguridad) y en la pestaña HSM Connections (Conexiones de HSM).
3. Haga clic en Create HSM Connection. (Crear conexión de HSM)



4. En la página Create HSM Connection (Crear conexión de HSM), escriba la siguiente información:
 - a. En el cuadro HSM Connection Name (Nombre de conexión de HSM), escriba un nombre para identificar esta conexión.
 - b. En el cuadro Description (Descripción), escriba una descripción de la conexión.
 - c. En el cuadro HSM IP Address (Dirección IP de HSM), escriba la dirección IP del HSM.
 - d. En el navegador Nombre de partición de HSM, escriba el nombre de la partición a la que debe conectarse Amazon Redshift.

- e. En el cuadro HSM Partition Password (Contraseña de partición de HSM), escriba la contraseña requerida para conectarse a la partición de HSM.
- f. Copie el certificado de servidor público del HSM y péguelo en el cuadro Paste the HSM's public server certificate here (Pegue aquí el certificado de servidor público de HSM).
- g. Seleccione Create (Crear).

Create HSM Connection

Provide an identifier and description to designate this connection:

HSM Connection Name* ⓘ

Description* ⓘ

Enter the details required for connecting to the HSM below. Please note: only SafeNet HSMs are supported.

HSM IP Address* ⓘ

HSM Partition Name* ⓘ

HSM Partition Password*

Confirm HSM Partition Password*

Paste the HSM's public server certificate here*

ⓘ

*Required

5. Después de que se crea la conexión, puede crear un certificado de cliente del HSM. Si desea crear un certificado de cliente de HSM inmediatamente después de crear la conexión, haga clic en Yes (Sí) y complete los pasos del siguiente procedimiento. De lo contrario, haga clic en Not now (Ahora no) para volver a la lista de conexiones de HSM y completar el resto del proceso en otro momento.

Create HSM Connection

✓ Your HSM Connection **example-hsm** was successfully created.

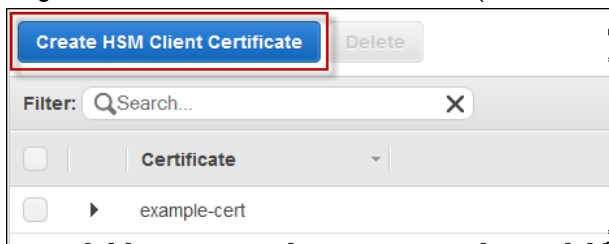
In order to configure a cluster to use this HSM configuration, you must also create an HSM client certificate. You can do this now or you may do it later (if you not have done so already).

Would you like to create an HSM client certificate now?

*Required

Para crear un certificado de cliente del HSM

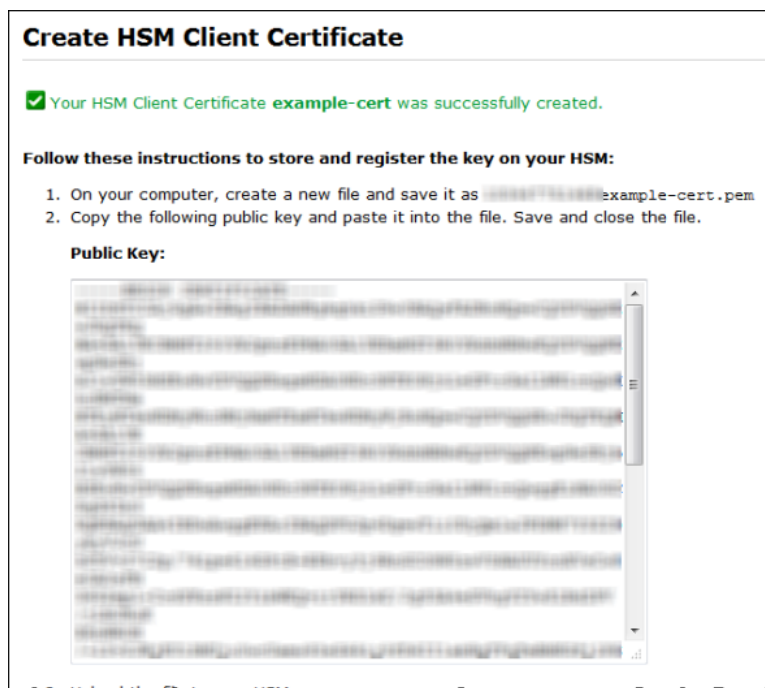
1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, haga clic en Security (Seguridad) y en la pestaña HSM Certificates (Certificados de HSM).
3. Haga clic en Create HSM Client Certificate (Crear certificado de cliente de HSM).



4. En la página Create HSM Client Certificate (Crear certificado de cliente de HSM), escriba un nombre en el cuadro HSM Client Certificate Identifier (Identificador del certificado de cliente de HSM) para identificar este certificado de cliente.

A screenshot of the 'Create HSM Client Certificate' form. The title 'Create HSM Client Certificate' is at the top. Below it, there is a label 'HSM Client Certificate Identifier*' followed by a text input field containing the value 'example-cert'. To the right of the input field is an information icon (a lowercase 'i' inside a circle). At the bottom left of the form, there is a note '*Required'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

5. Seleccione Siguiente.
6. Después de que se crea el certificado, aparece una página de confirmación con información para registrar la clave en el HSM. Si no tiene permiso para configurar el HSM, coordine los siguientes pasos con un administrador de HSM.



- a. Abra un nuevo archivo de texto en su equipo.
 - b. En la consola de Amazon Redshift, en la pestaña Creación de certificado de cliente HSM, copie la clave pública.
 - c. Pegue la clave pública en el archivo abierto y guárdelo con el nombre de archivo que aparece en el paso 1 de la página de confirmación. Asegúrese de guardar el archivo con la extensión `.pem`, por ejemplo: `123456789mykey.pem`.
 - d. Cargue el archivo `.pem` en el HSM.
 - e. En el HSM, abra una ventana de símbolo del sistema y ejecute los comandos enumerados en el paso 4 de la página de confirmación para registrar la clave. El comando utiliza el siguiente formato, donde `ClientName`, `KeyFilename` y `PartitionName` son valores que debe reemplazar por los suyos propios:


```
client register -client ClientName -hostname KeyFilename
```



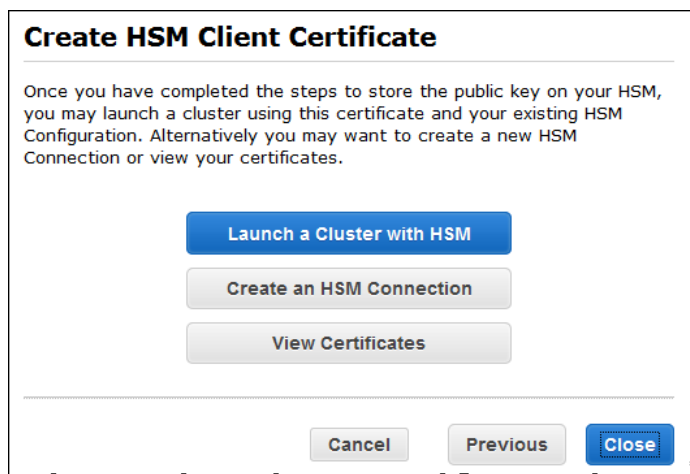
```
client assignPartition -client ClientName -partition PartitionName
```


Por ejemplo:


```
client register -client MyClient -hostname 123456789mykey
```



```
client assignPartition -client MyClient -partition MyPartition
```
 - f. Después de registrar la clave del HSM, haga clic en Next (Siguiente).
7. Después de que se crea y registra el certificado de cliente del HSM, haga clic en uno de los siguientes botones:



- **Launch a Cluster with HSM (Lanzar un clúster con HSM).** Esta opción inicia el proceso de lanzamiento de un clúster nuevo. Durante el proceso, puede seleccionar un HSM para almacenar claves de cifrado. Para obtener más información acerca del proceso de lanzamiento de clústeres, consulte [Administración de clústeres a través de la consola \(p. 44\)](#).

Create an HSM Connection (Crear una conexión de HSM). Esta opción inicia el proceso Create HSM Connection (Crear conexión de HSM).

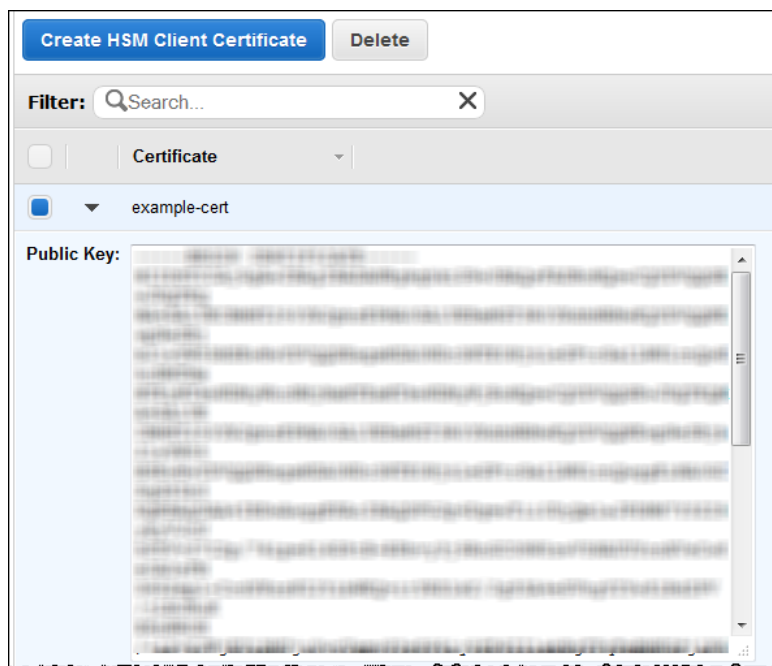
View Certificates (Ver certificados). Esta opción lo lleva de nuevo a HSM en el panel de navegación y muestra una lista de los certificados de cliente en la pestaña Certificates (Certificados).

Previous (Anterior). Esta opción lo lleva de nuevo a la página de confirmación Create HSM Client Certificates (Crear certificados de cliente de HSM).

Close (Cerrar). Esta opción lo lleva de nuevo al HSM del panel de navegación y muestra una lista de las conexiones del HSM en la pestaña Connections (Conexiones).

Para visualizar la clave pública de un certificado de cliente del HSM

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, haga clic en Security (Seguridad) y en la pestaña HSM Certificates (Certificados de HSM).
3. Haga clic en el certificado de cliente del HSM para visualizar la clave pública. Esta clave es la misma que añadió al HSM en el procedimiento anterior, [Para crear un certificado de cliente del HSM \(p. 296\)](#)



Para eliminar una conexión de HSM

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, haga clic en Security (Seguridad) y en la pestaña HSM Connections (Conexiones de HSM).
3. Haga clic en la conexión de HSM que desea eliminar.
4. En el navegadorEliminar conexión de HSM, elija.Eliminarpara eliminar la conexión de Amazon Redshift o elijaCancelVuelva a.conexiones de HMs sin eliminar la conexión.

Para eliminar un certificado de cliente del HSM

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, haga clic en Security (Seguridad) y seleccione la pestaña HSM Certificates (Certificados de HSM).
3. En la lista, haga clic en el certificado de cliente del HSM que desee eliminar.
4. En el navegadorEliminar certificado de cliente de HSM, elija.Eliminarpara eliminar el certificado de Amazon Redshift o elijaCancelVuelva a.Certificadossin eliminar el certificado.

Rotación de las claves de cifrado mediante la consola de Amazon Redshift

Puede utilizar el siguiente procedimiento para rotar las claves de cifrado mediante la consola de Amazon Redshift.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Rotar las claves de cifrado de un clúster.

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTES (CLÚSTERES) y seleccione el clúster del cual desee actualizar las claves de cifrado.
3. Para Actions (Acciones), haga clic en Rotate encryption (Rotar cifrado) para mostrar la página Rotate encryption keys (Rotar claves de cifrado).
4. En la página Rotate encryption keys (Rotar claves de cifrado), haga clic en Rotate encryption keys (Rotar claves de cifrado).

Consola original

Para rotar una clave de cifrado

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En la lista, haga clic en el clúster para el que desea rotar claves.
4. Haga clic en Database (Base de datos) y en Rotate Encryption Keys (Rotar claves de cifrado).
5. Haga clic en Yes, Rotate Keys (Sí, rotar claves) si desea rotar las claves o en Cancel (Cancelar) si no lo desea.

Note

El clúster no estará disponible por un momento hasta que se complete el proceso de rotación de claves.

Configuración del cifrado de la base de datos mediante la API de Amazon Redshift y la deAWS CLI

Utilice la API de Amazon Redshift yAWS Command Line Interface(AWS CLI) para configurar las opciones de clave de cifrado para las bases de datos de Amazon Redshift. Para obtener más información acerca del cifrado de la base de datos, consulte [Cifrado de base de datos de Amazon \(p. 286\)](#).

Configuración de Amazon Redshift para utilizarAWS KMSmediante la API de Amazon RedshiftAWS CLI

Puede utilizar las siguientes acciones de la API de Amazon Redshift para configurar Amazon Redshift para que utiliceAWS KMSClaves de cifrado.

- [CreateCluster](#)
- [CreateSnapshotCopyGrant](#)
- [DescribeSnapshotCopyGrants](#)
- [DeleteSnapshotCopyGrant](#)
- [DisableSnapshotCopy](#)
- [EnableSnapshotCopy](#)

Puede utilizar las siguientes operaciones de CLI de Amazon Redshift para configurar Amazon Redshift para que utiliceAWS KMSClaves de cifrado.

- [create-cluster](#)
- [create-snapshot-copy-grant](#)
- [describe-snapshot-copy-grants](#)
- [delete-snapshot-copy-grant](#)
- [disable-snapshot-copy](#)
- [enable-snapshot-copy](#)

Configuración de Amazon Redshift para utilizar un HSM mediante la API de Amazon Redshift y AWS CLI

Puede utilizar las siguientes acciones de la API de Amazon Redshift para gestionar los módulos de seguridad de hardware.

- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DeleteHsmClientCertificate](#)
- [DeleteHsmConfiguration](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

Puede utilizar las siguientes operaciones de la AWS CLI para administrar los módulos de seguridad de hardware.

- [create-hsm-client-certificate](#)
- [create-hsm-configuration](#)
- [delete-hsm-client-certificate](#)
- [delete-hsm-configuration](#)
- [describe-hsm-client-certificates](#)
- [describe-hsm-configurations](#)

Rotación de las claves de cifrado mediante la API de Amazon Redshift y la de AWS CLI

Puede utilizar las siguientes acciones de la API de Amazon Redshift para rotar las claves de cifrado.

- [RotateEncryptionKey](#)

Puede utilizar las siguientes operaciones de la AWS CLI para rotar las claves de cifrado.

- [rotate-encryption-key](#)

Cifrado en tránsito

Puede configurar su entorno para proteger los datos sobre confidencialidad e integridad en tránsito.

Cifrado de datos en tránsito entre un clúster de Amazon Redshift y clientes SQL mediante JDBC/ODBC:

- Puede conectarse a clústeres de Amazon Redshift desde herramientas de cliente SQL mediante conexiones Java Database Connectivity (JDBC) y Open Database Connectivity (ODBC, Conectividad de base de datos abierta).

- Amazon Redshift admite conexiones de Secure Sockets Layer (SSL) para cifrar datos y certificados de servidor a fin de validar el certificado de servidor al que se conecta el cliente. El cliente se conecta al nodo principal de un clúster de Amazon Redshift. Para obtener más información, consulte [Configuración de las opciones de seguridad para las conexiones \(p. 151\)](#).
- Para admitir conexiones SSL, Amazon Redshift crea e instala AWS Certificate Manager (ACM) emitieron certificados en cada grupo. Para obtener más información, consulte [Migración a certificados de ACM para las conexiones SSL \(p. 155\)](#).
- Para proteger sus datos en tránsito dentro de la AWS en la nube, Amazon Redshift utiliza SSL con aceleración por hardware para comunicarse con Amazon S3 o Amazon DynamoDB para las operaciones COPY, UNLOAD, copia de seguridad y restauración.

Cifrado de datos en tránsito entre un clúster de Amazon Redshift y Amazon S3 o DynamoDB:

- Amazon Redshift utiliza SSL con aceleración por hardware para comunicarse con Amazon S3 o DynamoDB para las operaciones COPY, UNLOAD, copia de seguridad y restauración.
- Redshift Spectrum admite el cifrado del lado de servidor (SSE) de Amazon S3, utilizando la clave predeterminada de su cuenta administrada por la AWS Key Management Service (KMS).
- Cifrado de cargas de Amazon Redshift con Amazon S3 y AWS KMS. Para obtener más información, consulte [Cifra las cargas de Amazon Redshift con Amazon S3 y AWS KMS](#).

Cifrado y firma de datos en tránsito entre AWS CLI, clientes de SDK o API y puntos de enlace de Amazon Redshift:

- Amazon Redshift proporciona puntos de enlace HTTPS para cifrar datos en tránsito.
- Para proteger la integridad de las solicitudes de API a Amazon Redshift, las llamadas a la API deben estar firmadas por el autor de la llamada. Las llamadas están firmadas por un certificado X.509 o la AWS Sigv4, clave de acceso secreta según Proceso de firma de Signature Versión 4 (Sigv4). Para obtener más información, consulte [Signature Version 4 Signing Process](#) en la AWS General Reference.
- Usar AWS CLI o una de las AWS SDK para realizar solicitudes a AWS. Estas herramientas firman automáticamente las solicitudes con la clave de acceso especificada al configurar las herramientas.

Cifrado de datos en tránsito entre los clústeres de Amazon Redshift y AQUA:

- Los datos se transmiten entre los clústeres AQUA y Amazon Redshift a través de un canal cifrado TLS. Este canal está firmado según Proceso de firma de Signature Versión 4 (Sigv4). Para obtener más información, consulte [Signature Version 4 Signing Process](#) en la AWS General Reference.

Administración de claves

Puede configurar su entorno para proteger los datos con las claves.

- Amazon Redshift se integra automáticamente con AWS Key Management Service (AWS KMS) para la administración de claves. AWS KMS utiliza el cifrado de sobres. Para obtener más información, consulte [Cifrado de sobres](#).
- Cuando las claves de cifrado se administran en AWS KMS, Amazon Redshift utiliza una arquitectura de cuatro niveles basada en claves para el cifrado. La arquitectura consta de claves de cifrado de datos AES-256 generadas aleatoriamente, una clave de base de datos, una clave de clúster y una clave maestra. Para obtener más información, consulte [Cómo utiliza Amazon Redshift AWS KMS](#).
- Puede crear su propia clave maestra del cliente (CMK) en KMS. Para obtener más información, consulte [Creación de claves](#).
- También puede importar su propio material de claves para las nuevas CMK. Para obtener más información, consulte [Importación del material de claves en AWS Key Management Service \(AWS KMS\)](#).

- Amazon Redshift admite la administración de claves de cifrado en módulos de seguridad de hardware (HSM) externos. El HSM puede ser local o AWS CloudHSM. Cuando utiliza un HSM, debe utilizar certificados de cliente y servidor para configurar una conexión segura entre Amazon Redshift y el HSM. Amazon Redshift AWS CloudHSM Clásico para la administración de claves. Para obtener más información, consulte [Cifrado para Amazon Redshift mediante módulos de seguridad de hardware \(p. 288\)](#) . Para obtener más información sobre AWS CloudHSM, consulte [¿Qué es ?AWS CloudHSM?](#)
- Puede cambiar las claves de cifrado para los clústeres cifrados. Para obtener más información, consulte [Rotación de claves de cifrado en Amazon Redshift \(p. 289\)](#) .

Tokenización de datos

Tokenización es el proceso de sustitución de valores reales por valores opacos para fines de seguridad de datos. Las aplicaciones sensibles a la seguridad utilizan la tokenización para reemplazar información confidencial (como información personalmente identificable o información sanitaria protegida) por tokens para reducir los riesgos de seguridad. Destokenización invierte los tokens con valores reales para los usuarios autorizados con las políticas de seguridad adecuadas.

Para la integración con servicios de tokenización de terceros, puede utilizar las funciones definidas por el usuario (UDF) de Amazon Redshift que cree mediante [AWS Lambda](#). Para obtener más información, consulte [Funciones de Lambda definidas por el usuario](#) en la Guía para desarrolladores de bases de datos Amazon Redshift. Por ejemplo, consulte [Protección](#).

Amazon Redshift envía solicitudes de tokenización a un servidor de tokenización al que se accede a través de una API REST o un endpoint predefinido. Dos o más funciones Lambda complementarias procesan las solicitudes de tokenización y destokenización. Para este procesamiento, puede usar las funciones de Lambda proporcionadas por un proveedor de tokenización de terceros. También puede utilizar las funciones de Lambda que registra como UDF de Lambda en Amazon Redshift.

Por ejemplo, supongamos que se envía una consulta que invoca una UDF de tokenización o destokenización en una columna. El clúster de Amazon Redshift almacena las filas de argumentos aplicables y envía esas filas en lotes a la función Lambda en paralelo. Las transferencias de datos entre los nodos de computación de Amazon Redshift y Lambda en una conexión de red separada y aislada que no es accesible para los clientes. La función Lambda pasa los datos al extremo del servidor de tokenización. El servidor de tokenización tokeniza o destokeniza los datos según sea necesario y los devuelve. A continuación, las funciones de Lambda transmiten los resultados al clúster de Amazon Redshift para su posterior procesamiento, si es necesario, y, a continuación, devuelven los resultados de la consulta.

Privacidad del tráfico entre redes

Para dirigir el tráfico entre Amazon Redshift y clientes y aplicaciones en una red corporativa:

- Configure una conexión privada entre su nube virtual privada (VPC) y su red corporativa. Configure una conexión VPN IPsec a través de Internet o una conexión física privada mediante [AWS Direct Connect](#) conexión de AWS Direct Connect. Le permite establecer una interfaz virtual privada desde la red en las instalaciones directamente a Amazon VPC, lo que le proporciona una conexión de red privada con un gran ancho de banda entre la red y la VPC. Con varias interfaces virtuales, puede incluso establecer conectividad privada con varias VPC al tiempo que mantiene aislada la red. Para obtener más información, consulte [¿Qué es ?AWS Site-to-Site VPN?](#) y [¿Qué es ?AWS Direct Connect?](#)

Para dirigir el tráfico entre un clúster de Amazon Redshift en una VPC y buckets de Amazon S3 en la misma AWS Región :

- Configure un punto de enlace de la VPC privado de Amazon S3 para tener acceso a los datos de Amazon S3 desde una carga o descarga de ETL. Para obtener más información, consulte [Puntos de enlace para Amazon S3](#).

- Habilite «Enhanced VPC routing» para un clúster de Amazon Redshift, especificando un punto de enlace de Amazon S3 VPC de destino. A continuación, el tráfico generado por los comandos COPY, UNLOAD o CREATE LIBRARY de Amazon Redshift se direcciona a través del punto de enlace privado. Para obtener más información, consulte [Habilitación de Enhanced VPC Routing \(p. 203\)](#).

Administración de identidades y accesos en Amazon Redshift

El acceso a Amazon Redshift requiere credenciales que AWS puede utilizar para autenticar las solicitudes. Estas credenciales deben tener permisos para obtener acceso a AWS. Como, por ejemplo, un clúster de Amazon Redshift. En las siguientes secciones presentamos más detalles sobre cómo usar [AWS Identity and Access Management \(IAM\)](#) para Amazon Redshift sus recursos controlando quién puede obtener acceso a ellos:

- [Authentication \(p. 304\)](#)
- [Control de acceso \(p. 305\)](#)

Authentication

Puede tener acceso a AWS como cualquiera de los siguientes tipos de identidades.

- Usuario raíz de la cuenta de AWS: cuando se crea una cuenta de AWS por primera vez, comienza con una única identidad de inicio de sesión que tiene acceso total a todos los servicios y recursos de AWS en la cuenta. Esta identidad recibe el nombre de usuario raíz de la cuenta de AWS y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Le recomendamos encarecidamente que no utilice el usuario raíz en sus tareas cotidianas, ni siquiera en las tareas administrativas. En lugar de ello, es mejor ceñirse a la [práctica recomendada de utilizar el usuario final exclusivamente para crear al primer usuario de IAM](#). A continuación, guarde las credenciales del usuario raíz en un lugar seguro y utilícelas tan solo para algunas tareas de administración de cuentas y servicios.
- Usuario de IAM— Un [Usuario de IAM](#) es una identidad dentro de su [AWS](#) Cuenta con permisos personalizados específicos para crear un clúster de en Amazon Redshift. Puede utilizar un nombre de usuario y una contraseña de IAM para iniciar sesión en páginas web seguras de AWS tales como [AWS Management Console](#), [foros de discusión de AWS](#) o el [Centro de AWS Support](#).

Además de un nombre de usuario y una contraseña, también puede generar [claves de acceso](#) para cada usuario. Puede utilizar estas claves al acceder a los servicios de AWS mediante programación, ya sea a través de [uno de los varios SDK](#) o mediante la [AWS Command Line Interface \(CLI\)](#). El SDK y las herramientas de CLI usan claves de acceso para firmar criptográficamente su solicitud. Si no utiliza las herramientas de AWS, debe firmar la solicitud usted mismo. Compatibilidad con Amazon Redshift Signature Version 4, un protocolo para autenticar solicitudes de API de entrada. Para obtener más información sobre las solicitudes de autenticación, consulte [Proceso de firma de Signature Version 4](#) en la Referencia general de AWS.

- Rol de IAM: un [rol de IAM](#) es una identidad de IAM que puede crear en la cuenta y que tiene permisos específicos. Un rol de IAM es similar a un usuario de IAM en que se trata de una identidad de AWS con políticas de permisos que determinan lo que la identidad puede hacer y lo que no en AWS. Sin embargo, en lugar de asociarse exclusivamente a una persona, la intención es que cualquier usuario pueda asumir un rol que necesite. Además, un rol no tiene asociadas credenciales a largo plazo estándar, como una contraseña o claves de acceso. En su lugar, cuando se asume un rol, este proporciona credenciales de seguridad temporales para la sesión de rol. Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuarios federados: en lugar de crear un usuario de IAM, puede utilizar identidades existentes de AWS Directory Service, del directorio de usuarios de su compañía o de un proveedor de identidades web. Estas identidades reciben el nombre de usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita el acceso a través de un [proveedor de identidades](#). Para obtener más información acerca de los usuarios federados, consulte [Usuarios federados y roles](#) en la Guía del usuario de IAM.
- Acceso a los servicios de AWS: un rol de servicio es un [rol de IAM](#) que un servicio asume para realizar acciones en su nombre. Los roles de servicio ofrecen acceso solo dentro de su cuenta y no se pueden utilizar para otorgar acceso a servicios en otras cuentas. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte [Creación de un rol para delegar permisos a un servicio de AWS](#) en la Guía del usuario de IAM.
- Aplicaciones que se ejecutan en Amazon EC2— Puede utilizar un rol de IAM para administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia EC2 y hacen que AWS CLI o AWS SDKs soliciten de API. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte [Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2](#) en la Guía del usuario de IAM.

Control de acceso

Puede tener credenciales válidas para autenticar las solicitudes, pero a menos que tenga permisos no podrá crear recursos de Amazon Redshift ni obtener acceso a ellos. Por ejemplo, debe tener permisos para crear un clúster de Amazon Redshift, crear una instantánea, añadir una suscripción a eventos, etc.

En las secciones siguientes se describe cómo administrar los permisos para Amazon Redshift. Le recomendamos que lea primero la información general.

- [Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift](#) (p. 305)
- [Uso de políticas basadas en identidad \(políticas de IAM\) para Amazon Redshift](#) (p. 311)

Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift

Cada recurso de AWS pertenece a una cuenta de AWS, y los permisos para crear u obtener acceso a los recursos se rigen por las políticas de permisos. Los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, usuarios, grupos y funciones). Algunos servicios (como AWS Lambda) también permiten asociar políticas de permisos con los recursos.

Note

Un administrador de la cuenta (o usuario administrador) es un usuario con privilegios de administrador. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

Cuando concede permisos, decide quién debe obtener los permisos, para qué recursos se obtienen permisos y qué acciones específicas desea permitir en esos recursos.

Recursos y operaciones de Amazon Redshift

En Amazon Redshift, el recurso principal es un clúster. Amazon Redshift admite otros recursos que pueden utilizarse con el recurso principal, como instantáneas, grupos de parámetros y suscripciones a eventos. Estos elementos se denominan subrecursos.

Estos recursos y subrecursos tienen nombres de recursos de Amazon (ARN) únicos asociados a ellos, tal y como se muestra en la siguiente tabla:

Tipo de recurso	Formato de ARN
Clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :cluster: <i>cluster-name</i>
Base de datos del clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :dbname: <i>cluster-name</i> / <i>database-name</i>
Usuario de base de datos del clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :dbuser: <i>cluster-name</i> / <i>database-user-name</i>
Grupo de usuarios de base de datos del clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :dbgroup: <i>cluster-name</i> / <i>database-group-name</i>
Grupo de parámetros del clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :parametergroup: <i>parameter-group-name</i>
Grupo de seguridad de clúster	arn:aws:redshift: <i>region</i> : <i>account-id</i> :securitygroup: <i>security-group-name</i>
Dirección IP/CIDR	arn:aws:redshift: <i>region</i> : <i>account-id</i> :securitygroupingress: <i>security-group-name</i> /cidrip/ <i>IP-range</i>
Grupo de seguridad de EC2	arn:aws:redshift: <i>region</i> : <i>account-id</i> :securitygroupingress: <i>security-group-name</i> /ec2securitygroup/ <i>owner</i> / <i>EC2-security-group-id</i>
Suscripción a eventos	arn:aws:redshift: <i>region</i> : <i>account-id</i> :eventsubscription: <i>event-subscription-name</i>
Certificado de cliente del módulo de seguridad de hardware (HSM)	arn:aws:redshift: <i>region</i> : <i>account-id</i> :hsmclientcertificate: <i>HSM-client-certificate-id</i>
Configuración del HSM	arn:aws:redshift: <i>region</i> : <i>account-id</i> :hsmconfiguration: <i>HSM-configuration-id</i>
Grupo de parámetros	arn:aws:redshift: <i>region</i> : <i>account-id</i> :parametergroup: <i>parameter-group-name</i>
Endpoint VPC administrado por RedShift	arn:aws:redshift: <i>region</i> : <i>account-id</i> :managedvpcendpoint: <i>endpoint-name</i>
Instantánea	arn:aws:redshift: <i>region</i> : <i>account-id</i> :snapshot: <i>cluster-name</i> / <i>snapshot-name</i>
Autorización de copia de snapshot	arn:aws:redshift: <i>region</i> : <i>account-id</i> :snapshotcopygrant: <i>snapshot-copy-grant-name</i>

Tipo de recurso	Formato de ARN
Subnet group	<code>arn:aws:redshift:<i>region</i>:<i>account-id</i>:subnetgroup:<i>subnet-group-name</i></code>

Amazon Redshift proporciona un conjunto de operaciones para trabajar con los recursos de Amazon Redshift. Para ver la lista de las operaciones disponibles, consulte [Referencia de permisos de la API de Amazon Redshift](#) (p. 322).

Titularidad de los recursos

El propietario del recurso es la cuenta de AWS que ha creado el recurso. Es decir, el propietario del recurso es el **AWSSAccount de entidad principal** (cuenta raíz, usuario de IAM o rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si usa las credenciales de la cuenta raíz de su AWS Para crear un clúster de base de datos, la cuenta de AWS es la propietaria del recurso de Amazon Redshift.
- Si crea un usuario de IAM en su AWS Para conceder permisos para crear recursos de Amazon Redshift a ese usuario, el usuario podrá crear recursos de Amazon Redshift. Sin embargo, su AWS La cuenta de a la que pertenece el usuario será la propietaria de los recursos de Amazon Redshift.
- Si crea un rol de IAM en su AWS Con permisos para crear recursos de Amazon Redshift, cualquier persona que pueda asumir el rol podrá crear recursos de Amazon Redshift. Su AWS La cuenta de a la que pertenece el rol será la propietaria de los recursos de Amazon Redshift.

Administración del acceso a los recursos

Política de permisos Describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

Note

En esta sección se explica cómo se utiliza IAM en el contexto de Amazon Redshift. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte [¿Qué es IAM?](#) en la Guía del usuario de IAM. Para obtener información acerca de la sintaxis y descripciones de la política de IAM, consulte [AWS Referencia de política de IAM](#) en la Guía del usuario de IAM.

Las políticas asociadas a una identidad de IAM se denominan políticas basadas en identidad (políticas de IAM) y las políticas asociadas a un recurso se denominan políticas basadas en recursos. Amazon Redshift solo admite políticas basadas en identidad (políticas de IAM).

Políticas basadas en identidad (políticas de IAM)

Puede asociar políticas a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Asociar una política de permisos a un usuario o grupo de su cuenta: un administrador de la cuenta puede utilizar una política de permisos asociada a un usuario determinado. Este tipo de política concede permisos a dicho usuario para crear un recurso de Amazon Redshift, por ejemplo, un clúster de.
- Asociar una política de permisos a un rol (conceder permisos entre cuentas): puede asociar una política de permisos basada en identidad a un rol de IAM para conceder permisos entre cuentas. Por ejemplo, el administrador de la Cuenta A puede crear una función para conceder permisos entre cuentas a otra cuenta de AWS (por ejemplo, a la Cuenta B) o a un servicio de AWS, tal y como se indica a continuación:
 1. El administrador de la Cuenta A crea un rol de IAM y asocia una política de permisos a dicho rol, que concede permisos sobre los recursos de la Cuenta A.

2. El administrador de la Cuenta A asocia una política de confianza al rol que identifica la Cuenta B como la entidad principal que puede asumir el rol.
3. A continuación, el administrador de la Cuenta B puede delegar permisos para asumir el rol a cualquier usuario de la Cuenta B. De este modo, los usuarios de la Cuenta B podrán crear recursos y obtener acceso a ellos en la Cuenta A. La entidad principal de la política de confianza también puede ser la entidad principal de un servicio de AWS si desea conceder permisos para asumir el rol a un servicio de AWS.

Para obtener más información acerca del uso de IAM para delegar permisos, consulte [Administración de accesos](#) en la Guía del usuario de IAM.

A continuación, se ofrece un ejemplo de una política que le permite a un usuario crear, eliminar, modificar y reiniciar clústeres de Amazon Redshift para su cuenta de AWSAccount.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowManageClusters",
      "Effect": "Allow",
      "Action": [
        "redshift:CreateCluster",
        "redshift>DeleteCluster",
        "redshift:ModifyCluster",
        "redshift:RebootCluster"
      ],
      "Resource": "*"
    }
  ]
}
```

Para obtener más información acerca del uso de políticas basadas en la identidad con Amazon Redshift, consulte [Uso de políticas basadas en identidad \(políticas de IAM\) para Amazon Redshift \(p. 311\)](#). Para obtener más información acerca de los usuarios, grupos, roles y permisos, consulte [Identidades \(usuarios, grupos y roles\)](#) en la Guía del usuario de IAM.

Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. Amazon Redshift no admite políticas basadas en recursos.

Especificación de elementos de política: Acciones, efectos, recursos y entidades de seguridad

Para cada recurso de Amazon Redshift (consulte [Recursos y operaciones de Amazon Redshift \(p. 306\)](#)), el servicio define un conjunto de operaciones de API (consulte [Actions](#)). Para conceder permisos a estas operaciones de la API, Amazon Redshift define un conjunto de acciones que puede especificar en una política. Para realizar una operación API pueden ser necesarios permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- **Recurso:** en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política. Para obtener más información, consulte [Recursos y operaciones de Amazon Redshift \(p. 306\)](#).
- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, `redshift:DescribeClusters` Permisos permiten al usuario ejecutar la consola de Amazon Redshift `DescribeClusters`.

- Efecto: especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- Entidad principal: en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). Amazon Redshift no admite políticas basadas en recursos.

Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte [AWSReferencia de política de IAM](#) en la Guía del usuario de IAM.

Para ver una tabla con todas las acciones de la API de Amazon Redshift y los recursos a los que se aplican, consulte [Referencia de permisos de la API de Amazon Redshift \(p. 322\)](#).

Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones en las que se debe aplicar una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información acerca de cómo especificar condiciones en un lenguaje de política de acceso, consulte [Elemento de la política de IAM JSON: Condición](#) en la Guía del usuario de IAM.

Para identificar las condiciones en las que se aplica una política de permisos, incluya un elemento de `Condition` en su política de permisos de IAM. Por ejemplo, puede crear una política que le permita a un usuario crear un clúster mediante el uso de la acción `redshift:CreateCluster` y puede añadir un elemento de `Condition` para limitar al usuario a que lo haga solamente en una región específica. Para obtener más información, consulte [Uso de condiciones de políticas de IAM para control de acceso preciso \(p. 309\)](#). Para ver una lista que muestre todos los valores de clave de condición y las acciones y recursos de Amazon Redshift a los que se aplican, consulte [Referencia de permisos de la API de Amazon Redshift \(p. 322\)](#).

Uso de condiciones de políticas de IAM para control de acceso preciso

En Amazon Redshift, puede utilizar claves de condición para restringir el acceso a los recursos, en función de las etiquetas de tales recursos. A continuación se muestran claves de condición de comunes de Amazon Redshift.

Clave de condición	Descripción
<code>aws:RequestTag</code>	Requiere que los usuarios incluyan una clave de etiqueta (nombre) y un valor cada vez que crean un recurso. Para obtener más información, consulte aws:RequestTag en la Guía del usuario de IAM.
<code>aws:ResourceTag</code>	Restringe el acceso del usuario a los recursos, en función de claves de etiqueta y valores específicos. Para obtener más información, consulte aws:ResourceTag en la Guía del usuario de IAM.
<code>aws:TagKeys</code>	Utilice esta clave para comparar las claves de etiqueta de una solicitud con las claves que especifique en la política. Para obtener más información, consulte aws:TagKeys en la Guía del usuario de IAM.

Para obtener información acerca de etiquetas, consulte [Información general del proceso de etiquetado \(p. 500\)](#).

Para obtener una lista de las acciones de API compatibles con las claves de condición `redshift:RequestTag` y `redshift:ResourceTag`, consulte [Referencia de permisos de la API de Amazon Redshift \(p. 322\)](#).

Las siguientes claves de condición se pueden utilizar con la acción `GetClusterCredentials` de Amazon Redshift.

Clave de condición	Descripción
<code>redshift:DurationSeconds</code>	Limita el número de segundos que se puede especificar para la duración.
<code>redshift:DbName</code>	Restringe los nombres de base de datos que se pueden especificar.
<code>redshift:DbUser</code>	Restringe los nombres de usuarios de base de datos que se pueden especificar.

Ejemplo 1: Restricción del acceso mediante el uso de la clave de condición `aws:ResourceTag`

Utilice la siguiente política de IAM para permitir que un usuario pueda modificar un clúster de Amazon Redshift únicamente para un `AWSaccount` de `us-west-2` región con una etiqueta llamada `environment` con un valor de etiqueta de `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"
      }
    }
  }
}
```

Ejemplo 2: Restricción del acceso mediante el uso de la clave de condición `aws:RequestTag`

Utilice la siguiente política de IAM para conceder a un usuario la creación de un clúster de Amazon Redshift únicamente si el comando para crear el clúster incluye una etiqueta denominada `usage` y un valor de etiqueta de `production`. La condición con `aws:TagKeys` y el modificador `ForAllValues` especifica que solo las claves `costcenter` y `usage` se pueden especificar en la solicitud.

```
{
  "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"  
    ]  
  }  
}  
}
```

Uso de políticas basadas en identidad (políticas de IAM) para Amazon Redshift

Este tema contiene ejemplos de políticas basadas en identidades, donde los administradores de cuentas pueden asociar políticas de permisos a identidades de IAM (es decir, a usuarios, grupos y funciones).

Important

Le recomendamos que consulte primero los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de Amazon Redshift. Para obtener más información, consulte [Información general sobre la administración de los permisos de acceso a los recursos de Amazon Redshift \(p. 305\)](#).

A continuación se muestra un ejemplo de una política de permisos. La política le permite a un usuario crear, eliminar, modificar y reiniciar todos los clústeres y, luego, le deniega permiso para eliminar o modificar todo clúster cuyo identificador comience con `production`.

```
{  
  "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 política tiene dos declaraciones:

- La primera instrucción concede permisos para que un usuario cree, elimine, modifique y reinicie clústeres. La instrucción especifica un comodín (*) como `Resource` para que la política se aplique a todos los recursos de Amazon Redshift que son propiedad de raíz `AWS` account.

- La segunda instrucción deniega el permiso para eliminar o modificar un clúster. La instrucción especifica un Amazon Resource Name (ARN, Nombre de recurso de Amazon) de clúster para el valor de `Resource` que incluye un carácter comodín (*). Como resultado, esta instrucción se aplica a todos los clústeres de Amazon Redshift que son propiedad de raízAWS donde el identificador del clúster comienza con `production`.

AWSPolíticas administradas por Amazon Redshift (predefinidas) para Amazon Redshift

AWS aborda muchos casos de uso comunes proporcionando políticas de IAM independientes creadas y administradas por AWS. Las políticas administradas por AWS conceden los permisos necesarios para casos de uso comunes, lo que le evita tener que investigar los permisos que se necesitan. Para obtener más información, consulte [AWSPolíticas administradas por](#) en la Guía del usuario de IAM.

Los siguientes ejemplos deAWSLas políticas administradas por, que puede asociar a los usuarios de su cuenta, son específicas de Amazon Redshift:

- `AmazonRedshiftReadOnlyAccess`: concede acceso de solo lectura a todos los recursos de Amazon Redshift para la consolaAWSaccount.
- `AmazonredShiftFullAccess`: concede acceso completo a todos los recursos de Amazon Redshift para la consolaAWSaccount.
- `AmazonredShiftQueryEditor`: concede acceso completo al editor de consultas en la consola de Amazon Redshift.
- `AmazonredShiftDataFullAccess`— Otorga acceso completo a las operaciones y recursos de la API de datos de Amazon Redshift para elAWSaccount.

También puede crear sus propias políticas de IAM personalizadas para conceder permisos a las acciones y recursos de la API de Amazon Redshift. Puede asociar estas políticas personalizadas a los usuarios o grupos de IAM que requieran esos permisos.

Permisos necesarios para usar Redshift Spectrum

Amazon Redshift Spectrum requiere permisos para otrosAWSPara obtener acceso a los recursos. Para obtener detalles acerca de los permisos en las políticas de IAM para Redshift Spectrum, consulte [Políticas de IAM para Amazon Redshift Spectrum](#) en la Guía para desarrolladores de bases de datos de Amazon Redshift.

Permisos necesarios para usar la consola de Amazon Redshift

Para que un usuario pueda trabajar con la consola de Amazon Redshift, debe tener un conjunto mínimo de permisos que le permitan describir los recursos de Amazon Redshift para suAWSaccount. Estos permisos también deben permitir al usuario describir otra información relacionada Amazon CloudWatch información de red y seguridad de.

Si crea una política de IAM que sea más restrictiva que el mínimo de permisos necesarios, la consola no funciona del modo esperado para los usuarios con esa política de IAM. Para asegurarse de que esos usuarios puedan seguir utilizando la consola de Amazon Redshift, asocie también la `AmazonRedshiftReadOnlyAccess` para el usuario. Cómo hacer esto se describe en [AWSPolíticas administradas por Amazon Redshift \(predefinidas\) para Amazon Redshift \(p. 312\)](#).

Para obtener información sobre cómo conceder a un usuario acceso al editor de consultas en la consola de Amazon Redshift, consulte [Permisos necesarios para usar el editor de consultas de consola Amazon Redshift \(p. 313\)](#).

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o la API de Amazon Redshift.

Permisos necesarios para usar el editor de consultas de consola Amazon Redshift

Para que un usuario pueda trabajar con el editor de consultas de Amazon Redshift, ese usuario debe tener un conjunto mínimo de permisos para las operaciones de la API de datos de Amazon Redshift y Amazon Redshift. Para conectarse a una base de datos mediante un secreto, también debe tener permisos de Secrets Manager.

Para conceder a un usuario acceso al editor de consultas en la consola de Amazon Redshift, asocie la `AmazonRedshiftQueryEditorReadOnlyAccess` AWS-Políticas administradas por `LaAmazonRedshiftQueryEditor` permite al usuario obtener permisos para recuperar los resultados de solo sus propias instrucciones SQL de. Es decir, las declaraciones presentadas por el mismo `aws:userid` como se muestra en esta sección de la `AmazonRedshiftQueryEditor` AWS-política administrada de.

```
{
  "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}"
    }
  }
}
```

Para permitir que un usuario recupere los resultados de sentencias SQL de otras personas en el mismo rol de IAM, cree su propia directiva sin la condición de limitar el acceso al usuario actual. Limite también el acceso para cambiar una directiva a un administrador.

Permisos necesarios para usar el programador de Amazon Redshift

Cuando utiliza el programador de Amazon Redshift, configura un rol de IAM con una relación de confianza con el programador de Amazon Redshift (`scheduler.redshift.amazonaws.com`) para permitir que el programador asuma permisos en su nombre. También adjunta una política (permisos) al rol para las operaciones de la API de Amazon Redshift que desea programar.

En el siguiente ejemplo se muestra el documento de la política en formato JSON para establecer una relación de confianza entre el programador de Amazon Redshift y Amazon Redshift.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "scheduler.redshift.amazonaws.com",

```

```
        "redshift.amazonaws.com"
      ],
    },
    "Action": "sts:AssumeRole"
  }
]
```

Para obtener más información sobre entidades de confianza, consulte [Creación de un rol para delegar permisos a un servicio de AWS](#) en la Guía del usuario de IAM.

También debe añadir permisos para las operaciones de Amazon Redshift que quiera programar.

Para que el programador utilice la operación `ResizeCluster`, añada un permiso similar al siguiente a su política de IAM. En función de su entorno, es posible que quiera crear una política más restrictiva.

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

Para consultar los pasos necesarios para crear un rol para el programador de Amazon Redshift, consulte [Creación de un rol para un AWS servicio \(consola\)](#) en la Guía del usuario de IAM. Realice estas elecciones cuando cree un rol en la consola de IAM de:

- Para Elegir el servicio que utilizará este rol: Seleccionar Redshift.
- Para Seleccionar su caso de uso: Seleccionar Redshift - Programador.
- Cree o añada una política al rol que permita programar una operación de Amazon Redshift. Seleccione `Create policy` (Crear política) o modifique el rol para añadir una política. Introduzca la política JSON para la operación que se va a programar.
- Después de crear el rol, edite la `Trust relationship` (Relación de confianza) del rol de IAM para incluir el servicio `redshift.amazonaws.com`.

El rol IAM que cree tiene entidades de confianza de `scheduler.redshift.amazonaws.com` y `redshift.amazonaws.com`. También tiene una política adjunta que permite una acción de API de Amazon Redshift compatible, por ejemplo, `redshift:ResizeCluster`.

Permisos necesarios para usar el programador de Amazon EventBridge

Cuando utiliza el programador de Amazon EventBridge, configura un rol de IAM con una relación de confianza con el programador de EventBridge (`events.amazonaws.com`) para permitir que el programador asuma permisos en su nombre. También adjunta una política (permisos) al rol para las operaciones de la API de datos de Amazon Redshift que quiere programar y una política para operaciones de Amazon EventBridge.

Utilice el programador de EventBridge cuando cree consultas programadas con el editor de consultas de Amazon Redshift en la consola.

Puede crear un rol de IAM para ejecutar consultas programadas en la consola de IAM. En esta función de IAM, adjunte `AmazonEventBridgeFullAccess` y `AmazonRedshiftDataFullAccess`.

En el siguiente ejemplo se muestra el documento de la política en formato JSON para establecer una relación de confianza entre el programador de EventBridge.

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

Para obtener más información sobre entidades de confianza, consulte [Creación de un rol para delegar permisos a un servicio de AWS](#) en la Guía del usuario de IAM.

Para ver los pasos necesarios para crear un rol para el programador de EventBridge, consulte [Creación de un rol para un AWS servicio \(consola\)](#) en la Guía del usuario de IAM. Realice estas elecciones cuando cree un rol en la consola de IAM de:

- Para Elegir el servicio que utilizará este rol: Seleccionar Eventos de CloudWatch.
- Para Seleccione su caso de uso: Seleccionar Eventos de CloudWatch.
- Adjunte las siguientes directivas de permisos: `AmazonEventBridgeFullAccess` y `AmazonRedshiftDataFullAccess`.

El rol de IAM que crea tiene una entidad de confianza de `events.amazonaws.com`. También tiene una política adjunta que permite acciones compatibles de la API de datos de Amazon Redshift, por ejemplo, `redshift-data:*`.

Políticas de recursos de GetClusterCredentials

Para conectarse a la base de datos de un clúster mediante una conexión JDBC u ODBC con credenciales de base de datos de IAM o para llamar mediante programación a la acción `GetClusterCredentials`, necesita, un conjunto mínimo de permisos. Como mínimo, necesita permiso para llamar a la acción `redshift:GetClusterCredentials` con acceso a un recurso `dbuser`.

Si usa una conexión JDBC o ODBC en lugar de `server` y `port`, puede especificar `cluster_id` y `region`, pero para ello la política debe permitir la acción `redshift:DescribeClusters` con acceso al recurso `cluster`.

Si llama a la acción `GetClusterCredentials` con los parámetros opcionales `Autocreate`, `DbGroups` y `DbName`, también tendrá que permitir las acciones y el acceso a los recursos indicados en la tabla siguiente.

Parámetro GetClusterCred	Acción	Recurso
Autocreate	redshift:CreateClusterUser	dbuser
DbGroups	redshift:JoinGroup	dbgroup
DbName	N/D	dbname

Para obtener más información acerca de recursos, consulte [Recursos y operaciones de Amazon Redshift \(p. 306\)](#).

También puede incluir las siguientes condiciones en la política:

- `redshift:DurationSeconds`
- `redshift:DbName`
- `redshift:DbUser`

Para obtener más información acerca de las condiciones, consulte [Especificación de las condiciones de una política \(p. 309\)](#).

Ejemplos de políticas administradas por el cliente

En esta sección, encontrará ejemplos de políticas de usuario que conceden permisos para varias acciones de Amazon Redshift. Estas políticas funcionan cuando se utiliza la API de Amazon Redshift, AWSSDK, o el AWS CLI.

Note

Todos los ejemplos utilizan la región EE. UU. Oeste (Oregón) (`us-west-2`) y contienen identificadores de cuenta ficticios.

Ejemplo 1: Permitir al usuario acceso completo a todos los recursos y acciones de Amazon Redshift

La política siguiente permite obtener acceso a todas las acciones de Amazon Redshift en todos los recursos.

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

El valor `redshift:*` en la `Action` indica todas las acciones de Amazon Redshift.

Ejemplo 2: Denegarle a un usuario obtener acceso a un conjunto de acciones de Amazon Redshift

De forma predeterminada, se deniegan todos los permisos. Sin embargo, en ocasiones se necesita denegar explícitamente el acceso a una acción o un conjunto de acciones específicas. La siguiente política permite obtener acceso a todas las acciones de Amazon Redshift y deniega explícitamente el acceso a cualquier acción de Amazon Redshift en la que el nombre empiece por `Delete`. Esta política se aplica a todos los recursos de Amazon Redshift de `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:*"
  }
]
```

Ejemplo 3: Permitirle a un usuario administrar clústeres

La siguiente política le permite a un usuario crear, eliminar, modificar y reiniciar todos los clústeres y, luego, le deniega permiso para eliminar o modificar todo clúster cuyo nombre comience 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"
    }
  ]
}
```

Ejemplo 4: Permitirle a un usuario que autorice y revoque el acceso a instantáneas

La siguiente política le permite a un usuario, por ejemplo el usuario A, hacer lo siguiente:

- Autorizar la obtención de acceso a toda snapshot creada a partir de un clúster denominado `shared`.
- Revocar la obtención de acceso a snapshots para toda snapshot creada a partir del clúster `shared` en el que el nombre de la snapshot comience 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"
    }
  ]
}
```

Si el usuario A le ha otorgado al usuario B acceso a la snapshot, el usuario B debe tener una política como la siguiente que le permita restaurar un clúster a partir de la snapshot. La siguiente política le permite al usuario B describir y restaurar a partir de snapshots, y crear clústeres. El nombre de estos clústeres debe comenzar 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"
    }
  ]
}
```

Ejemplo 5: Para permitir a un usuario copiar una instantánea de un clúster y restaurar un clúster a partir de una instantánea

La siguiente política le permite a un usuario copiar cualquier snapshot creada a partir del clúster denominado `big-cluster-1` y restaurar cualquier snapshot cuando el nombre de ella comience 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"
    }
  ]
}
```

Ejemplo 6: Permitir que un usuario obtenga acceso a Amazon Redshift y a recursos y acciones comunes de relacionadosAWSservices

En la política de ejemplo siguiente se permite el acceso a todas las acciones y recursos de Amazon Redshift, Amazon Simple Notification Service (Amazon SNS) y Amazon CloudWatch. También permite acciones especificadas en todos los recursos de relacionados de Amazon EC2 en la cuenta.

Note

Para las acciones de Amazon EC2 que se especifican en esta política de ejemplo no se admiten los permisos a nivel recurso.

```
{
  "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": [
            "*"
        ]
    }
]
```

Ejemplo 7: Permitir a un usuario etiquetar recursos con la consola de Amazon Redshift

El siguiente ejemplo de política de permite a un usuario etiquetar recursos con la consola de Amazon Redshift mediante elAWS Resource Groups. Esta política puede asociarse a un rol de usuario que invada la consola nueva u original de Amazon Redshift. Para obtener más información acerca del etiquetado, consulte [Etiquetado de recursos en Amazon Redshift \(p. 500\)](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Tagging permissions",
      "Effect": "Allow",
      "Action": [
        "redshift:DeleteTags",
        "redshift>CreateTags",
        "redshift:DescribeTags",
        "tag:UntagResources",
        "tag:TagResources"
      ],
      "Resource": "*"
    }
  ]
}
```

```
}
```

Política de ejemplo para usar GetClusterCredentials

La política siguiente utiliza estos valores de parámetros de ejemplo:

- Región: `us-west-2`
- `AWSaccount:123456789012`
- Nombre del clúster: `examplecluster`

La política siguiente habilita las acciones `GetClusterCredentials`, `CreateClusterUser` y `JoinGroup`. La política utiliza claves de condición para permitir que la propiedad `GetClusterCredentials` y `CreateClusterUser` solo se deben realizar acciones cuando el `AWSID` de usuario coincide con `"AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"`. El acceso de IAM solo se solicita para la base de datos `"testdb"`. La política también permite a los usuarios unirse a un grupo denominado `"common_group"`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GetClusterCredsStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:GetClusterCredentials"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/${redshift:DbUser}",
        "arn:aws:redshift:us-west-2:123456789012:dbname:examplecluster/testdb",
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "CreateClusterUserStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:CreateClusterUser"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/${redshift:DbUser}"
      ],
      "Condition": {
        "StringEquals": {
          "aws:userid": "AIDIODR4TAW7CSEXAMPLE:${redshift:DbUser}@yourdomain.com"
        }
      }
    },
    {
      "Sid": "RedshiftJoinGroupStatement",
      "Effect": "Allow",
      "Action": [
        "redshift:JoinGroup"
      ],
      "Resource": [
        "arn:aws:redshift:us-west-2:123456789012:dbgroup:examplecluster/common_group"
      ]
    }
  ]
}
```

```
}  
]  
}  
  
}  
}
```

Referencia de permisos de la API de Amazon Redshift

Cuando configura [Control de acceso](#) (p. 305), escriba políticas de permisos que vaya a asociar a una identidad de IAM (políticas basadas en identidad). Para obtener información de referencia detallada, consulte [Acciones, recursos y claves de condición para Amazon Redshift](#) en la Guía del usuario de IAM. Esta referencia contiene información sobre las operaciones de la API de Amazon Redshift que se pueden utilizar en una política de IAM. También incluye la [AWS](#) para el que puede conceder los permisos y las claves de condición que puede incluir para controlar el acceso con mayor detalle. Para obtener más información acerca de las condiciones, consulte [Uso de condiciones de políticas de IAM para control de acceso preciso](#) (p. 309).

Las acciones se especifican en el campo `Action` de la política, el valor del recurso en el campo `Resource` de la política y las condiciones en el campo `Condition` de la política. Para especificar una acción, use el prefijo `redshift:` seguido del nombre de operación de la API (por ejemplo, `redshift:CreateCluster`).

Uso de roles vinculados a servicios para Amazon Redshift

Amazon Redshift utiliza [AWS Identity and Access Management \(IAM\)](#) [roles vinculados al servicio](#). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon Redshift. Amazon Redshift predefine los roles vinculados a servicios e incluyen todos los permisos que el servicio requiere para llamar a [AWS](#) en nombre del clúster de Amazon Redshift.

Un rol vinculado a un servicio simplifica la configuración de Amazon Redshift porque ya no tendrá que añadir manualmente los permisos necesarios. El rol está vinculado a los casos de uso de Amazon Redshift y tiene permisos predefinidos. Solo Amazon Redshift puede asumir el rol y solo el rol vinculado a un servicio puede utilizar la política de permisos predefinida. Amazon Redshift crea un rol vinculado a servicios en su cuenta la primera vez que crea un clúster de. Puede eliminar el rol vinculado a servicios solo después de eliminar todos los clústeres de Amazon Redshift de su cuenta. De esta forma, se protegen los recursos de Amazon Redshift, ya que evita que se puedan eliminar accidentalmente los permisos necesarios para obtener acceso a los recursos.

Amazon Redshift admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte [Regiones y puntos de enlace de AWS](#).

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que indican Sí en la columna Roles vinculados a servicios. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de roles vinculados a servicios en Amazon Redshift

Amazon Redshift usa la función vinculada al servicio denominada `AWSServiceRoleForRedshift`— Permite que Amazon Redshift llame a [AWS](#) en su nombre.

El rol vinculado a un servicio `awsServiceRoleForRedshift` solo confía en `redshift.amazonaws.com` Para asumir el rol.

La política de permisos de la función vinculada al servicio de AWSServiceRoleForRedshift permite que Amazon Redshift realice las siguientes operaciones en todos los recursos relacionados:

- `ec2:DescribeVpcs`
- `ec2:DescribeSubnets`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeAddresses`
- `ec2:AssociateAddress`
- `ec2:DisassociateAddress`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:CreateVpcEndpoint`
- `ec2>DeleteVpcEndpoints`
- `ec2:DescribeVpcEndpoints`
- `ec2:ModifyVpcEndpoint`

Para permitir a una entidad de IAM que cree roles vinculados a servicios AWSServiceRoleForRedshift

Añada la siguiente instrucción de política a los permisos para esa entidad de IAM:

```
{
  "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"}}
}
```

Para permitir a una entidad de IAM eliminar roles vinculados a servicios AWSServiceRoleForRedshift

Añada la siguiente instrucción de política a los permisos para esa entidad de 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"}}
}
```

También puede utilizar una AWS política administrada de [Proporcione acceso completo](#) a Amazon Redshift.

Creación de un rol vinculado a un servicio en Amazon Redshift

No es necesario crear manualmente un rol vinculado a un servicio AWSServiceRoleForRedshift. Amazon Redshift crea el rol vinculado al servicio por usted. Si la función vinculada al servicio AWSServiceRoleForRedshift se ha eliminado de la cuenta, Amazon Redshift crea la función cuando se lanza un nuevo clúster de Amazon Redshift.

Important

Si utilizaba el servicio Amazon Redshift antes del 18 de septiembre de 2017, fecha en que comenzó a admitir los roles vinculados a servicios, Amazon Redshift creó la función `AWSServiceRoleForRedShift` en su cuenta. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Modificación de un rol vinculado a un servicio en Amazon Redshift

Amazon Redshift no le permite editar el rol vinculado al servicio `AWSServiceRoleForRedShift`. Después de crear un rol vinculado a un servicio, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia a él. Sin embargo, puede editar la descripción de la función utilizando la consola de IAM, la AWS Command Line Interface (AWS CLI) o la API de IAM. Para obtener más información, consulte [Modificación de un rol](#) en la Guía del usuario de IAM.

Eliminación de un rol vinculado a un servicio en Amazon Redshift

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, le recomendamos que elimine dicho rol. De esta forma no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa.

Antes de eliminar un rol vinculado a un servicio de una cuenta, necesita apagar y eliminar todos los clústeres de la cuenta. Para obtener más información, consulte [Cierre y eliminación de clústeres](#) (p. 33) .

Puede utilizar la consola de IAM, la AWS CLI o la API de IAM para eliminar un rol vinculado a un servicio. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

Uso de la autenticación de IAM para generar credenciales de usuario de base de datos

Puede generar credenciales de base de datos temporales basadas en los permisos otorgados a través de un AWS Identity and Access Management (IAM) para administrar el acceso que los usuarios tienen a su base de datos de Amazon Redshift.

Normalmente, los usuarios de bases de datos de Amazon Redshift se conectan a la base de datos proporcionando un nombre de usuario y una contraseña de la base de datos. Sin embargo, no es necesario mantener los nombres de usuario y las contraseñas en la base de datos de Amazon Redshift. Como alternativa, puede configurar el sistema para permitir que los usuarios creen credenciales de usuario e inicien sesión en la base de datos en función de sus credenciales de IAM.

Para obtener más información, consulte [Federación y proveedores de identidades](#) en la Guía del usuario de IAM.

Temas

- [Overview](#) (p. 324)
- [Creación de credenciales temporales de usuario de IAM](#) (p. 325)
- [Opciones para proporcionar credenciales de IAM](#) (p. 335)

Overview

Amazon Redshift proporciona el `GetClusterCredentials` Operación de la API para generar credenciales temporales de usuario de base de datos. Puede configurar su cliente SQL con controladores JDBC u

ODBC de Amazon Redshift que administren el proceso de llamar a la función `GetClusterCredentials`. Para ello, recuperan las credenciales de usuario de base de datos y establecen una conexión entre su cliente SQL y la base de datos de Amazon Redshift. También puede usar la aplicación de base de datos para llamar mediante programación a la operación `GetClusterCredentials`, recuperar las credenciales de usuario de base de datos y conectarse a la base de datos.

Si ya gestiona identidades de usuario fuera de AWS Para administrar el acceso a los recursos de Amazon Redshift, puede utilizar un proveedor de identidades (IdP) compatible con Security Assertion Markup Language (SAML) 2.0. Puede utilizar su IdP para permitir a los usuarios federados tener acceso a un rol de IAM. Con ese rol de IAM, puede generar credenciales de base de datos temporales e iniciar sesión en las bases de datos de Amazon Redshift.

Su cliente SQL necesita permiso para llamar a la operación `GetClusterCredentials` en su nombre. Estos permisos se administran creando un rol de IAM y asociando una política de permisos de IAM que conceda o restrinja el acceso a la operación `GetClusterCredentials` y acciones relacionadas.

La política también concede o restringe el acceso a recursos específicos, como clústeres, bases de datos, nombres de usuario de base de datos y nombres de grupos de usuarios de Amazon Redshift.

Note

Le recomendamos que utilice los controladores JDBC u ODBC de Amazon Redshift para administrar el proceso de llamar al método `GetClusterCredentials` e iniciar sesión en la base de datos. Para simplificar, asumimos que en este tema utiliza un cliente SQL con los controladores JDBC u ODBC.

Para obtener detalles concretos y ejemplos del uso de la operación `GetClusterCredentials` o del comando paralelo de la CLI `get-cluster-credentials`, vea [GetClusterCredentials](#) y [get-cluster-credentials](#).

Para administrar la autenticación y la autorización de forma centralizada, Amazon Redshift admite la autenticación de base de datos con IAM, lo que permite la autenticación de usuarios a través de la federación. En lugar de crear un usuario de IAM, en este enfoque puede utilizar identidades existentes de AWS Directory Service, el directorio de usuarios de la compañía o un proveedor de identidades web. Esto se conoce como usuarios federados. AWS asigna un rol a un usuario federado cuando se solicita acceso a través de un IdP.

Para proporcionar acceso federado a un usuario o aplicación cliente de la organización para llamar a operaciones de la API de Amazon Redshift, también puede utilizar el controlador JDBC u ODBC con compatibilidad con SAML 2.0 para solicitar la autenticación del IdP de la organización. En este caso, los usuarios de la organización no tienen acceso directo a Amazon Redshift.

Creación de credenciales temporales de usuario de IAM

En esta sección, puede encontrar cómo configurar el sistema para generar credenciales temporales de usuario de base de datos basadas en IAM e iniciar sesión en la base de datos con las nuevas credenciales.

En líneas generales, el proceso es el siguiente:

1. [Paso 1: Creación de un rol de IAM para el acceso de inicio de sesión único \(SSO\) de IAM \(p. 326\)](#)

(Opcional) Puede autenticar a los usuarios para que tengan acceso a una base de datos de Amazon Redshift integrando la autenticación de IAM y un proveedor de identidad (IdP) de terceros.

2. [Paso 2: Configuración de aserciones SAML para el IdP \(p. 326\)](#)

(Opcional) Para usar la autenticación de IAM mediante un IdP, necesita definir una regla de notificación en la aplicación de su IdP que asigne los usuarios o grupos de su organización

a un rol de IAM. Opcionalmente, puede incluir elementos de atributo para definir parámetros `GetClusterCredentials`.

3. [Paso 3: Cree un rol o usuario de IAM con permisos para llamar a `GetClusterCredentials` \(p. 327\)](#)

La aplicación de cliente de SQL asume el rol de IAM cuando llama a la operación `GetClusterCredentials`. Si ha creado un rol de IAM para el acceso al proveedor de identidad, puede añadir el permiso necesario a ese rol.

4. [Paso 4: Crear usuarios y grupos de usuarios de base de datos \(p. 329\)](#)

(Opcional) De forma predeterminada, `GetClusterCredentials` devuelve credenciales para crear un nuevo usuario si el nombre de usuario no existe. También puede elegir especificar grupos de usuarios a los que se unan los usuarios cuando inicien sesión. De forma predeterminada, los usuarios de la base de datos se unen al grupo `PUBLIC`.

5. [Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM \(p. 330\)](#)

Para conectarse a la base de datos de Amazon Redshift, debe configurar su cliente SQL para que utilice un controlador JDBC u ODBC de Amazon Redshift.

[Paso 1: Creación de un rol de IAM para el acceso de inicio de sesión único \(SSO\) de IAM](#)

Si no utiliza un proveedor de identidad para el acceso de inicio de sesión único, puede omitir este paso.

Si ya gestiona identidades de usuario fuera de AWS para autenticar a los usuarios para que tengan acceso a una base de datos de Amazon Redshift integrando la autenticación de IAM y un proveedor de identidad (IdP) SAML-2.0 de terceros.

Para obtener más información, consulte [Federación y proveedores de identidades](#) en la Guía del usuario de IAM.

Antes de poder utilizar la autenticación de IdP de Amazon Redshift, cree un AWS Proveedor de identidad SAML. Puede crear un IdP en la consola de IAM para informar a AWS sobre el IdP y su configuración. Esto establece una relación de confianza entre su AWS y el IdP. Para conocer los pasos para crear un rol, consulte [Creación de un rol para una federación SAML 2.0 \(consola\)](#) en la Guía del usuario de IAM.

[Paso 2: Configuración de aserciones SAML para el IdP](#)

Después de crear el rol de IAM, necesita definir una regla de reclamación en la aplicación de su IdP que asigne los usuarios o grupos de su organización al rol de IAM. Para obtener más información, consulte [Configuración de aserciones SAML para la respuesta de autenticación](#) en la Guía del usuario de IAM.

Si elige utilizar los parámetros `GetClusterCredentials` opcionales `DbUser`, `AutoCreate`, y `DbGroups`, tiene dos opciones. Puede establecer los valores de los parámetros con su conexión JDBC u ODBC, o bien puede establecer los valores agregando elementos de atributo SAML a su IdP. Para obtener más información acerca de los parámetros `DbUser`, `AutoCreate` y `DbGroups`, consulte [Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM \(p. 330\)](#).

Note

Si utiliza una variable de política de IAM `${redshift:DbUser}`, como se describe en [Políticas de recursos de `GetClusterCredentials` \(p. 315\)](#), el valor de `DbUser` se sustituye por el valor obtenido por el contexto de la solicitud de la operación de la API. Los controladores de Amazon Redshift utilizan el valor de la propiedad `DbUser` proporcionado por la URL de conexión en lugar del valor proporcionado como atributo SAML.

Para ayudar a proteger esta configuración, recomendamos que utilice una condición en una política de IAM para validar el valor de `DbUser` con el `RoleSessionName`. Puede encontrar

ejemplos de cómo establecer una condición utilizando una política de IAM en [Política de ejemplo para usar GetClusterCredentials](#) (p. 321).

Para configurar el IdP para que establezca los parámetros DbUser, AutoCreate y DbGroups, incluya los siguientes elementos de Attribute:

- Un elemento Attribute con el atributo Name establecido en "https://redshift.amazon.com/SAML/Attributes/DbUser"

Establecimiento de la propiedad deAttributeValueElemento en el nombre del usuario que se va a conectar a la base de datos de Amazon Redshift.

El valor del elemento AttributeValue debe estar en mayúsculas, empezar por una letra, contener solo caracteres alfanuméricos, guion bajo ('_'), signo más ('+'), punto ('.'), arroba ('@') o guion ('-') y tener menos de 128 caracteres. Normalmente, el nombre de usuario es un ID de usuario (por ejemplo, bobsmith) o una dirección de correo electrónico (por ejemplo, bobsmith@example.com). El valor no puede incluir un espacio (por ejemplo, un nombre de visualización de un usuario como Bob Smith).

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbUser">
  <AttributeValue>user-name</AttributeValue>
</Attribute>
```

- Un elemento Attribute con el atributo Name establecido en "https://redshift.amazon.com/SAML/Attributes/AutoCreate"

Establezca el elemento AttributeValue en true para crear un nuevo usuario de base de datos si no existe ninguno. Establezca el atributo AttributeValue en false para especificar que el usuario de base de datos debe existir en la base de datos de Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/AutoCreate">
  <AttributeValue>true</AttributeValue>
</Attribute>
```

- Un elemento Attribute con el atributo Name establecido en "https://redshift.amazon.com/SAML/Attributes/DbGroups"

Este elemento contiene uno o más elementos AttributeValue. Establecer cadaAttributeValue a un nombre de grupo de base de datos que el elementoDbUserDurante la sesión cuando se conecta a la base de datos de Amazon Redshift.

```
<Attribute Name="https://redshift.amazon.com/SAML/Attributes/DbGroups">
  <AttributeValue>group1</AttributeValue>
  <AttributeValue>group2</AttributeValue>
  <AttributeValue>group3</AttributeValue>
</Attribute>
```

Paso 3: Cree un rol o usuario de IAM con permisos para llamar a GetClusterCredentials

El cliente SQL necesita autorización para llamar a la operación GetClusterCredentials en su nombre. Para proporcionar esta autorización, crea un usuario o rol de IAM y asocia una política que concede los permisos necesarios.

Para crear un rol de IAM con permisos para llamar a GetClusterCredentials

1. Cree un usuario o rol de IAM con el servicio IAM. También puede utilizar un usuario o rol existente. Por ejemplo, si ha creado un rol de IAM para el acceso al proveedor de identidad, puede asociar las políticas de IAM necesarias a ese rol.

2. Asocie una política de permisos con permiso para llamar a la operación `redshift:GetClusterCredentials`. En función de los parámetros opcionales que especifique, también puede permitir o restringir acciones y recursos adicionales en la política:
- Para permitir que el cliente SQL recupere el ID del clúster, AWSLa región y el puerto incluyen permiso para llamar al método `redshift:DescribeClusters` con el recurso de clúster de Redshift.
 - Si utiliza la opción `AutoCreate`, incluya el permiso para llamar a `redshift:CreateClusterUser` con el recurso `dbuser`. El siguiente nombre de recurso de Amazon (ARN) especifica el de Amazon Redshift `dbuser`. Reemplazar `region`, `account-id`, y `cluster-name` Con los valores de su AWS Región, cuenta y clúster. Para `dbuser-name`, especifique el nombre de usuario que se utilizará para iniciar sesión en la base de datos del clúster.

```
arn:aws:redshift:region:account-id:dbuser:cluster-name/dbuser-name
```

- (Opcional) Agregue un ARN que especifique el `dbname` En el siguiente formato: Reemplazar `region`, `account-id`, y `cluster-name` Con los valores de su AWS Región, cuenta y clúster. En `database-name`, especifique el nombre de una base de datos en la que el usuario va a iniciar sesión.

```
arn:aws:redshift:region:account-id:dbname:cluster-name/database-name
```

- Si utiliza la `DbGroups` Para incluir el permiso para llamar a la opción `redshift:JoinGroup` operación con Amazon Redshift `dbgroup` En el siguiente formato: Reemplazar `region`, `account-id`, y `cluster-name` Con los valores de su AWS Región, cuenta y clúster. En `dbgroup-name`, especifique el nombre del grupo de usuarios al que se unirá el usuario cuando inicie sesión.

```
arn:aws:redshift:region:account-id:dbgroup:cluster-name/dbgroup-name
```

Para obtener más información y ejemplos, consulte [Políticas de recursos de GetClusterCredentials](#) (p. 315).

En el siguiente ejemplo se muestra una política que permite al rol de IAM llamar a la operación `GetClusterCredentials`. Especificación de Amazon Redshift `dbuser` El recurso concede a la función acceso al nombre de usuario de base de datos `temp_creds_user` en el clúster denominado `examplecluster`.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:examplecluster/temp_creds_user"
  }
}
```

Puede utilizar el carácter comodín (*) para sustituir todo o una parte del nombre del clúster, el nombre de usuario y los nombres de grupos de usuarios de base de datos. El siguiente ejemplo permite el acceso a cualquier usuario que empiece por `temp_` a cualquier clúster en la cuenta especificada.

Important

En la instrucción del ejemplo siguiente, se especifica un carácter comodín (*) como parte del valor del recurso, de modo que la política admita cualquier recurso que comience por los caracteres

especificados. Utilizar un carácter comodín en las políticas de IAM puede resultar demasiado permisivo. Como práctica recomendada, es conveniente utilizar la política más restrictiva posible en la aplicación empresarial.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "redshift:GetClusterCredentials",
    "Resource": "arn:aws:redshift:us-west-2:123456789012:dbuser:*/temp_*"
  }
}
```

El siguiente ejemplo muestra una política que permite al rol de IAM llamar a la operación `GetClusterCredentials` con la opción para crear automáticamente un nuevo usuario y especificar los grupos a los que se une el usuario al iniciar sesión. La cláusula `"Resource": "*"` concede al rol acceso a cualquier recurso, incluidos clústeres, usuarios de bases de datos o grupos de usuarios.

```
"Version": "2012-10-17",
"Statement": {
  "Effect": "Allow",
  "Action": [
    "redshift:GetClusterCredentials",
    "redshift:CreateClusterUser",
    "redshift:JoinGroup"
  ],
  "Resource": "*"
}
```

Para obtener más información, consulte [Sintaxis de ARN de Amazon Redshift](#).

Paso 4: Crear usuarios y grupos de usuarios de base de datos

De manera opcional, puede crear un usuario de base de datos que utilice para iniciar sesión en la base de datos del clúster. Si crea credenciales de usuario temporales para un usuario existente, puede deshabilitar la contraseña del usuario para obligar al usuario a que inicie sesión con la contraseña temporal. También puede usar la opción `Autocreate` de `GetClusterCredentials` para crear automáticamente un nuevo usuario de base de datos.

Puede utilizar los permisos que quiera para crear los grupos de usuarios de base de datos a los que el usuario de base de datos de IAM se va a unir al iniciar sesión. Cuando llama a la operación `GetClusterCredentials`, puede especificar una lista de nombres de grupos de usuarios a los que se une el usuario cuando inicia sesión. Esta pertenencia a grupos solo es válida para las sesiones creadas utilizando las credenciales generadas con la solicitud especificada.

Para crear un usuario y grupos de usuarios de base de datos

1. Inicie sesión en la base de datos de Amazon Redshift y cree un usuario de base de datos mediante [CREAR USUARIO](#) o altere un usuario existente usando [ALTER USER](#).
2. Si lo desea, especifique la opción `PASSWORD DISABLE` para impedir que el usuario utilice una contraseña. Cuando se deshabilita la contraseña de un usuario, el usuario solo puede iniciar sesión con credenciales de usuario de IAM temporales. Si la contraseña no está deshabilitada, el usuario puede iniciar sesión con la contraseña o con las credenciales de usuario de IAM temporales. No puede deshabilitar la contraseña de un super usuario.

El siguiente ejemplo crea un usuario con la contraseña deshabilitada.

```
create user temp_creds_user password disable;
```

El siguiente ejemplo deshabilita la contraseña de un usuario existente.

```
alter user temp_creds_user password disable;
```

3. Cree grupos de usuarios de base de datos mediante [CREATE GROUP](#).
4. Utilice el comando [GRANT](#) para definir privilegios de acceso para los grupos.

Paso 5: Configurar una conexión JDBC u ODBC para usar credenciales de IAM

Puede configurar su cliente SQL con un controlador JDBC u ODBC de Amazon Redshift. Este controlador administra el proceso de creación de credenciales de usuario de base de datos y establecer una conexión entre el cliente SQL y la base de datos de Amazon Redshift.

Si usa un proveedor de identidad para la autenticación, especifique el nombre de un complemento de proveedor de credenciales. Los controladores JDBC y ODBC de Amazon Redshift incluyen complementos para los siguientes proveedores de identidad basados en SAML:

- Active Directory Federation Services (AD FS)
- PingOne
- Okta
- Microsoft Azure AD

Para ver los pasos para configurar Microsoft Azure AD como proveedor de identidades, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD](#) (p. 340).

Para configurar una conexión JDBC para usar las credenciales de IAM

1. Descargue el controlador JDBC de más reciente de Amazon Redshift de la [Configuración de una conexión de controlador JDBC versión 1.0](#) (p. 129) (Se ha creado el certificado).
2. Cree una URL de JDBC con las opciones de credenciales de IAM en uno de los siguientes formatos. Para utilizar la autenticación de IAM, agregue `iam:a` a la URL JDBC de Amazon Redshift siguiente `jdbc:redshift:Como se muestra en el ejemplo siguiente`.

```
jdbc:redshift:iam://
```

Addcluster-name,region,yaccount-id. El controlador JDBC usa la información de su cuenta de IAM y el nombre del clúster para recuperar el ID del clúster yAWSRegión . Para ello, el usuario o rol de IAM debe tener permiso para llamar a la operación `redshift:DescribeClusters` con el clúster especificado. Si el usuario o la función de IAM no tiene permiso para llamar a `laredshift:DescribeClusters`, incluya el ID del clúster,AWSRegión y puerto como se muestra en el ejemplo siguiente. El número de puerto es opcional. El puerto predeterminado es 5439.

```
jdbc:redshift:iam://examplecluster.abc123xyz789.us-west-2.redshift.amazonaws.com:5439/dev
```

3. Añada opciones de JDBC para proporcionar las credenciales de IAM. Para proporcionar las credenciales de IAM se usan diferentes combinaciones de opciones de JDBC. Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos](#) (p. 360).

La siguiente URL especifica AccessKeyID y SecretAccessKey para un usuario de IAM.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?  
AccessKeyID=AKIAIOSFODNN7EXAMPLE&SecretAccessKey=wJalrXUtnFEMI/K7MDENG/  
bPxRfICYEXAMPLEKEY
```

En el siguiente ejemplo se especifica un perfil con nombre que contiene las credenciales de IAM.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?Profile=user2
```

4. Agregue las opciones JDBC que utiliza el controlador JDBC para llamar a la operación de la API `GetClusterCredentials`. No incluya estas opciones si llama a la operación de la API `GetClusterCredentials` mediante programación.

El siguiente ejemplo incluye las opciones `GetClusterCredentials` de JDBC.

```
jdbc:redshift:iam://examplecluster:us-west-2/dev?  
plugin_name=com.amazon.redshift.plugin.AzureCredentialsProvider&UID=user&PWD=password&idp_tenant=my
```

Para configurar una conexión ODBC para usar las credenciales de IAM

En el procedimiento siguiente, sólo puede encontrar pasos para configurar la autenticación de IAM. Para ver el procedimiento para usar la autenticación estándar, que usa un nombre de usuario y una contraseña de la base de datos, consulte [Configuración de una conexión ODBC \(p. 138\)](#).

1. Instale y configure el controlador ODBC de Amazon Redshift para su sistema operativo. Para obtener más información, consulte la página [Configuración de una conexión ODBC \(p. 138\)](#).

Important

El controlador ODBC de Amazon Redshift debe ser 1.3.6.1000 o posterior.

2. Siga los pasos correspondientes a su sistema operativo para configurar las opciones de conexión.

Para obtener más información, consulte una de las siguientes:

- [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows \(p. 139\)](#)
 - [Utiliza un administrador de controladores ODBC para configurar el controlador en sistemas operativos Linux y macOS X \(p. 144\)](#)
3. En los sistemas operativos Microsoft Windows, obtenga acceso a la ventana Amazon Redshift ODBC Driver DSN Setup de.
 - a. En Connection Settings (Configuración de conexión), escriba la siguiente información:
 - Data Source Name
 - Server (Servidor) (opcional)
 - Port (Puerto) (opcional)
 - Base de datos

Si el usuario o la función de IAM tiene permiso para llamar a la operación `laredshift:DescribeClusters`, sólo se necesitan los datos de la base de datos. Amazon Redshift utiliza la región para obtener el servidor y el puerto llamando al método `DescribeCluster`.

Si el usuario o la función de IAM no tiene permiso para llamar a la operación `redshift:DescribeClusters`, proporcione valores para `Server` (Servidor) y `Port` (Puerto). El puerto predeterminado es 5439.

- b. En Autenticación, elija un valor para Tipo de autenticación.

Para cada tipo de autenticación, introduzca los valores que se enumeran a continuación:

Perfil de AWS

Introduzca la información siguiente:

- ID del clúster
- Región
- Profile name (Nombre de perfil)

Ingrese el nombre de un perfil en un `AWSEI` archivo de configuración contiene valores para las opciones de conexión ODBC. Para obtener más información, consulte [Uso de un perfil de configuración \(p. 336\)](#).

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Credenciales de IAM

Introduzca la información siguiente:

- ID del clúster
- Región
- AccessKeyId (ID de clave de acceso) y SecretAccessKey (Clave de acceso secreta)

El ID de clave de acceso y la clave de acceso secreta del rol o usuario de IAM configurado para la autenticación de la base de datos de IAM.

- SessionToken

SessionToken (Token de sesión) es obligatorio para las funciones de IAM con credenciales temporales. Para obtener más información, consulte [Credenciales de seguridad temporales](#).

Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser (obligatorio)
- User AutoCreate (Creación automática de usuarios) (opcional)
- DbGroups (Grupos de base de datos) (opcional)

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Proveedor de identidades: AD FS

Para la autenticación integrada de Windows con AD FS, deje User (Usuario) y Password (Contraseña) vacíos.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades) (opcional)

El puerto usado por el proveedor de identidad. El valor predeterminado es 443.

- Preferred Role (Función preferida)

El nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` de varios valores del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte [Configuración de aserciones SAML para el IdP \(p. 326\)](#).

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Proveedor de identidades: PingFederate

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades) (opcional)

El puerto usado por el proveedor de identidad. El valor predeterminado es 443.

- Preferred Role (Función preferida)

El nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` de varios valores del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte [Configuración de aserciones SAML para el IdP \(p. 326\)](#).

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser

- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Proveedor de identidades: Okta

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

Proporcione los detalles del IdP:

- IdP Host (Host del proveedor de identidades)

El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales (/).

- IdP Port (Puerto del proveedor de identidades)

Este valor no es utilizado por Okta.

- Preferred Role (Función preferida)

Un nombre de recurso de Amazon (ARN) de un rol de IAM obtenido de los elementos `AttributeValue` del atributo `Role` en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido.

Para obtener más información, consulte [Configuración de aserciones SAML para el IdP \(p. 326\)](#).

- Okta App ID (ID de aplicación Okta)

Un ID de una aplicación Okta. El valor de App ID se incluye detrás de "amazon_aws" en el enlace incrustado de la aplicación Okta. Póngase en contacto con el administrador de su IdP para obtener este valor.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Proveedor de identidades: Azure AD

En User (Usuario) y Password (Contraseña), introduzca el nombre de usuario y la contraseña del IdP.

ParaCluster ID (ID del clúster)yRegión, ingrese el ID del clúster yAWSRegión del clúster de Amazon Redshift.

ParaBase de datos, introduzca la base de datos que creó para su clúster de Amazon Redshift.

Proporcione los detalles del IdP:

- Arrendatario de IdP

El inquilino utilizado para Azure AD.

- Secreto de cliente de Azure

El secreto de cliente de la aplicación empresarial de Amazon Redshift en Azure.

- ID de cliente de Azure

El ID de cliente (ID de aplicación) de la aplicación empresarial de Amazon Redshift en Azure.

(Opcional) Proporcione detalles de las opciones que utiliza el controlador ODBC para llamar a la operación de la API `GetClusterCredentials`:

- DbUser
- User AutoCreate (Creación automática de usuarios)
- DbGroups

Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos \(p. 360\)](#).

Opciones para proporcionar credenciales de IAM

Para proporcionar credenciales de IAM para una conexión JDBC u ODBC, elija una de las siguientes opciones.

- AWS profile

Como alternativa a proporcionar valores de credenciales en forma de opciones de JDBC u ODBC, puede incluir los valores en un perfil con nombre. Para obtener más información, consulte [Uso de un perfil de configuración \(p. 336\)](#).

- Credenciales de IAM

Proporcione valores para `AccessKeyId`, `SecretAccessKey` y, opcionalmente, `SessionToken` en forma de opciones de JDBC u ODBC. `SessionToken` es obligatorio únicamente para un rol de IAM con credenciales temporales. Para obtener más información, consulte [Opciones de JDBC y ODBC para proporcionar credenciales de IAM \(p. 336\)](#).

- Federación de proveedores de identidades

Cuando utilice la federación de proveedores de identidades para permitir que los usuarios de un proveedor de identidades se autenticquen en Amazon Redshift, especifique el nombre de un complemento de proveedor de credenciales. Para obtener más información, consulte [Uso de un complemento de proveedor de credenciales \(p. 337\)](#).

Los controladores JDBC y ODBC de Amazon Redshift incluyen complementos para los siguientes proveedores de credenciales de federación de identidades basados en SAML:

- Servicios de identidad federada de Microsoft Active (AD FS)
- PingOne
- Okta
- Microsoft Azure Active Directory (Azure AD)

Puede proporcionar el nombre del complemento y los valores relacionados en forma de opciones de JDBC u ODBC o mediante un perfil. Para obtener más información, consulte [Configurar las opciones del controlador JDBC \(p. 134\)](#) y [Configurar las opciones del controlador ODBC \(p. 148\)](#).

Para obtener más información, consulte [Configurar una conexión JDBC u ODBC para usar credenciales de IAM](#) (p. 330).

Uso de un perfil de configuración

Puede proporcionar las opciones de credenciales de IAM `yGetClusterCredentials` como configuración en perfiles con nombre en su `AWS` Archivo de configuración. Para proporcionar el nombre del perfil, utilice la opción `Profile JDBC`. La configuración se guarda en un archivo llamado `config` un archivo denominado `credentials` en una carpeta denominada `.aws` en el directorio principal.

Para un complemento de proveedor de credenciales basado en SAML incluido con un controlador JDBC u ODBC de Amazon Redshift, puede utilizar la configuración descrita anteriormente en [Uso de un complemento de proveedor de credenciales](#) (p. 337). Si no se utiliza `plugin_name`, se ignoran las demás opciones.

En el siguiente ejemplo se muestra el archivo `~/.aws/credentials` con dos perfiles.

```
[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/////////
wEXAMPLEtc764bNrC9SAPBSM22wD0k4x4HIZ8j4FZTWdQWLWsKWHGBuFqwAeMicRXmxfpSPfIeoIYRqTflfKD8YUuwthAx7mSEI/
qkPpKPi/kMcGd
QrmGdeehM4IC1NtBmUpp2wUE8phUZampKsburEDy0KPKyQDYwT7WZ0wq5VSXDvp75YU
9HFv1Rd8Tx6q6fE8YQcHNVXakiY9q6d+xo0rKwT38xVqr7ZD0u0iPPkUL64lIZbqBAz
+scqKmlzm8FDrypNC9Yjc8fPOLn9FX9KSYvKTr4rvx3iSi1TJabIQwj2ICCR/oLxBA==
```

Para usar las credenciales para el ejemplo `user2`, especifique `Profile=user2` en la URL de JDBC.

Para obtener más información sobre el uso de perfiles, consulte [Perfiles con nombre](#) en la AWS Command Line Interface Guía del usuario de .

Para obtener más información sobre el uso de perfiles para el controlador JDBC, consulte [Guía de instalación y configuración de controladores JDBC de Amazon Redshift](#).

Para obtener más información sobre el uso de perfiles para el controlador ODBC, consulte [Guía de instalación y configuración de controladores ODBC de Amazon Redshift](#).

Opciones de JDBC y ODBC para proporcionar credenciales de IAM

En la tabla siguiente se indican las opciones de JDBC y ODBC para proporcionar credenciales de IAM.

Opción	Descripción
Iam	Para uso exclusivo en una cadena de conexión de ODBC. Establézcalo en 1 para usar la autenticación de IAM.
AccessKeyId	El ID de clave de acceso y clave de acceso secreta para el rol de IAM o usuario de IAM configurado para autenticación de base de datos de IAM. <code>SessionToken</code> es necesario para un rol de IAM con credenciales temporales. <code>SessionToken</code> no se usa para un usuario de IAM. Para obtener más información, consulte Credenciales de seguridad temporales .
SecretAccessKey	
SessionToken	

Opción	Descripción
<code>plugin_name</code>	El nombre completo de una clase que implementa un proveedor de credenciales. El Amazon Redshift BC de incluye complementos de proveedores de credenciales basados en SAML. Si proporciona <code>plugin_name</code> , también puede proporcionar otras opciones relacionadas. Para obtener más información, consulte Uso de un complemento de proveedor de credenciales (p. 337) .
<code>Profile</code>	El nombre de un perfil en unAWSque contenga valores para las opciones de conexión de JDBC. Para obtener más información, consulte Uso de un perfil de configuración (p. 336) .

Uso de un complemento de proveedor de credenciales

Amazon Redshift utiliza complementos de proveedores de credenciales para la autenticación de inicio de sesión único (SSO)

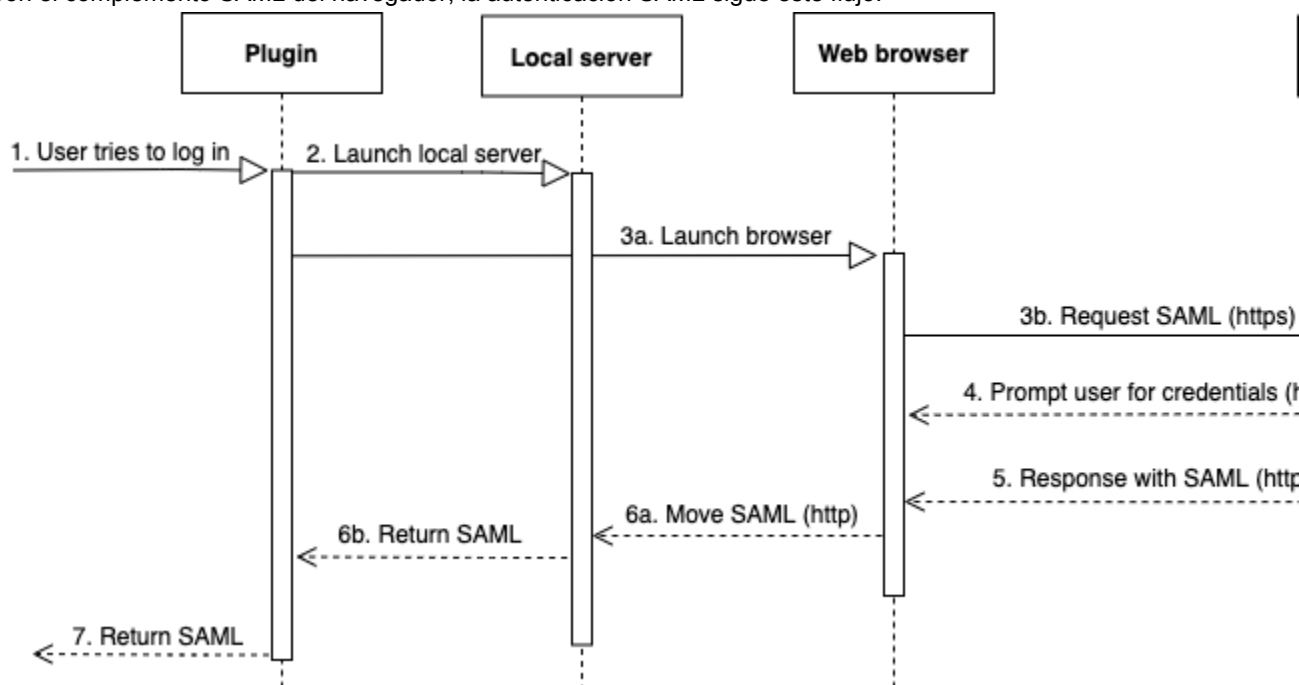
Para admitir la autenticación de inicio de sesión único (SSO), Amazon Redshift proporciona el complemento de Azure AD para Microsoft Azure Active Directory. Para obtener información sobre cómo configurar este complemento, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD \(p. 340\)](#).

Configuración de la autenticación multifactor

Configuración de la autenticación multifactor

Para admitir Multi-Factor Authentication (MFA), Amazon Redshift proporciona complementos basados en navegador. Utilice el complemento SAML del navegador para Okta, PingOne ty y el complemento de Azure AD del navegador para Microsoft Azure Active Directory.

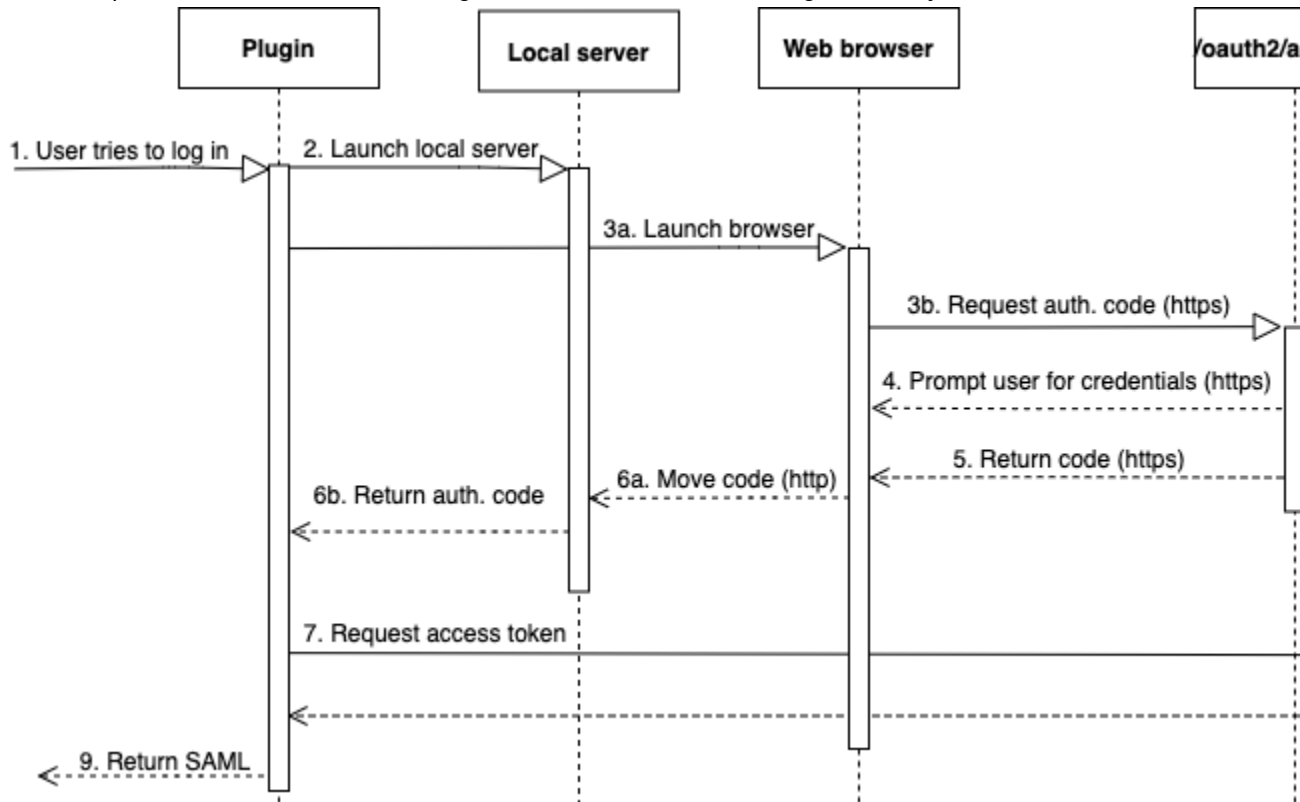
Con el complemento SAML del navegador, la autenticación SAML sigue este flujo:



1. Un usuario intenta iniciar sesión.
2. El complemento lanza un servidor local para escuchar las conexiones entrantes en el localhost.

3. El complemento lanza un navegador web para solicitar una respuesta SAML a través de HTTPS desde el punto de enlace del proveedor de identidad federada de la URL de inicio de sesión SSO especificado.
4. El navegador web sigue el enlace y pide al usuario que escriba las credenciales.
5. Una vez que el usuario autentica y otorga su consentimiento, el punto de enlace del proveedor de identidad federadas devuelve una respuesta SAML a través de HTTPS al URI indicado por `redirect_uri`.
6. El navegador web traslada el mensaje de respuesta con la respuesta SAML a la `redirect_uri` indicada.
7. El servidor local acepta la conexión entrante y el complemento recupera la respuesta SAML y la transfiere a Amazon Redshift.

Con el complemento de Azure AD del navegador, la autenticación SAML sigue este flujo:



1. Un usuario intenta iniciar sesión.
2. El complemento lanza un servidor local para escuchar las conexiones entrantes en el localhost.
3. El complemento lanza un explorador web para solicitar un código de autorización desde el punto de enlace `oauth2/authorize` de Azure AD.
4. El navegador web sigue el enlace generado a través de HTTPS y solicita al usuario que escriba las credenciales. El enlace se genera utilizando propiedades de configuración, como `tenant` y `client_id`.
5. Una vez que el usuario se autentica y otorga su consentimiento, el punto de enlace `oauth2/authorize` de Azure AD devuelve y envía una respuesta a través de HTTPS con el código de autorización al `redirect_uri` indicado.
6. El navegador web traslada el mensaje de respuesta con la respuesta SAML a la `redirect_uri` indicada.
7. El servidor local acepta la conexión entrante y las solicitudes del complemento, recupera el código de autorización y envía una solicitud POST al punto de enlace `oauth2/token` de Azure AD.

8. El punto de enlace `oauth2/token` de Azure AD devuelve una respuesta con un token de acceso al `redirect_uri` indicado.
9. El complemento recupera la respuesta SAML y la transfiere a Amazon Redshift.

Consulte las siguientes secciones:

- Active Directory Federation Services (AD FS)

Para obtener más información, consulte [Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con AD FS \(p. 348\)](#).

- PingOne (Ping)

Ping solo puede usarse con el adaptador de IdP PingOne mediante la autenticación de formularios.

Para obtener más información, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Ping Identity \(p. 352\)](#).

- Okta

Okta solo es compatible con la aplicación suministrada por Okta que se utiliza con la AWS Management Console.

Para obtener más información, consulte [Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con Okta \(p. 356\)](#).

- Microsoft Azure Active Directory

Para obtener más información, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD \(p. 340\)](#).

Configuración de las opciones del complemento

Configuración de las opciones del complemento

Para usar un complemento de proveedor de credenciales basado en SAML, especifique las siguientes opciones utilizando las opciones de JDBC u ODBC o un perfil con nombre. Si `plugin_name` no se especifica, se ignoran las demás opciones.

Opción	Descripción
<code>plugin_name</code>	Para JDBC, el nombre de la clase que implementa un proveedor de credenciales. Especifique uno de los siguientes valores: • Para Active Directory Federation Services <code>com.amazon.redshift.plugin.AdfsCredentialsProvider</code> • Para Okta <code>com.amazon.redshift.plugin.OktaCredentialsProvider</code> • Para PingFederate <code>com.amazon.redshift.plugin.PingCredentialsProvider</code> • Para Microsoft Azure Active Directory <code>com.amazon.redshift.plugin.AzureCredentialsProvider</code>

Opción	Descripción
	- Para SAML MFA com.amazon.redshift.plugin.BrowserSamlCredentialsProvider - Para inicio de sesión único de Microsoft Azure Active Directory con MFA com.amazon.redshift.plugin.BrowserAzureCredentialsProvider Para ODBC, especifique uno de los siguientes valores: - Para Active Directory Federation Services: adfs - Para Okta: okta - Para PingFederate: ping - Para Microsoft Azure Active Directory: azure - Para SAML MFA: browser saml - Para inicio de sesión único de Microsoft Azure Active Directory con MFA: browser azure ad
idp_host	El nombre del host del proveedor de identidad corporativo. Este nombre no debe incluir barras diagonales ("/"). Para un proveedor de identidad de Okta, el valor de idp_host debe terminar por .okta.com.
idp_port	El puerto usado por el proveedor de identidad. El valor predeterminado es 443. Este puerto se omite para Okta.
preferred_role	El nombre de recurso de Amazon (ARN) de los elementos AttributeValue para el atributo Role en la aserción SAML. Póngase en contacto con el administrador de su IdP para encontrar el valor adecuado para el rol preferido. Para obtener más información, consulte Configuración de aserciones SAML para el IdP (p. 326) .
user	Un nombre de usuario corporativo, incluido el dominio cuando proceda. Por ejemplo, en Active Directory, el nombre de dominio debe tener el formato dominio\nombre_usuario.
password	La contraseña del usuario corporativo. Le recomendamos que no utilice esta opción. En lugar de ello, use el cliente SQL para proporcionar la contraseña.
app_id	Un ID de una aplicación Okta. Solo se usa con Okta. El valor de app_id se incluye detrás de amazon_aws en el enlace incrustado de la aplicación Okta. Para obtener este valor, póngase en contacto con el administrador de su IdP. A continuación se muestra un ejemplo de un enlace incrustado de aplicación: https://example.okta.com/home/amazon_aws/00a2hylwrpM8UGehd1t7/272
idp_tenant	Un inquilino utilizado para Azure AD. Se utiliza solo con Azure.
client_id	Un ID de cliente para la aplicación empresarial de Amazon Redshift en Azure AD. Se utiliza solo con Azure.

Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD

Puede utilizar Microsoft Azure AD como proveedor de identidades (IdP) para tener acceso al clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información sobre la configuración de AWS como

proveedor de servicios para el IdP, consulte [Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el IdP de SAML 2.0](#) en la Guía del usuario de IAM.

Note

Para usar Azure AD con JDBC, el controlador JDBC de Amazon Redshift debe ser la versión 1.2.37.1061 o posterior. Para utilizar Azure AD con ODBC, el controlador ODBC de Amazon Redshift debe ser la versión 1.4.10.1000 o posterior.

Vea el siguiente vídeo para obtener información sobre cómo federar el acceso de Amazon Redshift con el inicio de sesión único de Microsoft Azure AD: [Federación del acceso a Amazon Redshift con el inicio de sesión único de Microsoft Azure AD](#).

Para configurar Azure AD y su AWS cuenta para confiar el uno en el otro

1. Cree o use un clúster de Amazon Redshift de existente para que los usuarios de Azure AD se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte [Creating a Cluster \(Creación de un clúster\)](#).
2. Configure Azure Active Directory, grupos y usuarios utilizados para AWS en el portal de Microsoft Azure.
3. Añada Amazon Redshift como aplicación empresarial en el portal de Microsoft Azure para utilizar el inicio de sesión único en el AWS. Inicio de sesión de consola y federado en Amazon Redshift. Elija Enterprise application (Aplicación de Enterprise).
4. Elija +New application (+Nueva aplicación). Aparecerá la página Add an application (Agregar una aplicación).
5. Buscar **AWS** en el campo de búsqueda.
6. Seleccionar Amazon Web Services (AWS) y elija Add. Esto crea el AWS. Revisión de.
7. En Manage (Administrar), elija Single sign-on (Inicio de sesión único).
8. Elija SAML. Amazon Web Services (AWS) aparecerá la página Inicio de sesión basado en SAML.
9. Elija Yes (Sí) para continuar con la página Set up Single Sign-On with SAML (Configurar inicio de sesión único con SAML). En esta página se muestra la lista de preconfigurados AWS. Atributos relacionados con SSO.
10. En Basic SAML Configuration (Configuración básica de SAML), elija el icono de edición y, a continuación, Save (Guardar).
11. Cuando esté configurando para más de una aplicación, proporcione un valor de identificador. Por ejemplo, escriba **<https://signin.aws.amazon.com/saml#2>**. Tenga en cuenta que a partir de la segunda aplicación, utilice este formato con un signo # para especificar un valor SPN único.
12. En la sección User Attributes and Claims (Atributos y reclamaciones de usuario), elija el icono de edición.

De forma predeterminada, las reclamaciones Identificador único de usuario (UID), Role, RoleSessionName y SessionDuration están preconfiguradas.

13. Elija + Add new claim (+Agregar nueva reclamación) para agregar una reclamación para los usuarios de base de datos.

En Name (Nombre), escriba **DbUser**.

En Namespace (Espacio de nombres), escriba **<https://redshift.amazon.com/SAML/Attributes>**.

En Source (Origen), elija Attribute (Atributo).

En Source attribute (Atributo de origen), elija user.userprincipalname. A continuación, elija Save (Guardar).

14. Elija + Add new claim (+Agregar nueva reclamación) para agregar una reclamación para AutoCreate.

En Name (Nombre), escriba **AutoCreate**.

En Namespace (Espacio de nombres), escriba **https://redshift.amazon.com/SAML/Attributes**.

En Source (Origen), elija Attribute (Atributo).

En Source attribute (Atributo de origen), elija "true". A continuación, elija Save (Guardar).

Aquí, **123456789012** es su AWS account, **AzureSSO** es un rol de IAM que ha creado y **AzureADProvider** es el proveedor de IAM.

Nombre de la reclamación	Valor
Identificador de usuario único (ID de nombre)	user.userprincipalname
https://aws.amazon.com/SAML/Attributes/SessionDuration	"900"
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: 123456789012 :role/ AzureSSO ,arn:aws:iam:: 123456789012 :saml-provider/ AzureADProvider
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. En Registro de aplicaciones > **your-application-name** > Autenticación, agregue Aplicación móvil y de escritorio. Especifique la URL como http://localhost/redshift/.
16. En la sección SAML Signing Certificate (Certificado de firma SAML), elija Download (Descargar) para descargar y guardar el archivo XML de metadatos de federación para usarlo cuando cree un proveedor de identidad SAML de IAM. Este archivo se utiliza para crear el AWS SSO identidad federada.
17. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Azure Enterprise Application. Para conocer los pasos en detalle, consulte [Creación y administración de un proveedor de identidades de IAM \(consola\)](#) en la Guía del usuario de IAM.
18. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de un rol para SAML](#) en la Guía del usuario de IAM.
19. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de políticas de IAM \(Consola\)](#) en la Guía del usuario de IAM.

Modifique la siguiente política (en formato JSON) para su entorno:

- Sustituya la AWS Región del clúster para **us-west-1**.
- Sustituya su AWS account de **123456789012**.
- Sustituya el identificador de clúster (o * para todos los clústeres) por **cluster-identifier**.

- Sustituya la base de datos (o * para todas las bases de datos) por *dev*.
- Sustituya el identificador único de su rol de IAM por *AROAJ2UCCR6DPCEXAMPLE*.
- Sustituya el dominio de correo electrónico de su arrendatario o empresa por *example.com*.
- Sustituya el grupo de base de datos al que planea asignar el usuario por *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-  
identifier/my_dbgroup"
    },
    {
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeClusters",
        "iam:ListRoles"
      ],
      "Resource": "*"
    }
  ]
}
```

Esta política concede permisos de la siguiente manera:

- La primera sección concede permiso a la operación `GetClusterCredentials` de la API para obtener credenciales temporales para el clúster especificado. En este ejemplo, el recurso es *cluster-identifier* Base de datos de *dev*, en account *123456789012*, y en AWS Región *us-west-1*. La cláusula `${redshift:DbUser}` permite que sólo los usuarios que coincidan con el valor `DbUser` especificado en Azure AD se conecten.
- La cláusula de condición obliga a que solo ciertos usuarios obtengan credenciales temporales. Se trata de usuarios con el rol especificado por el identificador único de rol *AROAJ2UCCR6DPCEXAMPLE* en la cuenta de IAM identificada por una dirección de email en el dominio de correo electrónico de su empresa. Para obtener más información sobre los ID únicos, consulte [ID únicos](#) en la Guía del usuario de IAM.

La configuración con el IdP (en este caso, Azure AD) determina cómo se escribe la cláusula de condición. Si el correo electrónico de su empleado es `johndoe@example.com`, primero establezca `${redshift:DbUser}` en el supercampo que coincida con el nombre de usuario del empleado `johndoe`. A continuación, para que esta condición funcione, establezca la propiedad `AWSSAMLRoleSessionName` para el supercampo que coincida con el correo electrónico del empleado `johndoe@example.com`. Cuando tome este enfoque, tenga en cuenta lo siguiente:

- Si establece `${redshift:DbUser}` para que sea el correo electrónico del empleado, quite el `@example.com` en el archivo JSON de muestra para que coincida con el `RoleSessionName`.
- Si establece `RoleSessionId` para que solo sea el nombre de usuario del empleado, quite el `@example.com` en el ejemplo para que coincida con el `RoleSessionName`.
- En el JSON de ejemplo, `${redshift:DbUser}` y `RoleSessionName` se establecen en el correo electrónico del empleado. En este ejemplo, JSON utiliza el nombre de usuario de base de datos de Amazon Redshift `con@example.com` para que el usuario inicie sesión para obtener acceso al clúster de.
- La segunda sección concede permiso para crear un nombre `dbuser` en el clúster especificado. En este JSON de muestra, restringe la creación a `${redshift:DbUser}`.
- La tercera sección concede permisos para especificar a qué `dbgroup` puede unirse un usuario. En este JSON de muestra, un usuario puede unirse al grupo `my_dbgroup` en el clúster especificado.
- La cuarta sección otorga permiso a las acciones que el usuario puede realizar en todos los recursos. En este ejemplo JSON, permite a los usuarios llamar a `aredshift:DescribeClusters` para obtener información del clúster, como el extremo del clúster, `AWSRegión` y puerto. También permite a los usuarios llamar a `iam:ListRoles` para comprobar qué roles puede asumir un usuario.

Para configurar JDBC para la autenticación en Microsoft Azure AD

- Configure el cliente de la base de datos para conectarse al clúster a través de JDBC mediante el inicio de sesión único de Azure AD.

Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Azure AD o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#).

Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

- a. Inicie SQL Workbench/J. En la **Select Connection Profile**, agregue una **Grupo de perfiles Clave de AzureAuth**.
- b. En **Connection Profile (Perfil de conexión)**, escriba **Azure**.
- c. Elija **Manage Drivers (Administrar controladores)**, y elija **Amazon Redshift**. Elija el icono **Open folder (Abrir carpeta)** junto a **Library (Biblioteca)** y a continuación, elija el archivo **JDBC .jar** adecuado.
- d. En la página **Select connection profile (Seleccionar perfil de conexión)** agregue información al perfil de conexión de la siguiente manera:
 - En **User (Usuario)**, escriba su nombre de usuario de Microsoft Azure. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse.
 - En **Password (Contraseña)**, escriba la contraseña de Microsoft Azure.

- En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
 - En URL, escriba **jdbc:redshift:iam//your-cluster-identifier:your-cluster-region/your-database-name**.
- e. Elija Extended properties (Propiedades extendidas) para agregar información adicional a las propiedades de conexión, como se describe a continuación.

Para la configuración de inicio de sesión único (SSO) de Azure AD, agregue información adicional como se indica a continuación:

- En plugin_name, escriba **com.amazon.redshift.plugin.AzureCredentialsProvider**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de Azure AD como método de autenticación.
- En idp_tenant, escriba **your-idp-tenant**. Se utiliza solo para Microsoft Azure AD. Este es el nombre del arrendatario de su empresa configurado en Azure AD. Este valor puede ser el nombre del arrendatario o el identificador único del inquilino con guiones.
- En client_secret, escriba **your-azure-redshift-application-client-secret**. Se utiliza solo para Microsoft Azure AD. Este es el secreto de cliente de la aplicación de Amazon Redshift de que creó al configurar la configuración de inicio de sesión único de Azure. Esto solo es aplicable al complemento com.amazon.redshift.plugin.AzureCredentialsProvider.
- En client_id, escriba **your-azure-redshift-application-client-id**. Se utiliza solo para Microsoft Azure AD. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift de que creó al configurar la configuración de inicio de sesión único de Azure.

Para el inicio de sesión único (SSO) de Azure AD con configuración de MFA, agregue información adicional a las propiedades de conexión de la siguiente manera:

- En plugin_name, escriba **com.amazon.redshift.plugin.BrowserAzureCredentialsProvider**. Este valor especifica al controlador que debe utilizar el inicio de sesión único de Azure AD con MFA como método de autenticación.
- En idp_tenant, escriba **your-idp-tenant**. Se utiliza solo para Microsoft Azure AD. Este es el nombre del arrendatario de su empresa configurado en Azure AD. Este valor puede ser el nombre del arrendatario o el identificador único del inquilino con guiones.
- En client_id, escriba **your-azure-redshift-application-client-id**. Esta opción solo se usa para Microsoft Azure AD. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift de que creó al configurar la configuración del inicio de sesión único de Azure con MFA.
- En listen_port, escriba **your-listen-port**. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890.
- En idp_response_timeout, escriba **the-number-of-seconds**. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión.

Para configurar ODBC para la autenticación en Microsoft Azure AD

- Configure el cliente de base de datos para que se conecte al clúster a través de ODBC mediante el inicio de sesión único de Azure AD.

Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y macOS X. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de más reciente de Amazon Redshift para su sistema operativo según se indica a continuación:

- Para Windows, vea [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows](#) (p. 139).
- Para macOS, consulte [Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X](#) (p. 143).
- Para Linux, vea [Instalación del controlador ODBC de Amazon Redshift en Linux](#) (p. 141).

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba **your-DSN**. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth type (Tipo de autenticación) para la configuración de inicio de sesión único de Azure AD, elija **Identity Provider: Azure AD**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Azure.
- En Auth type (Tipo de autenticación) para la configuración de inicio de sesión único Azure AD SSO con MFA, elija **Identity Provider: Browser Azure AD**. Este es el método de autenticación que utiliza el controlador ODBC para autenticarse mediante el inicio de sesión único de Azure con MFA.
- En Cluster ID (ID de clúster), escriba **your-cluster-identifier**.
- En Region (Región), escriba **your-cluster-region**.
- En Database (Base de datos), escriba **your-database-name**.
- En User (Usuario), escriba **your-azure-username**. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Usa esto solo con Tipo de autenticacionesProveedor de identidades: Azure AD.
- En Password (Contraseña), escriba **your-azure-password**. Usa esto solo con Tipo de autenticacionesProveedor de identidades: Azure AD.
- En IdP Tenant (Arrendatario de IdP), escriba **your-idp-tenant**. Este es el nombre del arrendatario de su empresa configurado en su IdP (Azure). Este valor puede ser el nombre del arrendatario o el identificador único del inquilino con guiones.
- En Azure Client Secret (Secreto de cliente de Azure), escriba **your-azure-redshift-application-client-secret**. Este es el secreto de cliente de la aplicación de Amazon Redshift de que creó al configurar la configuración de inicio de sesión único de Azure.
- En Azure Client ID (ID de cliente de Azure), escriba **your-azure-redshift-application-client-id**. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó al configurar la configuración de inicio de sesión único de Azure.
- En Puerto de escucha, escriba **your-listen-port**. Este es el puerto de escucha predeterminado en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento Browser Azure AD.
- En Response Timeout (Tiempo de espera de respuesta), escriba **the-number-of-seconds**. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión. Esta opción solo se aplica al complemento Browser Azure AD.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

Note

Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba **your-cluster-identifier**. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba **your-cluster-region**. Este es el AWS Región del clúster de Amazon Redshift creado.
- En database, escriba **your-database-name**. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **en-us**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **1**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En plugin_name para la configuración de inicio de sesión único de Azure AD, escriba **AzureAD**. Esto especifica al controlador que debe utilizar el inicio de sesión único de Azure como método de autenticación.
- En plugin_name para la configuración del inicio de sesión único de Azure AD con MFA, escriba **BrowserAzureAD**. Esto especifica al controlador que debe utilizar el inicio de sesión único de Azure con MFA como método de autenticación.
- En uid, escriba **your-azure-username**. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Utilice esto solo para plugin_name es AzureAD.
- En pwd, escriba **your-azure-password**. Utilice esto solo para plugin_name es AzureAD.
- En idp_tenant, escriba **your-idp-tenant**. Este es el nombre del arrendatario de su empresa configurado en su IdP (Azure). Este valor puede ser el nombre del arrendatario o el identificador único del inquilino con guiones.
- En client_secret, escriba **your-azure-redshift-application-client-secret**. Este es el secreto de cliente de la aplicación de Amazon Redshift de que creó al configurar la configuración de inicio de sesión único de Azure.
- En client_id, escriba **your-azure-redshift-application-client-id**. Este es el ID de cliente (con guiones) de la aplicación de Amazon Redshift que creó al configurar la configuración de inicio de sesión único de Azure.
- En listen_port, escriba **your-listen-port**. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto se aplica al complemento Browser Azure AD.
- En idp_response_timeout, escriba **the-number-of-seconds**. Este es el período de tiempo especificado en segundos que esperar la respuesta de Azure. Esta opción se aplica al complemento Browser Azure AD.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Para solucionar problemas con el complemento Azure AD de navegador

1. Para utilizar el complemento Azure AD de navegador, debe establecer la URL de respuesta especificada en la solicitud para que coincida con la URL de respuesta configurada para la aplicación.

Vaya a la página Configurar el inicio de sesión único con SAML en el portal de Microsoft Azure. A continuación, compruebe que la URL de respuesta está establecida en <http://localhost/redshift/>.

2. Si aparece un error de inquilino de IdP, compruebe que el nombre de Inquilino de IdP coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

En Windows, vaya a la pestaña Configuración de conexión de Sección sobre de la Configuración de DSN ODBC de Amazon Redshift (Se ha creado el certificado). A continuación, compruebe que el nombre de inquilino de su empresa configurado en su IdP (Azure) coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

En macOS y Linux, busque el archivo `odbc.ini`. A continuación, compruebe que el nombre de inquilino de su empresa configurado en su IdP (Azure) coincide con el nombre de dominio que utilizó inicialmente para configurar Active Directory en Microsoft Azure.

3. Si aparece un error que indica que la URL de respuesta especificada en la solicitud no coincide con las URL de respuesta configuradas para la aplicación, verifique que los URI de redirección son los mismos que la URL de respuesta.

Vaya a la página Registro de aplicaciones de su aplicación en el portal de Microsoft Azure. A continuación, compruebe que los URI de redirección coinciden con la URL de respuesta.

4. Si obtiene la respuesta inesperada de error no autorizado, verifique que haya completado la configuración de Aplicaciones móviles y de escritorio.

Vaya a la página Registro de aplicaciones de su aplicación en el portal de Microsoft Azure. A continuación, vaya a Autenticación y compruebe que ha configurado Aplicaciones móviles y de escritorio para utilizar `http://localhost/redshift/` como URI de redirección.

Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con AD FS

Puede utilizar AD FS como proveedor de identidad (IdP) para acceder al clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información sobre la configuración de AWS como proveedor de servicios para AD FS, consulte [Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el IdP](#) de [AWS IAM](#) en la Guía del usuario de IAM.

Para configurar AD FS y su AWS cuenta para confiar el uno en el otro

1. Cree o use un clúster de Amazon Redshift de existente para que los usuarios de AD FS se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte [Creating a Cluster \(Creación de un clúster\)](#).
2. Configurar AD FS para controlar el acceso de Amazon Redshift en Microsoft Management Console:
 1. Elija ADFS 2.0, y, a continuación, elija Add Relying Party Trust (Agregar confianza de parte de confianza). En la página Add Relying Party Trust Wizard (Asistente para agregar confianza de parte), elija Start (Inicio).
 2. En la página Select Data Source (Seleccionar origen de datos), elija Import data about the relying party published online or on a local network (Importar los datos sobre el usuario de confianza publicado en línea o en una red local).
 3. En Federation metadata address (host name or URL) (Dirección de metadatos de federación [nombre de host o URL]), escriba `https://signin.aws.amazon.com/saml-metadata.xml`. El archivo XML de metadatos es un documento de metadatos SAML estándar que describe AWS como parte confiante.
 4. En la página Specify Display Name (Especificar nombre para mostrar), escriba un valor para Display name (Nombre para mostrar).
 5. En la página Choose Issuance Authorization Rules (Elegir reglas de autorización de emisión), elija una regla de autorización de emisión para permitir o denegar a todos los autores que accedan a esta parte de confianza.

6. En la página Ready to Add Trust (Listo para agregar confianza), revise la configuración.
7. En la página Finish (Finalizar), elija Open the Edit Claim Rules dialog for this relying party trust when the wizard closes (Abrir el cuadro de diálogo Editar reglas de reclamación para esta relación de confianza para usuarios autenticado al cerrarse el asistente).
8. En el menú contextual (clic con el botón derecho), elija Relying Party Trusts (Relaciones de confianza para usuario autenticado).
9. Para el usuario autenticado, abra el menú contextual (haga clic con el botón derecho) y elija Edit Claim Rules (Editar reglas de reclamación). En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla).
10. En Claim rule template (Plantilla de regla de reclamación), elija Transform an Incoming Claim (Transformar una reclamación entrante) y, a continuación, en la página Edit Rule – NameId (Editar regla – NameId), haga lo siguiente:
 - En Claim rule name (Nombre de regla de reclamación), escriba NameId.
 - En Incoming claim name (Nombre de reclamación entrante), elija Windows Account Name (Nombre de cuenta de Windows).
 - En Outgoing claim name (Nombre de reclamación saliente), elija Name ID (ID de nombre).
 - En Outgoing name ID format (Formato de ID de nombre saliente), elija Persistent Identifier (Identificador persistente).
 - Elija Pass through all claim values (Acceso directo a todos los valores de reclamación).
11. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), en Claim rule template (Plantilla de regla de reclamación), elija Send LDAP Attributes as Claims (Enviar atributos LDAP como reclamaciones).
12. En la página Configure Rule (Configurar regla), haga lo siguiente:
 - En Claim rule name (Nombre de regla de reclamación), escriba RoleSessionName.
 - En Attribute store (Almacén de atributos), elija Active Directory.
 - En LDAP Attribute (Atributo LDAP), elija Email Addresses (Direcciones de correo electrónico).
 - Para Tipo de reclamación saliente, elija `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
13. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), para Claim rule template (Plantilla de regla de reclamación), elija Send Claims Using a Custom Rule (Enviar reclamaciones utilizando una regla personalizada).
14. En la página Edit Rule – Get AD Groups (Editar regla – Obtener grupos de AD), en Claim rule name (Nombre de regla de reclamación), escriba Get AD Groups (Obtener grupos de AD).
15. En Custom rule (Regla personalizada), escriba lo siguiente.

```
c:[Type ==  
identity/claims/windowsaccountname",  
    Issuer == "AD AUTHORITY"] => add(store = "Active  
Directory",  
    types = ("http://temp/variable"), query =  
    ";tokenGroups;{0}",  
    param = c.Value);
```

16. En la página Edit Claim Rules (Editar reglas de reclamación), elija Add Rule (Agregar regla). En la página Select Rule Template (Seleccionar plantilla de regla), para Claim rule template (Plantilla de regla de reclamación), elija Send Claims Using a Custom Rule (Enviar reclamaciones utilizando una regla personalizada).
17. En la página Edit Rule – Roles (Editar regla – Roles), en Claim rule name (Nombre de regla de reclamación), escriba Roles.
18. En Custom rule (Regla personalizada), escriba lo siguiente.


```
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-"));
```

Tenga en cuenta los ARN del proveedor SAML y el rol que se van a asumir. En este ejemplo, `arn:aws:iam:123456789012:saml-provider/ADFS` es el ARN del proveedor SAML y `arn:aws:iam:123456789012:role/ADFS-` es el ARN del rol.

3. Asegúrese de haber descargado el archivo `federationmetadata.xml`. Compruebe que el contenido del documento no tenga caracteres no válidos. Este es el archivo de metadatos que utiliza al configurar la relación de confianza con AWS.
4. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Azure Enterprise Application. Para conocer los pasos en detalle, consulte [Creación y administración de un proveedor de identidades de IAM \(consola\)](#) en la Guía del usuario de IAM.
5. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de un rol para SAML](#) en la Guía del usuario de IAM.
6. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de políticas de IAM \(Consola\)](#) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD](#) (p. 340).

Para configurar JDBC para la autenticación en AD FS

- Configure el cliente de la base de datos para conectarse al clúster a través de JDBC mediante el inicio de sesión único de AD FS.

Puede usar cualquier cliente que utilice un controlador JDBC para conectarse mediante el inicio de sesión único de AD FS o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte [Configuración de una conexión de controlador JDBC versión 1.0](#) (p. 129).

Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

- a. Inicie SQL Workbench/J. En la **Select Connection Profile**, agregue una **Grupo de perfiles**, por ejemplo: **ADFS**.
- b. En **Connection Profile** (Perfil de conexión), escriba el nombre de perfil de su conexión, por ejemplo **ADFS**.
- c. Elija **Manage Drivers** (Administrar controladores), y elija Amazon Redshift. Elija el icono **Open folder** (Abrir carpeta) junto a **Library** (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.
- d. En la página **Select connection profile** (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:
 - En **User** (Usuario), escriba su nombre de usuario de AD FS. Este es el nombre de usuario de la cuenta de que está utilizando para el inicio de sesión único que tiene permisos en el clúster en el que está intentando autenticarse.
 - En **Password** (Contraseña), escriba su contraseña de AD FS.

- En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
 - En URL, escriba **`jdbc:redshift:iam//your-cluster-identifier:your-cluster-region/your-database-name`**.
- e. SeleccionarPropiedades ampliadas. En plugin_name, escriba **`com.amazon.redshift.plugin.AdfsCredentialsProvider`**. Este valor especifica que el controlador debe utilizar el inicio de sesión único de AD FS como método de autenticación.

Para configurar ODBC para la autenticación en AD FS

- Configure el cliente de base de datos para que se conecte al clúster a través de ODBC mediante el inicio de sesión único de AD FS.

Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y macOS X. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de más reciente de Amazon Redshift para su sistema operativo según se indica a continuación:

- Para Windows, vea [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows \(p. 139\)](#).
- Para macOS, consulte [Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X \(p. 143\)](#).
- Para Linux, vea [Instalación del controlador ODBC de Amazon Redshift en Linux \(p. 141\)](#).

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba **`your-DSN`**. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- ParaTipo de autenticación, elijaProveedor de identidades: SAML. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de AD FS.
- En Cluster ID (ID de clúster), escriba **`your-cluster-identifier`**.
- En Region (Región), escriba **`your-cluster-region`**.
- En Database (Base de datos), escriba **`your-database-name`**.
- En User (Usuario), escriba **`your-adfs-username`**. Este es el nombre de usuario de la cuenta de AD FS que está utilizando para el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Usa esto solo conTipo de autenticacionesProveedor de identidades: SAML.
- En Password (Contraseña), escriba **`your-adfs-password`**. Usa esto solo conTipo de autenticacionesProveedor de identidades: SAML.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

Note

Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba **`your-cluster-identifier`**. Este es el nombre del clúster de Amazon Redshift creado.

- En `region`, escriba **`your-cluster-region`**. Este es el AWS Región del clúster de Amazon Redshift creado.
- En `database`, escriba **`your-database-name`**. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En `locale`, escriba **`en-us`**. Este es el idioma en el que se muestran los mensajes de error.
- En `iam`, entra **`1`**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En `plugin_name`, realice una de las operaciones siguientes:
 - Para la configuración de inicio de sesión único de AD FS con MFA, escriba **`BrowserSAML`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar en AD FS.
 - Para la configuración de inicio de sesión único de AD FS, escriba **`ADFS`**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Azure AD.
- En `uid`, escriba **`your-adfs-username`**. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Utilice esto solo para `plugin_name` es ADFS.
- En `pwd`, escriba **`your-adfs-password`**. Utilice esto solo para `plugin_name` es ADFS.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Ping Identity

Puede utilizar Ping Identity como proveedor de identidades (IdP) para acceder a su clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin mediante el portal de PingOne. Para obtener más información sobre la configuración de AWS como proveedor de servicios para Ping Identity, consulte [Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el IdP de SAML 2.0](#) en la Guía del usuario de IAM.

Para configurar la identidad de Ping y la AWS cuenta para confiar el uno en el otro

1. Cree o use un clúster de Amazon Redshift existente para que los usuarios de Ping Identity se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte [Creating a Cluster \(Creación de un clúster\)](#).
2. Agregue Amazon Redshift como una nueva aplicación SAML en el portal de PingOne. Para obtener información detallada sobre los pasos, consulte la [documentación de Ping Identity](#).
 1. Vaya a My Applications (Mis aplicaciones).
 2. En Add Application (Agregar aplicación), elija New SAML Application (Nueva aplicación SAML).
 3. En Application name (Nombre de la application), escriba **`Amazon Redshift`**.
 4. En Protocol Version (Versión de protocolo), elija SAML v2.0.
 5. En Category (Categoría), elija **`your-application-category`**.
 6. En Assertion Consumer Service (ACS), escriba **`your-redshift-local-host-url`**. Éste es el host local y el puerto al que redirige la aserción SAML.

7. En Entity ID (ID de entidad), escriba `urn:amazon:webservices`.
8. En Signing (Firma), elija Sign Assertion (Aserción de firma).
9. En la sección SSO Attribute Mapping (Mapeo de atributos de SSO), cree las reclamaciones como se muestra en la tabla siguiente.

Atributo de aplicación	Atributo de puente de identidad de valor literal
<code>https://aws.amazon.com/SAML/Attributes/Role</code>	<code>arn:aws:iam::123456789012:role/Ping,arn:aws:iam::123456789012:saml-provider/PingProvider</code>
<code>https://aws.amazon.com/SAML/Attributes/RoleSessionName</code>	<code>email</code>
<code>https://redshift.amazon.com/SAML/Attributes/AutoCreate</code>	<code>"true"</code>
<code>https://redshift.amazon.com/SAML/Attributes/DbUser</code>	<code>email</code>
<code>https://redshift.amazon.com/SAML/Attributes/DbGroups</code>	Los grupos en los atributos «DBGroups» contienen el prefijo <code>@directory</code> . Para eliminar esto, en Puente de identidades, introduzca <code>memberOf</code> . En Función, elija <code>ExtractByRegexp</code> . En Expresión, introduzca <code>(.*) [\ @] (? : .*)</code> .

3. En Group Access (Acceso de grupo), configure el acceso de grupo siguiente en caso necesario:
 - `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. Revise la configuración y realice cambios, si es necesario.
5. Utilice la Initiate Single Sign-On (SSO) URL ((URL iniciar inicio de sesión único (SSO)) como URL de inicio de sesión para el complemento Browser SAML.
6. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Ping Identity. Para conocer los pasos en detalle, consulte [Creación y administración de un proveedor de identidades de IAM \(consola\)](#) en la Guía del usuario de IAM.
7. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de un rol para SAML](#) en la Guía del usuario de IAM.
8. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de políticas de IAM \(Consola\)](#) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD](#) (p. 340).

Para configurar JDBC para autenticación en Ping Identity

- Configure el cliente de base de datos para que se conecte al clúster a través de JDBC mediante el inicio de sesión único de Ping Identity.

Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Ping Identity o usar un lenguaje como Java para conectarse mediante un script. Para

obtener información sobre la instalación y configuración, consulte [Configuración de una conexión de controlador JDBC versión 1.0 \(p. 129\)](#).

Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

- a. Inicie SQL Workbench/J. En la Select Connection Profile, agregue una Grupo de perfiles, por ejemplo: **Ping**.
- b. En Connection Profile (Perfil de conexión), escriba ***your-connection-profile-name***, por ejemplo **Ping**.
- c. Elija Manage Drivers (Administrar controladores), y elija Amazon Redshift. Elija el icono Open folder (Abrir carpeta) junto a Library (Biblioteca) y a continuación, elija el archivo JDBC .jar adecuado.
- d. En la página Select connection profile (Seleccionar perfil de conexión) agregue información al perfil de conexión de la siguiente manera:
 - En User (Usuario), especifique el nombre de usuario de PingOne. Este es el nombre de usuario de la cuenta de PingOne que está utilizando con el inicio de sesión único que tiene permisos para el clúster en el que está intentando autenticarse.
 - En Password (Contraseña), escriba la contraseña de PingOne.
 - En Drivers (Controladores), elija Amazon Redshift (com.amazon.redshift.jdbc.Driver).
 - En URL, escriba ***jdbc:redshift:iam://your-cluster-identifier:your-cluster-region/your-database-name***.
- e. Elija Extended Properties (Propiedades extendidas) y realice una de las acciones siguientes:
 - En login_url, escriba ***your-ping-sso-login-url***. Este valor especifica la dirección URL que va a utilizar el inicio de sesión único como autenticación al iniciar sesión.
 - Para Ping Identity, en nombre_complemento, escriba **com.amazon.redshift.plugin.PingCredentialsProvider**. Este valor especifica que el controlador utilice el inicio de sesión único de Ping Identity como método de autenticación.
 - Para el inicio de sesión único en Ping Identity, en nombre_complemento, escriba **com.amazon.redshift.plugin.BrowserSamlCredentialsProvider**. Este valor especifica al controlador que utilice el inicio de sesión único de PingOne para Ping Identity como método de autenticación.

Para configurar ODBC para la autenticación en Ping Identity

- Configure el cliente de la base de datos para que se conecte al clúster a través de ODBC utilizando el inicio de sesión único de PingOne para Ping Identity.

Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y macOS X. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de más reciente de Amazon Redshift para su sistema operativo según se indica a continuación:

- Para Windows, vea [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows \(p. 139\)](#).

- Para macOS, consulte [Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X \(p. 143\)](#).
- Para Linux, vea [Instalación del controlador ODBC de Amazon Redshift en Linux \(p. 141\)](#).

En Windows, en la página Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift) en Connection Settings (Configuración de conexión), escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba **your-dsn**. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth Type (Tipo de autenticación), realice una de las operaciones siguientes:
 - En la configuración de Ping Identity, elija Proveedor de identidades: Ping Federate. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante inicio de sesión único Ping Identity.
 - Para la configuración de inicio de sesión único con Ping Identity, elija Proveedor de identidades: SAML del navegador. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante inicio de sesión único Ping Identity.
- En Cluster ID (ID de clúster), escriba **your-cluster-identifier**.
- En Region (Región), escriba **your-cluster-region**.
- En Database (Base de datos), escriba **your-database-name**.
- En User (Usuario), escriba **your-ping-username**. Este es el nombre de usuario de la cuenta de PingOne que está utilizando con el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Usa esto solo con Tipo de autenticaciones Proveedor de identidades: PingFederate.
- En Password (Contraseña), escriba **your-ping-password**. Usa esto solo con Tipo de autenticaciones Proveedor de identidades: PingFederate.
- En Puerto de escucha, escriba **your-listen-port**. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.
- En Response Timeout (Tiempo de espera de respuesta), escriba **the-number-of-seconds**. Este es el número de segundos que se deben esperar antes de que el servidor IdP devuelva una respuesta. El número mínimo de segundos debe ser 10. Si establecer la conexión toma más que este umbral de tiempo, se anula la conexión. Esto solo se aplica al complemento SAML del navegador.
- En Login URL (URL de inicio de sesión), escriba **your-login-url**. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

Note

Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba **your-cluster-identifier**. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba **your-cluster-region**. Este es el AWS Región del clúster creado por Amazon Redshift.
- En database, escriba **your-database-name**. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **en-us**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **1**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.

- En `plugin_name`, realice una de las operaciones siguientes:
 - Para la configuración de Ping Identity, escriba **BrowserSAML**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar con Ping Identity.
 - Para la configuración de inicio de sesión único con Ping Identity, escriba **ping**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante inicio de sesión único Ping Identity.
- En `uid`, escriba **your-ping-username**. Este es el nombre de usuario de la cuenta de Microsoft Azure que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Usa esto solo con `plugin_name=ping`.
- En `pwd`, escriba **your-ping-password**. Usa esto solo con `plugin_name=ping`.
- En `login_url`, escriba **your-login-url**. Esta es la URL de inicio de sesión único que devuelve la respuesta SAML. Esto solo se aplica al complemento SAML del navegador.
- En `idp_response_timeout`, escriba **the-number-of-seconds**. Este es el período de tiempo especificado en segundos que se va a esperar a que PingOne Identity responda. Esto solo se aplica al complemento SAML del navegador.
- En `listen_port`, escriba **your-listen-port**. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Configuración de la autenticación de inicio de sesión único de JDBC u ODBC con Okta

Puede utilizar Okta como proveedor de identidades (IdP) para acceder a su clúster de Amazon Redshift. A continuación, puede encontrar un procedimiento que describa cómo configurar una relación de confianza para este fin. Para obtener más información sobre la configuración de AWS como proveedor de servicios para Okta, consulte [Configuración de una relación de confianza para usuario autenticado y agregación de notificaciones en el IdP de SAML 2.0](#) en la Guía del usuario de IAM.

Para configurar Okta y su AWS cuenta para confiar el uno en el otro

1. Cree o use un clúster de Amazon Redshift de existente para que los usuarios de Okta se conecten a él. Para configurar la conexión, se necesitan ciertas propiedades de este clúster, como el identificador del clúster. Para obtener más información, consulte [Creating a Cluster \(Creación de un clúster\)](#).
2. Agregue Amazon Redshift como una nueva aplicación en el portal Okta. Para ver los pasos detallados, consulte la [documentación de Okta](#).
 - Elija Add Application (Agregar aplicación).
 - En Add Application (Agregar aplicación), elija Create New App (Crear nueva aplicación).
 - En la página Create a New Add Application Integration (Crear una nueva integración Agregar aplicación), en Platform (Plataforma), elija Web.
 - En Sign on method (Método de inicio de sesión), elija SAML v2.0.
 - En la página General Settings (Configuración general), en App name (Nombre de la aplicación), escriba **your-redshift-saml-sso-name**. Se trata del nombre de la aplicación.
 - En la página Configuración de SAML, en URL de inicio de sesión único, escriba **your-redshift-local-host-url**. Este es el host local y el puerto al que redirige la aserción SAML, por ejemplo `http://localhost:7890/redshift/`.

3. UsarURL de inicio de sesión únicoValor comoURL del destinatarioyDirección URL de destino.
4. En Signing (Firma), elija Sign Assertion (Aserción de firma).
5. ParaID de entidad SP Entity ID), introduzca**urn:amazon:webservices**para las reclamaciones, como se muestra en el cuadro siguiente.
6. En el navegadorConfiguración avanzadasección deID de emisor SAML, introduzca**your-Identity-Provider-Issuer-ID**Encontrará en laVer instrucciones de configuraciónsección de.
7. En la sección Attribute Statements (Declaraciones de atributos), cree las reclamaciones como se muestra en la tabla siguiente.

Nombre de la reclamación	Valor
https://aws.amazon.com/SAML/Attributes/Role	arn:aws:iam:: 123456789012 :role/ Okta ,arn:aws:iam:: 123456789012 :saml-provider/ Okta
https://aws.amazon.com/SAML/Attributes/RoleSessionName	user.email
https://redshift.amazon.com/SAML/Attributes/AutoCreate	"true"
https://redshift.amazon.com/SAML/Attributes/DbUser	user.email

8. En la sección App Embed Link (Enlace de inserción de aplicaciones), busque la URL que quiere usar como URL de inicio de sesión con el complemento Browser SAML.
9. Cree un proveedor de identidad SAML de IAM en la consola de IAM. El documento de metadatos que proporciona es el archivo XML de metadatos de federación que guardó al configurar Okta. Para conocer los pasos en detalle, consulte [Creación y administración de un proveedor de identidades de IAM \(consola\)](#) en la Guía del usuario de IAM.
10. Cree un rol de IAM para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de un rol para SAML](#) en la Guía del usuario de IAM.
11. Cree una directiva de IAM que pueda adjuntar al rol de IAM creado para la federación de SAML 2.0 en la consola de IAM. Para conocer los pasos en detalle, consulte [Creación de políticas de IAM \(Consola\)](#) en la Guía del usuario de IAM. Para ver un ejemplo de Azure AD, consulte [Configuración de la autenticación de inicio de sesión único JDBC u ODBC con Microsoft Azure AD](#) (p. 340).

Para configurar JDBC para la autenticación en Okta

- Configure su cliente de base de datos para conectarse a su clúster a través de JDBC mediante el inicio de sesión único de Okta.

Puede usar cualquier cliente que use un controlador JDBC para conectarse mediante el inicio de sesión único de Okta o usar un lenguaje como Java para conectarse mediante un script. Para obtener información sobre la instalación y configuración, consulte [Configuración de una conexión de controlador JDBC versión 1.0](#) (p. 129).

Por ejemplo, puede usar SQLWorkBench/J como cliente. Al configurar SQLWorkbench/J, la dirección URL de la base de datos utiliza el siguiente formato.

```
jdbc:redshift:iam://cluster-identifier:us-west-1/dev
```

Si utiliza SQLWorkbench/J como cliente, siga los siguientes pasos:

- a. Inicie SQL Workbench/J. En la **Select Connection Profile**, agregue una **Grupo de perfiles**, por ejemplo: **Okta**.
- b. En **Connection Profile (Perfil de conexión)**, escriba ***your-connection-profile-name***, por ejemplo **Okta**.
- c. Elija **Manage Drivers (Administrar controladores)**, y elija **Amazon Redshift**. Elija el icono **Open folder (Abrir carpeta)** junto a **Library (Biblioteca)** y a continuación, elija el archivo **JDBC .jar** adecuado.
- d. En la página **Select connection profile (Seleccionar perfil de conexión)** agregue información al perfil de conexión de la siguiente manera:
 - Para **User (Usuario)**, escriba su nombre de usuario de Okta. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse.
 - En **Password (Contraseña)**, escriba su contraseña de Okta.
 - En **Drivers (Controladores)**, elija **Amazon Redshift (com.amazon.redshift.jdbc.Driver)**.
 - En **URL**, escriba **`jdbc:redshift:iam//your-cluster-identifier:your-cluster-region/your-database-name`**.
- e. Elija **Extended Properties (Propiedades extendidas)** y realice una de las acciones siguientes:
 - En **login_url**, escriba ***your-okta-sso-login-url***. Este valor especifica la dirección URL para utilizar el inicio de sesión único como autenticación para iniciar sesión en Okta.
 - Para el inicio de sesión único en Okta, en **plugin_name**, escriba **`com.amazon.redshift.plugin.OktaCredentialsProvider`**. Este valor especifica que el controlador utilice el inicio de sesión único de Okta como método de autenticación.
 - Para el inicio de sesión único de Okta con MFA, en **nombre_complemento**, escriba **`com.amazon.redshift.plugin.BrowserSamlCredentialsProvider`**. Este valor especifica que el controlador utilice el inicio de sesión único de Okta con MFA como método de autenticación.

Para configurar ODBC para la autenticación en Okta

- Configure el cliente de base de datos para que se conecte a su clúster a través de ODBC mediante el inicio de sesión único de Okta.

Amazon Redshift proporciona controladores ODBC para los sistemas operativos Linux, Windows y macOS X. Antes de instalar un controlador ODBC, determine si su herramienta del cliente SQL es de 32 bits o 64 bits. Instale el controlador ODBC que coincida con los requisitos de la herramienta cliente SQL.

También instale y configure el controlador ODBC de más reciente de Amazon Redshift para su sistema operativo según se indica a continuación:

- Para Windows, vea [Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows \(p. 139\)](#).
- Para macOS, consulte [Instalación del controlador ODBC de Amazon Redshift de Amazon Redshift en macOS X \(p. 143\)](#).
- Para Linux, vea [Instalación del controlador ODBC de Amazon Redshift en Linux \(p. 141\)](#).

En Windows, en la página **Amazon Redshift ODBC Driver DSN Setup (Configuración del DSN del controlador ODBC de Amazon Redshift)** en **Connection Settings (Configuración de conexión)**, escriba la siguiente información:

- En Data Source Name (Nombre de origen de datos), escriba **your-DSN**. Especifica el nombre del origen de datos utilizado como nombre del perfil de ODBC.
- En Auth Type (Tipo de autenticación), realice una de las operaciones siguientes:
 - Para la configuración de inicio de sesión único de Okta, elija **Identity Provider: Okta**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Okta.
 - Para la configuración del inicio de sesión único de Okta con MFA, elija **Identity Provider: Browser SAML**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar usando el inicio de sesión único de Okta con MFA.
- En Cluster ID (ID de clúster), escriba **your-cluster-identifier**.
- En Region (Región), escriba **your-cluster-region**.
- En Database (Base de datos), escriba **your-database-name**.
- En User (Usuario), escriba **your-okta-username**. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único que tiene permiso para el clúster con el que está intentando autenticarse. Usa esto solo con Tipo de autenticación Proveedor de identidades: Okta.
- En Password (Contraseña), escriba **your-okta-password**. Usa esto solo con Tipo de autenticación Proveedor de identidades: Okta.

En Mac OS y Linux, edite el archivo `odbc.ini` de la siguiente manera:

Note

Ninguna de las entradas distingue entre mayúsculas y minúsculas.

- En clusterid, escriba **your-cluster-identifier**. Este es el nombre del clúster de Amazon Redshift creado.
- En region, escriba **your-cluster-region**. Este es el AWS Región del clúster creado por Amazon Redshift.
- En database, escriba **your-database-name**. Este es el nombre de la base de datos a la que intenta tener acceso en el clúster de Amazon Redshift.
- En locale, escriba **en-us**. Este es el idioma en el que se muestran los mensajes de error.
- En iam, entra **1**. Este valor especifica que el controlador debe autenticarse mediante credenciales de IAM.
- En plugin_name, realice una de las operaciones siguientes:
 - Para la configuración de inicio de sesión único de Okta con MFA, escriba **BrowserSAML**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar el inicio de sesión único de Okta con MFA.
 - Para la configuración del inicio de sesión único de Okta, escriba **Okta**. Este es el método de autenticación que utiliza el controlador ODBC para autenticar mediante el inicio de sesión único de Okta.
- En uid, escriba **your-okta-username**. Este es el nombre de usuario de la cuenta de Okta que está utilizando para el inicio de sesión único, que tiene permisos en el clúster en el que está intentando autenticarse. Use esto solo para plugin_name es Okta.
- En pwd, escriba **your-okta-password**. Use esto solo para plugin_name es Okta.
- En login_url, escriba **your-login-url**. Esta es la URL de inicio de sesión único que devuelve la respuesta SAML. Esto solo se aplica al complemento SAML del navegador.
- En idp_response_timeout, escriba **the-number-of-seconds**. Este es el período de tiempo especificado en segundos que se va a esperar a que PingOne responda. Esto solo se aplica al complemento SAML del navegador.

- En `listen_port`, escriba **your-listen-port**. Este es el puerto en el que escucha el servidor local. El valor predeterminado es 7890. Esto solo se aplica al complemento SAML del navegador.

En Mac OS y Linux, edite también la configuración del perfil para agregar las siguientes exportaciones:

```
export ODBCINI=/opt/amazon/redshift/Setup/odbc.ini
```

```
export ODBCINSTINI=/opt/amazon/redshift/Setup/odbcinst.ini
```

Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos

Para utilizar el controlador JDBC u ODBC de Amazon Redshift para crear credenciales de usuario de base de datos, proporcione el nombre de usuario de base de datos como una opción JDBC u ODBC. Si lo desea, puede hacer que el controlador cree un nuevo usuario de base de datos si no existe ninguno y puede especificar una lista de grupos de usuarios de base de datos a los que se une el usuario cuando inicia sesión.

Si usa un proveedor de identidad (IdP), póngase en contacto con el administrador de su IdP para determinar los valores correctos para estas opciones. El administrador de su IdP también puede configurar su IdP para proporcionar estas opciones, en cuyo caso no necesita proporcionarlas como opciones de JDBC u ODBC. Para obtener más información, consulte [Configuración de aserciones SAML para el IdP \(p. 326\)](#).

Note

Si utiliza una variable de política de IAM `${redshift:DbUser}`, como se describe en [Políticas de recursos de GetClusterCredentials \(p. 315\)](#), el valor de `DbUser` se sustituye por el valor obtenido por el contexto de la solicitud de la operación de la API. Los controladores de Amazon Redshift utilizan el valor de la propiedad `DbUser` proporcionado por la URL de conexión en lugar del valor proporcionado como atributo SAML.

Para ayudar a proteger esta configuración, recomendamos que utilice una condición en una política de IAM para validar el valor de `DbUser` con el `RoleSessionName`. Puede encontrar ejemplos de cómo establecer una condición utilizando una política de IAM en [Política de ejemplo para usar GetClusterCredentials \(p. 321\)](#).

En la tabla siguiente se indican las opciones para crear credenciales de usuario de base de datos.

Opción	Descripción
DbUser	El nombre de un usuario de base de datos. Si un usuario llamado DbUser existe en la base de datos, las credenciales temporales del usuario tienen los mismos permisos que el usuario existente. Si DbUser no existe en la base de datos y AutoCreate está establecido en true, se crea un nuevo usuario llamado DbUser. Si lo desea, deshabilite la contraseña de un usuario existente. Para obtener más información, consulte ALTER_USER .
AutoCreate	Establezca esta opción en true para crear un usuario de base de datos con el nombre especificado para DbUser si no existe ninguno. El valor predeterminado es false.
DbGroups	Una lista delimitada por comas de los nombres de uno o varios grupos de usuarios de base de datos a los que se une el usuario de base de datos durante la sesión actual. De forma predeterminada, el nuevo usuario se añade solamente a PUBLIC.

Generación de credenciales de base de datos de IAM mediante la CLI o la API de Amazon Redshift

Para generar credenciales temporales de usuario de base de datos, Amazon Redshift proporciona el `get-cluster-credentials` Comando de la AWS Command Line Interface (AWS CLI) y el `GetClusterCredentials` Operación API de. También puede configurar su cliente SQL con controladores JDBC u ODBC de Amazon Redshift que administren el proceso de llamar al método `GetClusterCredentials` Para obtener las credenciales de usuario de base de datos y establecer una conexión entre su cliente SQL y la base de datos de Amazon Redshift. Para obtener más información, consulte [Opciones de JDBC y ODBC para crear credenciales de usuario de base de datos](#) (p. 360) .

Note

Le recomendamos que utilice los controladores JDBC u ODBC de Amazon Redshift para generar credenciales de usuario de base de datos.

En esta sección, encontrará los pasos para llamar mediante programación a la operación `GetClusterCredentials` o el comando `get-cluster-credentials`, recuperar las credenciales de usuario de base de datos y conectarse a la base de datos.

Para generar y usar credenciales temporales de base de datos

1. Cree o modifique un usuario o rol de IAM con los permisos necesarios. Para obtener más información sobre los permisos de IAM, consulte [Crear un rol o usuario de IAM con permisos para llamar a `GetClusterCredentials`](#) (p. 327).
2. Como usuario o rol de IAM con los permisos concedidos en el paso anterior, ejecute el comando `get-cluster-credentials` de la CLI o llame a la operación de la API `GetClusterCredentials` y proporcione los siguientes valores:
 - Identificador de clúster: nombre del clúster que contiene la base de datos.
 - Nombre de usuario de la base de datos: nombre de un usuario de base de datos nuevo o existente.
 - Si el usuario no existe en la base de datos y `AutoCreate` está establecido en `true`, se crea un nuevo usuario con la contraseña deshabilitada.
 - Si el usuario no existe y `AutoCreate` está establecido en `false`, la solicitud produce un error.
 - En este ejemplo, el nombre de usuario de base de datos es `temp_creds_user`.
 - `Autocreate`— (Opcional) Cree un nuevo usuario si el nombre de usuario de base de datos no existe.
 - Nombre de base de datos— (opcional) nombre de la base de datos en la que el usuario tiene permiso para iniciar sesión. Si no se especifica el nombre de la base de datos, el usuario puede iniciar sesión en cualquier base de datos del clúster.
 - Grupos de datos— (Opcional) lista de grupos de usuarios de bases de datos existentes. Tras iniciar sesión correctamente, el usuario de base de datos se agrega a los grupos de usuarios especificados. Si no se especifica ningún grupo, el usuario sólo tiene permisos `PUBLIC`. Los nombres de los grupos de usuarios deben coincidir con los ARN de recursos `dbgroup` especificados en la directiva de IAM asociada al usuario o rol de IAM.
 - Tiempo de caducidad— (opcional) fecha de caducidad, en segundos, de las credenciales temporales. Puede especificar un valor comprendido entre 900 segundos (15 minutos) y 3 600 segundos (60 minutos). El valor predeterminado es de 900 segundos.
3. Amazon Redshift verifica que el usuario de IAM tiene permiso para llamar al método `GetClusterCredentials` con los recursos especificados.
4. Amazon Redshift devuelve una contraseña temporal y el nombre de usuario de la base de datos.

En el siguiente ejemplo se utiliza la CLI de Amazon Redshift para generar credenciales temporales de base de datos para un usuario existente denominado `temp_creds_user`.

```
aws redshift get-cluster-credentials --cluster-identifier examplecluster --db-user  
temp_creds_user --db-name exampledb --duration-seconds 3600
```

El resultado es el siguiente.

```
{  
  "DbUser": "IAM:temp_creds_user",  
  "Expiration": "2016-12-08T21:12:53Z",  
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpdHwXVPyJYBDm/  
gqX2Eeq6P3DgTzgPg=="  
}
```

En el siguiente ejemplo se utiliza la CLI de Amazon Redshift con creación automática para generar credenciales temporales de base de datos para un nuevo usuario y agregar el usuario al grupo `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
```

El resultado es el siguiente.

```
{  
  "DbUser": "IAMA:temp_creds_user:example_group",  
  "Expiration": "2016-12-08T21:12:53Z",  
  "DbPassword": "EXAMPLEjArE3hcnQj8zt4XQj9Xtma8oxYEM8OyxpdHwXVPyJYBDm/  
gqX2Eeq6P3DgTzgPg=="  
}
```

5. Establezca una conexión de autenticación SSL (Secure Socket Layer) con el clúster de Amazon Redshift y envíe una solicitud de inicio de sesión con el nombre de usuario y la contraseña del `GetClusterCredentials`La respuesta de. Incluya el prefijo `IAM:` o `IAMA:` con el nombre de usuario, por ejemplo `IAM:temp_creds_user` o `IAMA:temp_creds_user`.

Important

Configure el cliente SQL para que requiera SSL. En caso contrario, si el cliente SQL intenta conectarse automáticamente con SSL, puede cambiar a una conexión distinta de SSL en caso de que se produzca algún error. En tal caso, el primer intento de conexión podría producir un error porque las credenciales han caducado o no son válidas, y el segundo intento de conexión podría producir un error porque la conexión no es SSL. Si eso ocurre, el primer mensaje de error podría pasarse por alto. Para obtener más información acerca de la conexión al clúster mediante SSL, consulte [Configuración de las opciones de seguridad para las conexiones](#) (p. 151).

6. Si la conexión no usa SSL, el intento de conexión produce un error.
7. El clúster envía una solicitud `authentication` al cliente SQL.
8. El cliente SQL envía entonces la contraseña temporal al clúster.
9. Si la contraseña es válida y no ha caducado, el clúster realiza la conexión.

Autorizar a Amazon Redshift a obtener acceso a otrosAWSservices de en su nombre

Algunas funciones de Amazon Redshift requieren que Amazon Redshift acceda a otros usuarios deAWS en su nombre. Por ejemplo, el [COPY](#) y [DESCARGAR](#) Los comandos de pueden cargar o descargar datos en el clúster de Amazon Redshift mediante un bucket de Amazon S3. La [CREACIÓN DE FUNCIÓN EXTERNA](#) puede invocar un comandoAWS Función Lambda mediante una función escalar Lambda definida por el usuario (UDF). Amazon Redshift Spectrum puede utilizar un catálogo de datos en Amazon Athena o enAWS Glue. Para que los clústeres de Amazon Redshift actúen en su nombre, debe suministrarles credenciales de seguridad. El método preferido para proporcionar credenciales de seguridad consiste en especificar unAWS Identity and Access Management(IAM). Para COPY y UNLOAD, puede proporcionarAWS Claves de acceso.

A continuación, obtenga información sobre cómo crear un rol de IAM con los permisos adecuados para tener acceso a otrosAWSservices de . También necesitará asociar el rol al clúster y especificar el nombre de recurso de Amazon (ARN) del rol cuando ejecute el comando Amazon Redshift. Para obtener más información, consulte [Autorización de uso de las operaciones COPY, UNLOAD, CREATE EXTERNAL SCHEMA mediante roles de IAM \(p. 368\)](#) .

Además, un superusuario puede conceder el privilegio ASSUMEROLE a usuarios y grupos específicos para proporcionar acceso a un rol para las operaciones COPY y UNLOAD. Para obtener información, consulte [CONCESIÓN](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Creación de un rol de IAM para permitir a su clúster de Amazon Redshift acceder aAWSservices

Para crear un rol de IAM que permita al clúster de Amazon Redshift comunicarse con otrosAWS en su nombre, siga estos pasos. Los valores utilizados en esta sección son ejemplos, puede elegir valores en función de sus necesidades.

Para crear un rol de IAM que permita a Amazon Redshift acceder aAWSservices

1. Abra la [consola de IAM](#).
2. Seleccione Roles en el panel de navegación.
3. Elija Create role.
4. SeleccioneAWSservice y luego elijaRedshift.
5. **UNDER**Select your use case, elijaPersonalizableHaga clic en y luego enSiguiente: Permisos. Aparece la página Attach permissions policy (Asociar política de permisos).
6. Por ejemplo, para obtener acceso a Amazon S3 mediante COPY, puede utilizar**AmazonS3ReadOnlyAccess** y anexar. Para acceder a Amazon S3 mediante COPY o UNLOAD, le sugerimos que cree políticas gestionadas que restrinjan el acceso al bucket y prefijo deseados en consecuencia. Para las operaciones de lectura y escritura, recomendamos aplicar los privilegios mínimos y restringir únicamente a los buckets y prefijos clave de Amazon S3 que Amazon Redshift requiere.

Para acceder a invocar funciones de Lambda para el comando CREATE EXTERNAL FUNCTION, agregue**AWSLambdaRole**.

Para Redshift Spectrum, además del acceso a Amazon S3, añada**AWSGlueConsoleFullAccess** o**AmazonAthenaFullAccess**.

Seleccione Next (Siguiente): Tags (Etiquetas).

7. Aparece la página Add tags (Añadir etiquetas). Si lo desea, puede añadir etiquetas. Seleccione Next (Siguiente): Consulte.

8. En Role Name (Nombre de la función), escriba un nombre para la función; por ejemplo, **RedshiftCopyUnload**. Elija Create role.
9. El nuevo rol está disponible para todos los usuarios en clústeres que utilizan el rol. Para restringir el acceso solo para usuarios específicos o para clústeres en regiones específicas, edite la relación de confianza del rol. Para obtener más información, consulte [Restricción de acceso a los roles de IAM \(p. 364\)](#).
10. Asocie el rol al clúster. Puede asociar un rol de IAM a un clúster cuando crea el clúster o añade el rol a un clúster existente. Para obtener más información, consulte [Asociación de roles de IAM a los clústeres \(p. 369\)](#).

Note

Para restringir el acceso a datos específicos, utilice un rol de IAM que otorgue los privilegios mínimos necesarios.

Restricción de acceso a los roles de IAM

De forma predeterminada, los roles de IAM que están disponibles en un clúster de Amazon Redshift están disponibles para todos los usuarios de ese clúster. Puede optar por restringir los roles de IAM para usuarios específicos de la base de datos de Amazon Redshift en clústeres o regiones específicas.

Para permitir la utilización de un rol de IAM solo a usuarios específicos de la base de datos, siga estos pasos.

Para identificar a los usuarios específicos de la base de datos con acceso a un rol de IAM

1. Identifique el nombre de recurso de Amazon (ARN) de los usuarios de bases de datos en el clúster de Amazon Redshift. El ARN de un usuario de la base de datos está en el formato: `arn:aws:redshift:region:account-id:dbuser:cluster-name/user-name`.
2. Abra el icono [Consola de IAM](https://console.aws.amazon.com/) la url=» <https://console.aws.amazon.com/>.
3. Seleccione Roles en el panel de navegación.
4. Seleccione el rol de IAM que desea restringir para usuarios específicos de bases de datos de Amazon Redshift.
5. Seleccione la pestaña Trust Relationships (Relaciones de confianza) y Edit Trust Relationship (Editar relación de confianza). Un nuevo rol de IAM que permite a Amazon Redshift obtener acceso a otrosAWSLos servicios en su nombre tienen la siguiente relación de confianza:

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

6. Añada una condición a la sección de acción `sts:AssumeRole` de la relación de confianza que limita el campo `sts:ExternalId` a los valores que usted especifique. Incluya un ARN para cada usuario de la base de datos al que desea concederle acceso al rol. El ID externo puede ser cualquier cadena única.

Por ejemplo, la siguiente relación de confianza especifica que solo los usuarios de la base de datos `user1` y `user2` en el clúster `my-cluster` en la región `us-west-2` tienen permiso para utilizar este rol de 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. Elija Update Trust Policy.

Restricción de un rol de IAM a unAWSRegión

Puede restringir un rol de IAM para que sea accesible solo en un determinadoAWSRegión . De forma predeterminada, los roles de IAM para Amazon Redshift no se restringen a ninguna región.

Para restringir la utilización de un rol de IAM por región, siga estos pasos.

Para identificar las regiones permitidas para un rol de IAM

1. Abra el icono [Consola de IAM](https://console.aws.amazon.com/) a las <https://console.aws.amazon.com/>.
2. Seleccione Roles en el panel de navegación.
3. Seleccione el rol que desea modificar con regiones específicas.
4. Seleccione la pestaña Trust Relationships (Relaciones de confianza) y Edit Trust Relationship (Editar relación de confianza). Un nuevo rol de IAM que permite a Amazon Redshift obtener acceso a otrosAWSLos servicios en su nombre tienen la siguiente relación de confianza:

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

5. Modifique la lista `Service` para el `Principal` con la lista de las regiones específicas a las que desea permitir la utilización del rol. Cada región de la lista `Service` debe indicarse con el formato siguiente: `redshift.region.amazonaws.com`.

Por ejemplo, la siguiente relación de confianza editada permite la utilización del rol de IAM solo en las regiones `us-east-1` y `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. Seleccione Update Trust Policy (Actualizar política de confianza)

Encadenamiento de roles de IAM en Amazon Redshift

Cuando asocia un rol a un clúster, el clúster puede adoptar dicho rol para acceder a Amazon S3, Amazon Athena, AWS Glue, y AWS Lambda en su nombre. Si un rol que está asociado al clúster no tiene acceso a los recursos necesarios, puede encadenar otro rol, que posiblemente pertenezca a otra cuenta. El clúster asumirá de forma temporal el rol encadenado para obtener acceso a los datos. También puede conceder acceso entre cuentas mediante el encadenamiento de roles. Cada uno de los roles de la cadena asume el rol siguiente, hasta que el clúster asume el rol situado al final de la cadena. Puede encadenar un máximo de 10 roles.

Por ejemplo, supongamos que la empresa A desea obtener acceso a los datos de un bucket de Amazon S3 que pertenece a la empresa B. La empresa A crea un rol de servicio de Amazon Redshift llamado `RoleA` y lo adjunta a su clúster. La empresa B crea un rol denominado `RoleB` que está autorizado para obtener acceso a los datos del bucket de la empresa B. Para obtener acceso a los datos del bucket de la empresa B, la empresa A ejecuta un comando COPY utilizando un parámetro `iam_role` que encadena `RoleA` y `RoleB`. Durante la operación COPY, `RoleA` asume temporalmente `RoleB` para acceder al bucket de Amazon S3.

Para encadenar roles, debe establecer una relación de confianza entre ellos. Un rol que asume otro rol (por ejemplo, `RoleA`) debe tener una política de permisos que le permita asumir el rol encadenado siguiente (por ejemplo, `RoleB`). A su vez, el rol que transfiere los permisos (`RoleB`) debe tener una política de confianza que le permita transferir sus permisos al rol encadenado anterior (`RoleA`). Para obtener más información, consulte [Uso de roles de IAM](#) en la guía del usuario de IAM.

El primer rol de la cadena debe ser un rol asociado al clúster. El primer rol y cada uno de los roles posteriores que asuma el rol siguiente en la cadena deben tener una política que incluya una instrucción específica. Esta instrucción tiene el efecto `Allow` en la acción `sts:AssumeRole` y el nombre de recurso de Amazon (ARN) del rol siguiente en un elemento `Resource`. En nuestro ejemplo, `RoleA` tiene la siguiente política de permisos que le permite asumir `RoleB`, propiedad de `AWSaccount210987654321`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1487639602000",
      "Effect": "Allow",
      "Action": [
        "sts:AssumeRole"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "arn:aws:iam::210987654321:role/RoleB"  
  }  
]  
}
```

Un rol que se transfiere a otro rol debe establecer una relación de confianza con el rol que lo asume o con el rol de AWS que posee el rol. En nuestro ejemplo, RoleB tiene la siguiente política de confianza para establecer una relación de confianza con RoleA.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Principal": {  
        "AWS": "arn:aws:iam::role/RoleA"  
      }  
    }  
  ]  
}
```

La siguiente política de confianza establece una relación de confianza con el propietario de RoleA, AWSaccount123456789012.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "sts:AssumeRole",  
      "Principal": {  
        "AWS": "arn:aws:iam::123456789012:root"  
      }  
    }  
  ]  
}
```

Note

Para restringir la autorización de encadenamiento de roles a usuarios específicos, defina una condición. Para obtener más información, consulte [Restricción de acceso a los roles de IAM \(p. 364\)](#).

Cuando ejecute un comando UNLOAD, COPY, CREATE EXTERNAL FUNCTION o CREATE EXTERNAL SCHEMA para encadenar roles incluyendo una lista de ARN de rol separada por comas en el cuadro de diálogo iam_role Parámetro. A continuación se muestra la sintaxis para encadenar roles en el parámetro 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

La cadena de roles debe estar encerrada entre comillas simples y no puede contener espacios.

En los ejemplos siguientes, RoleA se adjunta al clúster que pertenece aAWSaccount123456789012. RoleB, que pertenece a la cuenta210987654321 Tiene permiso para

acceder al bucket llamados `s3://companyb/redshift/`. En el siguiente ejemplo se encadenan `RoleA` y `RoleB` para DESCARGAR datos en el 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';
```

En el siguiente ejemplo se utiliza un comando `COPY` para cargar los datos que se descargaron en el ejemplo anterior.

```
copy venue
from 's3://companyb/redshift/venue_pipe_'
iam_role 'arn:aws:iam::123456789012:role/RoleA,arn:aws:iam::210987654321:role/RoleB';
```

En el siguiente ejemplo, `CREATE EXTERNAL SCHEMA` utiliza roles encadenados para asumir el rol `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';
```

En el siguiente ejemplo, `CREATE EXTERNAL FUNCTION` utiliza roles encadenados para asumir el rol `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';
```

Temas relacionados

- [Autorización de uso de las operaciones COPY, UNLOAD, CREATE EXTERNAL SCHEMA mediante roles de IAM \(p. 368\)](#)

Autorización de uso de las operaciones COPY, UNLOAD, CREATE EXTERNAL SCHEMA mediante roles de IAM

Puede utilizar la [COPY](#) para cargar (o importar) datos en Amazon Redshift y [DESCARGAR](#) para descargar (o exportar) datos de Amazon Redshift. Puede utilizar el comando `CREATE EXTERNAL FUNCTION` para crear funciones definidas por el usuario que invoquen funciones desde [AWS Lambda](#).

Cuando se utiliza Amazon Redshift Spectrum, se utiliza la función [CREACIÓN DE ESQUEMAS EXTERNOS](#) para especificar la ubicación de un bucket de Amazon S3 que contenga sus datos. Cuando ejecuta los comandos `COPY`, `UNLOAD` o `CREATE EXTERNAL SCHEMA`, proporciona credenciales de seguridad. Estas credenciales autorizan a su clúster de Amazon Redshift a leer o escribir datos en o desde su lugar de destino, como un bucket de Amazon S3.

Cuando ejecuta la función `CREATE EXTERNAL`, proporciona credenciales de seguridad mediante el parámetro de rol de IAM. Estas credenciales autorizan a su clúster de Amazon Redshift a invocar funciones de [Lambda](#) desde [AWS Lambda](#). El método preferido para proporcionar credenciales de seguridad consiste en especificar un [AWS Identity and Access Management \(IAM\)](#). Para `COPY` y `UNLOAD`, puede proporcionar [AWS Claves de acceso](#). Para obtener información sobre la creación de un rol de IAM, consulte [Autorizar a Amazon Redshift a obtener acceso a otros AWS Servicios de en su nombre \(p. 363\)](#).

Los pasos para utilizar un rol de IAM son los siguientes:

- Cree un rol de IAM para usar con el clúster de Amazon Redshift.
- Asocie el rol de IAM al clúster.
- Incluya el ARN del rol de IAM cuando llame al comando COPY, UNLOAD, CREATE EXTERNAL SCHEMA o CREATE EXTERNAL FUNCTION.

En este tema, aprenderá a asociar un rol de IAM a un clúster de Amazon Redshift.

Asociación de roles de IAM a los clústeres

Una vez que haya creado un rol de IAM que autorice a Amazon Redshift a obtener acceso a otros AWS services, debe asociar ese rol con un clúster de Amazon Redshift. Debe hacerlo para poder utilizar el rol para cargar o descargar datos.

Permisos requeridos para asociar un rol de IAM a un clúster

Para asociar un rol de IAM a un clúster, un usuario de IAM debe disponer del permiso `iam:PassRole` para dicho rol de IAM. Este permiso hace que un administrador pueda restringir los roles de IAM que un usuario puede asociar a clústeres de Amazon Redshift.

En el siguiente ejemplo, se muestra una política de IAM que puede adjuntarse a un usuario de IAM para permitirle realizar estas acciones:

- Obtenga los detalles de todos los clústeres de Amazon Redshift que son propiedad de esa cuenta de usuario.
- Asociar cualquiera de los tres roles de IAM a uno de los dos clústeres de 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 vez que el usuario de IAM tenga los permisos adecuados, ese usuario puede asociar un rol de IAM con un clúster de Amazon Redshift. El rol de IAM estará listo entonces para su uso con el comando COPY o UNLOAD u otros comandos de Amazon Redshift.

Para obtener más información acerca de las políticas de IAM, consulte [Información general de las políticas de IAM](#) en la Guía del usuario de IAM.

Administración de la asociación de roles de IAM a un clúster

Puede asociar un rol de IAM a un clúster de Amazon Redshift cuando cree el clúster. O puede modificar un clúster existente y añadir o eliminar una o más asociaciones a roles de IAM.

Tenga en cuenta lo siguiente:

- Puede asociar un máximo de 10 roles de IAM a un clúster de Amazon Redshift.
- Puede asociar un rol de IAM a varios clústeres de Amazon Redshift.
- Solo puede asociar un rol de IAM a un clúster de Amazon Redshift si el rol de IAM y el clúster son propiedad del mismo.AWSaccount.

Uso de la consola para administrar las asociaciones de roles de IAM

Puede administrar las asociaciones de roles de IAM a un clúster con la consola mediante el siguiente procedimiento.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para administrar las asociaciones a roles de IAM

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y seleccione el clúster que desee actualizar.
3. En Actions (Acciones), seleccione Administrar roles de IAM para mostrar la lista actual de roles de IAM asociados al clúster.
4. En la página Manage IAM roles (Administrar roles de IAM), seleccione los roles de IAM disponibles que desea añadir y luego seleccione Add IAM role (Añadir rol de IAM).
5. Seleccione Done (Aceptar) para guardar los cambios.

Consola original

Para administrar las asociaciones a roles de IAM

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En la lista, seleccione el clúster para el que desea administrar las asociaciones de roles de IAM.
4. Choose See IAM Roles (Ver roles de IAM).
5. Para asociar un rol de IAM a un clúster, seleccione el rol de IAM en la lista Available roles (Roles disponibles). También puede escribir manualmente un rol de IAM si no lo ve incluido en la lista (por ejemplo, si el rol de IAM aún no se creó).

6. Para desvincular una función de IAM del clúster, seleccione X en la función de IAM que desee desvincular.
7. Cuando haya terminado de modificar las asociaciones de funciones de IAM en el clúster, seleccione Apply Changes (Aplicar cambios) para actualizar las funciones de IAM que están asociadas al clúster.

En el panel Manage IAM Roles (Administrar funciones de IAM), se muestra el estado de las asociaciones de funciones de IAM del clúster. Los roles que se asociaron al clúster muestran un estado de `in-sync`. Los roles que se encuentran en el proceso de asociación al clúster muestran un estado de `adding`. Los roles que se están desvinculando del clúster muestran un estado de `removing`.

Manage IAM Roles

Relate IAM roles to your cluster to support copy and unload commands.
Add IAM roles

Available roles

IAM Role	Status	
redshift-admin	in-sync	✕
redshift-iam-role	in-sync	✕
redshift-role	in-sync	✕

[Cancel](#) [Apply changes](#)

Uso de la AWS CLI para administrar las asociaciones de roles de IAM

Puede administrar las asociaciones de roles de IAM a un clúster con la AWS CLI a través de los siguientes métodos.

Asociación de un rol de IAM a un clúster mediante la AWS CLI

Para asociar un rol de IAM a un clúster cuando se crea el clúster, especifique el nombre de recurso de Amazon (ARN) del rol de IAM para el parámetro `--iam-role-arns` del comando `create-cluster`. Puede especificar que se añadan hasta 10 roles de IAM cuando llama al comando `create-cluster`.

Asociar y desasociar roles de IAM a clústeres de Amazon Redshift es un proceso asíncrono. Llame al comando `describe-clusters` para obtener el estado de todas las asociaciones de roles de IAM a su clúster.

En el siguiente ejemplo se asocian dos roles de IAM al clúster recién creado con el nombre `my-redshift-cluster`.

```
aws redshift create-cluster \  
  --cluster-identifier "my-redshift-cluster" \  
  --node-type "dc1.large" \  
  --number-of-nodes 16 \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload" \  
  --iam-role-arns "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

```
"arn:aws:iam::123456789012:role/SecondRedshiftRole"
```

Para asociar un rol de IAM con un clúster de Amazon Redshift existente, especifique el nombre de recurso de Amazon (ARN) del rol de IAM para el atributo `--add-iam-roles` Parámetro de `iam modify-cluster-` `iam-roles` El comando de. Puede especificar que se añadan hasta 10 roles de IAM cuando llama al comando `modify-cluster-iam-roles`.

En el siguiente ejemplo se asocia un rol de IAM a un clúster existente con el nombre `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
  --cluster-identifier "my-redshift-cluster" \
  --add-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Desvinculación de un rol de IAM de un clúster mediante la AWS CLI

Para desvincular un rol de IAM de un clúster, especifique el ARN del rol de IAM para el parámetro `--remove-iam-roles` del comando `modify-cluster-iam-roles`. Puede especificar que se quiten hasta 10 roles de IAM cuando llama al comando `modify-cluster-iam-roles`.

En el siguiente ejemplo se quita la asociación de un rol de IAM para la clase `123456789012 AWS` de un clúster llamado `my-redshift-cluster`.

```
aws redshift modify-cluster-iam-roles \
  --cluster-identifier "my-redshift-cluster" \
  --remove-iam-roles "arn:aws:iam::123456789012:role/RedshiftCopyUnload"
```

Descripción de asociaciones de roles de IAM a un clúster mediante la AWS CLI

Para obtener una lista de todas las funciones de IAM asociadas a un clúster de Amazon Redshift y el estado de la asociación de funciones de IAM, llame al método `describe-clusters` El comando de. El ARN de cada rol de IAM asociado al clúster se devuelve en la lista `IamRoles` como se muestra en el siguiente resultado de ejemplo.

Los roles que se asociaron al clúster muestran un estado de `in-sync`. Los roles que se encuentran en el proceso de asociación al clúster muestran un estado de `adding`. Los roles que se están desvinculando del clúster muestran un estado de `removing`.

```
{
  "Clusters": [
    {
      "ClusterIdentifier": "my-redshift-cluster",
      "NodeType": "dc1.large",
      "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": "dc1.large",
      "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"
  }
],
...
}
```

Para obtener más información sobre el uso de AWS CLI, consulte [AWS CLI Guía del usuario](#).

Registro y monitoreo en Amazon Redshift

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el desempeño de Amazon Redshift y sus AWS Soluciones. Puede recopilar datos de monitoreo de todas las partes de su AWS Para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. AWS proporciona varias herramientas para supervisar sus recursos de Amazon Redshift y responder a posibles incidentes.

Alarmas de Amazon CloudWatch

Con las alarmas de Amazon CloudWatch, verá una sola métrica durante un período de tiempo que especifique. Si la métrica supera un determinado umbral, se envía una notificación a un tema de Amazon SNS o a un AWS Auto Scaling Política. Las alarmas de CloudWatch no invocan acciones simplemente porque se encuentren en determinado estado. En su lugar, el estado debe haber cambiado y debe mantenerse durante el número de periodos especificado. Para obtener más información, consulte [Creación de una alarma \(p. 466\)](#). Para ver una lista de métricas, consulte [Supervisión de Amazon Redshift mediante las métricas de CloudWatch \(p. 422\)](#).

Registros de AWS CloudTrail

CloudTrail proporciona un registro de las operaciones de la API adoptadas por un usuario, un rol o un AWS en Amazon Redshift. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Amazon Redshift, la dirección IP desde la que se realizó, quién la realizó y cuándo, etc. Para obtener más información, consulte [Registro de llamadas de la API de Amazon Redshift con AWS CloudTrail \(p. 380\)](#).

Registro de auditoría de bases de datos

Temas

- [Overview \(p. 374\)](#)
- [Registros de Amazon Redshift \(p. 374\)](#)
- [Habilitación de registros \(p. 376\)](#)
- [Administración de los archivos de registro \(p. 377\)](#)
- [Solución de problemas del registro de auditoría de Amazon Red \(p. 380\)](#)

- [Registro de llamadas de la API de Amazon Redshift conAWS CloudTrail \(p. 380\)](#)
- [ID de cuenta de Amazon Redshift enAWS CloudTraillogs \(p. 383\)](#)
- [Configuración de la auditoría con la consola \(p. 385\)](#)
- [Configuración del registro mediante elAWS CLIy la API de Amazon Redshift \(p. 387\)](#)

Overview

Amazon Redshift registra información sobre las conexiones y las actividades de usuario en la base de datos. Estos registros ayudan a monitorear la base de datos con fines de seguridad y solución de problemas, un proceso que suele denominarse auditoría de base de datos. Los registros se almacenan en buckets de Amazon S3. Ofrecen un acceso conveniente con características de seguridad de datos a los usuarios que se encargan de las actividades de monitorización de la base de datos.

Registros de Amazon Redshift

Amazon Redshift registra información en los siguientes archivos de registro:

- Registro de conexiónregistra los intentos de autenticación y las conexiones y desconexiones.
- Registro de usuarioregistra información acerca de los cambios en las definiciones de usuario de base de datos.
- Registro de actividad de usuario— registra cada consulta antes de su ejecución en la base de datos.

Los registros de usuario y de conexión son útiles principalmente por fines de seguridad. Puede utilizar el registro de conexión para supervisar la información sobre los usuarios que se conectan a la base de datos y la información de conexión relacionada. Esta información puede ser su dirección IP, cuándo hicieron la solicitud, qué tipo de autenticación utilizaron, etc. Puede utilizar el registro de usuario para monitorear los cambios en las definiciones de los usuarios de la base de datos.

El registro de actividad de usuario es útil principalmente para la solución de problemas. Realiza un seguimiento de la información acerca de las consultas que realizan los usuarios y el sistema en la base de datos.

El registro de conexión y el registro de usuario corresponden a la información que se almacena en las tablas de sistema de la base de datos. Puede utilizar las tablas de sistema para obtener la misma información, pero los archivos de registro proporcionan un mecanismo más sencillo de recuperación y revisión. Los archivos de registro utilizan los permisos de Amazon S3 en lugar de los de la base de datos para realizar consultas en las tablas. Además, al revisar la información de los archivos de registro en lugar de consultar las tablas de sistema, se reduce cualquier impacto de interacción con la base de datos.

Note

Los archivos de registro no están tan actualizados como las tablas base de registro del sistema [STL_USERLOG](#) y [STL_CONNECTION_LOG](#). Los registros que son más antiguos que el registro más reciente (sin incluir este) se copian en archivos log.

Registro de conexión

Registra los intentos de autenticación y las conexiones y desconexiones. En la siguiente tabla se describe la información del registro de conexión.

Nombre de la columna	Descripción
event	Evento de conexión o de autenticación.
recordtime	Hora cuando se produjo el evento.

Nombre de la columna	Descripción
remotehost	Nombre o dirección IP del host remoto.
remoteport	Número del puerto para el host remoto.
pid	ID del proceso asociado a la instrucción.
dbname	Nombre de la base de datos.
username	Nombre de usuario.
authmethod	Método de autenticación.
duration	Duración de la conexión en microsegundos.
sslversion	Versión de la capa de conexión segura (SSL).
sslcipher	Cifrado SSL.
mtu	Unidad de transmisión máxima (MTU).
sslcompression	Tipo de compresión de la SSL.
sslexpansion	Tipo de expansión de la SSL.
iamauthguid	ID de autenticación de IAM para la solicitud de CloudTrail.
application_name	Nombre original o actualizado de la aplicación para una sesión.
versión_controlador	La versión del controlador ODBC o JDBC que se conecta al clúster de Amazon Redshift desde las herramientas de cliente SQL de terceros.
versión de os_	La versión del sistema operativo que se encuentra en el equipo cliente que se conecta al clúster de Amazon Redshift.
plugin_name	El nombre del complemento utilizado para conectarse al clúster de Amazon Redshift.

Registro de usuario

Registra detalles de los siguientes cambios realizados en un usuario de una base de datos:

- Creación de usuario
- Eliminación de usuario
- Modificación de usuario (cambio de nombre)
- Modificación de usuario (modificación de propiedades)

Nombre de la columna	Descripción
userid	ID de usuario afectado por el cambio.
username	Nombre del usuario afectado por el cambio.
oldusername	En el caso de una acción de cambio de nombre, el nombre de usuario original. Para el resto de las acciones, este campo está vacío.

Nombre de la columna	Descripción
action	Acción que ocurrió. Valores válidos: • Modificación • Crear • Drop (Eliminar) • Cambio de nombre
usecreatedb	Si es true (1), indica que el usuario ha creado privilegios de base de datos.
usesuper	Si es true (1), indica que el usuario es un superusuario.
usecatupd	Si es true (1), indica que el usuario puede actualizar los catálogos de sistema.
valuntil	Fecha de vencimiento de la contraseña.
pid	ID de proceso.
xid	ID de transacción.
recordtime	Hora en UTC en que comenzó la consulta.

Registro de actividad de usuario

Registra cada consulta antes de su ejecución en la base de datos.

Nombre de la columna	Descripción
recordtime	Hora cuando se produjo el evento.
db	Nombre de la base de datos.
user	Nombre de usuario.
pid	ID del proceso asociado a la instrucción.
userid	ID de usuario.
xid	ID de transacción.
query	Prefijo de LOG: seguido del texto de la consulta, incluidas las líneas nuevas.

Habilitación de registros

El registro de auditoría no está habilitado de forma predeterminada en Amazon Redshift. Cuando habilita el registro en el clúster, Amazon Redshift crea y carga los registros en Amazon S3 que capturan datos desde el momento en que se habilita el registro de auditoría hasta el momento actual. Cada actualización de registros es una continuación de la información que ya estaba registrada.

Note

El registro de auditoría de Amazon S3 es un proceso manual y opcional. Cuando habilita el registro en el clúster, está habilitando solo el registro en Amazon S3. El registro en las tablas de sistema no es opcional y ocurre automáticamente en el clúster. Para obtener más información

acerca del registro de en las tablas de sistema, consulte [Referencia de las tablas de sistema](#) En la Guía de desarrollador de base de datos de Amazon Redshift.

El registro de conexión, el registro de usuario y el registro de actividad del usuario se habilitan juntos con la herramienta de AWS Management Console, la referencia de la API de Amazon Redshift o la AWS Command Line Interface (AWS CLI). Para el registro de actividad de usuario, también debe habilitar el parámetro `enable_user_activity_logging` de la base de datos. Si habilita solo la función de registro de auditoría y no el parámetro asociado, los registros de auditoría de la base de datos registrarán únicamente la información de los registros de conexión y de usuario, no la del registro de actividad del usuario. El parámetro de `enable_user_activity_logging` no está habilitado (`false`) de forma predeterminada. Puede configurarlo como `true` para habilitar el registro de actividad del usuario. Para obtener más información, consulte [Grupos de parámetros de Amazon Redshift \(p. 210\)](#).

Note

En estos momentos solo es posible usar cifrado de claves administradas por Amazon S3 (SSE-S3) (AES-256) para el registro de auditorías.

Administración de los archivos de registro

El número y el tamaño de los archivos de registro de Amazon Redshift en Amazon S3 dependen en gran medida de la actividad del clúster. Si tiene un clúster activo que genera un gran número de registros, es posible que Amazon Redshift genere los archivos de registro con mayor frecuencia. Es posible que tenga una serie de archivos de registro para el mismo tipo de actividad, como tener varios registros de conexión en la misma hora.

Dado que Amazon Redshift utiliza Amazon S3 para almacenar registros, se le aplican cargos por el almacenamiento que utilice en Amazon S3. Antes de configurar el registro, debe tener pensado durante cuánto tiempo necesita almacenar los archivos de registro. Como parte de esto, determine cuándo se pueden eliminar o archivar los archivos de registro según sus necesidades de auditoría. El plan que cree depende en gran medida del tipo de datos que almacene, como datos sujetos a requisitos normativos o de conformidad. Para obtener más información acerca de los precios de Amazon S3, consulte [Precios de Amazon Simple Storage Service \(S3\)](#).

Permisos de bucket para el registro de auditoría de Amazon Redshift

Cuando habilita el registro, Amazon Redshift recopila la información de los registros y la carga en los archivos de registro almacenados en Amazon S3. Es posible utilizar un bucket existente o uno nuevo. Amazon Redshift necesita los siguientes permisos de IAM en el bucket:

- `s3:GetBucketAcl` El servicio requiere permisos de lectura en el bucket de Amazon S3 para poder identificar al propietario del bucket.
- `s3:PutObject` El servicio requiere permisos de colocación de objetos para cargar los registros. Además, el usuario de IAM o rol de IAM que habilita el registro debe tener `s3:PutObject` para el bucket de Amazon S3. Cada vez que se cargan registros, el servicio determina si el propietario del bucket actual coincide con el propietario del bucket en el momento que se habilitó el registro. Si estos propietarios no coinciden, recibirá un error.

Si hace que Amazon Redshift cree un nuevo bucket para usted como parte de la configuración, se aplicarán los permisos correctos al bucket. Sin embargo, si crea su propio bucket en Amazon S3 o utiliza un bucket existente, tendrá que añadir una política de bucket que incluya el nombre del bucket. También necesita el ID de cuenta de Amazon Redshift que se corresponda con su AWS Región de la siguiente tabla.

Nombre de la región	Región	ID de cuenta
US East (N. Virginia) Region	us-east-1	193672423079

Nombre de la región	Región	ID de cuenta
US East (Ohio) Region	us-east-2	391106570357
US West (N. California) Region	us-west-1	262260360010
US West (Oregon) Region	us-west-2	902366379725
Región de África (Ciudad del Cabo)	af-south-1	365689465814
Región Asia Pacífico (Hong Kong)	ap-east-1	313564881002
Asia Pacific (Mumbai) Region	ap-south-1	865932855811
Región de Asia-Pacífico (Osaka)	ap-northeast-3	090321488786
Asia Pacific (Seoul) Region	ap-northeast-2	760740231472
Región Asia Pacífico (Singapur)	ap-southeast-1	361669875840
Región Asia Pacífico (Sídney)	ap-southeast-2	762762565011
Región Asia Pacífico (Tokio)	ap-northeast-1	404641285394
Canada (Central) Region	ca-central-1	907379612154
Europe (Frankfurt) Region	eu-central-1	053454850223
Europe (Ireland) Region	eu-west-1	210876761215
Europe (London) Region	eu-west-2	307160386991
Región Europa (Milán)	eu-south-1	945612479654
Región de Europa (París)	eu-west-3	915173422425
Región de Europa (Estocolmo)	eu-north-1	729911121831
Región Medio Oriente (Baréin)	me-south-1	013126148197
Región América del Sur (São Paulo)	sa-east-1	075028567923

La política de bucket usa el siguiente formato, en **BucketName** es un marcador de posición para su valor propio. La **AccountId** pertenece a la tabla de identificadores de cuenta de Amazon Redshift que corresponde a su AWS Región .

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::AccountId:user/logs"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::BucketName/*"
    },
    {
      "Sid": "Get bucket policy needed for audit logging ",
      "Effect": "Allow",
```

```
"Principal": {
  "AWS": "arn:aws:iam::AccountID:user/logs"
},
"Action": "s3:GetBucketAcl",
"Resource": "arn:aws:s3:::BucketName"
}
]
}
```

En el ejemplo siguiente se muestra una política de bucket de para la región EE. UU. Este (Norte de Virginia) y un bucket denominado AuditLogs.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Put bucket policy needed for audit logging",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::193672423079:user/logs"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::AuditLogs/*"
    },
    {
      "Sid": "Get bucket policy needed for audit logging ",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::193672423079:user/logs"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::AuditLogs"
    }
  ]
}
```

Para obtener más información acerca de la creación de buckets de Amazon S3 y la adición de políticas de bucket, consulte [Creación de un bucket](#) y [Edición de permisos de bucket](#) en la Guía del usuario de la consola de Amazon Simple Storage Service.

Estructura de bucket para el registro de auditoría de Amazon Redshift

De forma predeterminada, Amazon Redshift organiza los archivos de registro en el bucket de Amazon S3 utilizando la siguiente estructura de bucket y

objetos:AWSLogs/AccountID/ServiceName/Region/Year/Month/Day/AccountID_ServiceName_Region_ClusterName.gz

Por ejemplo: AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz

Si proporciona un key prefix de Amazon S3, este se coloca al comienzo de la clave.

Por ejemplo, si especifica un prefijo de myprefix: myprefix/AWSLogs/123456789012/redshift/us-east-1/2013/10/29/123456789012_redshift_us-east-1_mycluster_userlog_2013-10-29T18:01.gz

El key prefix de Amazon S3 no puede tener más de 512 caracteres. No puede contener espacios (), comillas dobles (") , comillas simples (') ni una barra inversa (\). También existe un número de caracteres especiales y de control que no están permitidos. Los códigos hexadecimales para estos caracteres son:

- de x00 a x20
- x22

- x27
- x5c
- x7f o mayores

Solución de problemas del registro de auditoría de Amazon Red

El registro de auditoría de Amazon Redshift se puede interrumpir por las siguientes razones:

- Amazon Redshift no tiene permiso para cargar registros en el bucket de Amazon S3. Compruebe que el bucket esté configurado con la política de IAM correcta. Para obtener más información, consulte [Permisos de bucket para el registro de auditoría de Amazon Redshift \(p. 377\)](#).
- Cambió el propietario del bucket. Cuando Amazon Redshift carga los registros, compruebe que el propietario del bucket sea el mismo que cuando se habilitó el registro. Si el propietario del bucket ha cambiado, Amazon Redshift no puede cargar registros hasta que usted configure otro bucket para utilizar en el registro de auditoría. Para obtener más información, consulte [Modificación del bucket para el registro de auditoría \(p. 387\)](#).
- No se ha encontrado el bucket. Si el bucket se elimina en Amazon S3, Amazon Redshift no puede cargar registros. Tendrá que volver a crear el bucket o configurar Amazon Redshift para que cargue los registros a un bucket diferente. Para obtener más información, consulte [Modificación del bucket para el registro de auditoría \(p. 387\)](#).

Registro de llamadas de la API de Amazon Redshift conAWS CloudTrail

Amazon Redshift está integrado conAWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o unAWS en Amazon Redshift. CloudTrail captura como eventos todas las llamadas a las API de Amazon Redshift. Se incluyen las llamadas desde la consola de Amazon Redshift y las llamadas desde código a las operaciones de la API de Amazon Redshift. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Amazon Redshift. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Event history (Historial de eventos). Mediante la información recopilada por CloudTrail, puede determinar ciertos detalles. Se incluyen la solicitud que se envió a Amazon Redshift, la dirección IP desde la que se realizó, quién la realizó y cuándo, entre otros.

Puede utilizar CloudTrail de forma independiente o junto con el registro de auditoría de base de datos de Amazon Redshift.

Para obtener más información sobre CloudTrail, consulte la[AWS CloudTrailGuía del usuario](#).

Información de Amazon Redshift en CloudTrail

CloudTrail está habilitado en suAWSUna cuenta de al crearla. Cuando se produce una actividad en Amazon Redshift, dicha actividad se registra en un evento de CloudTrail junto con losAWS eventos de servicios enHistorial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail Event](#).

Para mantener un registro continuo de los eventos deAWS, incluidos los eventos de Amazon Redshift, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar archivos de registro a un bucket de Amazon S3. De forma predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones. El registro de seguimiento registra los eventos de todas las regiones deAWSy entrega los archivos de registro al bucket de Amazon S3 especificado. Además, puede configurar otrosAWSServicios de para analizar y actuar en función de los datos de eventos recopilados en los registros de CloudTrail. Para obtener más información, consulte:

- [Introducción a la creación de registros de seguimiento](#)

- [Consulte Servicios e integraciones compatibles con CloudTrail.](#)
- [Configuración de notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de registro de CloudTrail de varias regiones y Recepción de archivos de registro de CloudTrail de varias cuentas](#)

CloudTrail registra todas las acciones de Amazon Redshift y se documentan en la [Referencia de la API de Amazon Redshift](#). Por ejemplo, las llamadas a las acciones `CreateCluster`, `DeleteCluster` y `DescribeCluster` generan entradas en los archivos de log de CloudTrail.

Cada entrada de registro o evento contiene información acerca de quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro servicio de AWS.

Para obtener más información, consulte [CloudTrail userIdentity Element](#).

Descripción de las entradas de archivos de registro de Amazon Redshift

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registro en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log. Un evento representa una única solicitud de cualquier origen e incluye información acerca de la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etcétera. Los archivos de registro de CloudTrail no son un rastro de la stack ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

En el ejemplo siguiente se muestra una entrada del registro de CloudTrail para una llamada `CreateCluster` de ejemplo.

```
{
  "eventVersion": "1.04",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAMVNPBQA3EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/Admin",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "Admin",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-03T16:51:56Z"
      }
    }
  },
  "invokedBy": "signin.amazonaws.com",
  "eventTime": "2017-03-03T16:56:09Z",
  "eventSource": "redshift.amazonaws.com",
  "eventName": "CreateCluster",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "52.95.4.13",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "clusterIdentifier": "my-dw-instance",
    "allowVersionUpgrade": true,
    "enhancedVpcRouting": false,
    "encrypted": false,
    "clusterVersion": "1.0",
```



```

        "masterUsername": "awsuser",
        "masterUserPassword": "*****",
        "automatedSnapshotRetentionPeriod": 1,
        "port": 5439,
        "dbName": "mydbtest",
        "clusterType": "single-node",
        "nodeType": "dc1.large",
        "publiclyAccessible": true,
        "vpcSecurityGroupIds": [
            "sg-95f606fc"
        ]
    },
    "responseElements": {
        "nodeType": "dc1.large",
        "preferredMaintenanceWindow": "sat:05:30-sat:06:00",
        "clusterStatus": "creating",
        "vpcId": "vpc-84c22aed",
        "enhancedVpcRouting": false,
        "masterUsername": "awsuser",
        "clusterSecurityGroups": [],
        "pendingModifiedValues": {
            "masterUserPassword": "*****"
        },
        "dbName": "mydbtest",
        "clusterVersion": "1.0",
        "encrypted": false,
        "publiclyAccessible": true,
        "tags": [],
        "clusterParameterGroups": [
            {
                "parameterGroupName": "default.redshift-1.0",
                "parameterApplyStatus": "in-sync"
            }
        ],
        "allowVersionUpgrade": true,
        "automatedSnapshotRetentionPeriod": 1,
        "numberOfNodes": 1,
        "vpcSecurityGroups": [
            {
                "status": "active",
                "vpcSecurityGroupId": "sg-95f606fc"
            }
        ],
        "iamRoles": [],
        "clusterIdentifier": "my-dw-instance",
        "clusterSubnetGroupName": "default"
    },
    "requestID": "4c506036-0032-11e7-b8bf-d7aa466e9920",
    "eventID": "13ba5550-56ac-405b-900a-8a42b0f43c45",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}

```

En el ejemplo siguiente se muestra una entrada del registro de CloudTrail para una llamada DeleteCluster de ejemplo.

```

{
    "eventVersion": "1.04",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAMVNPBQA3EXAMPLE",
        "arn": "arn:aws:iam::123456789012:user/Admin",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",

```

```

    "userName": "Admin",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2017-03-03T16:58:23Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2017-03-03T17:02:34Z",
  "eventSource": "redshift.amazonaws.com",
  "eventName": "DeleteCluster",
  "awsRegion": "us-east-2",
  "sourceIPAddress": "52.95.4.13",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "clusterIdentifier": "my-dw-instance",
    "skipFinalClusterSnapshot": true
  },
  "responseElements": null,
  "requestID": "324cb76a-0033-11e7-809b-1bbbef7710bf",
  "eventID": "59bcc3ce-e635-4cce-b47f-3419a36b3fa5",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}

```

ID de cuenta de Amazon Redshift enAWS CloudTraillogs

Cuando Amazon Redshift llama a otroAWSPara usted, la llamada se registra con un ID de cuenta que pertenece a Amazon Redshift. No se registra con su ID de cuenta. Por ejemplo, suponga que Amazon Redshift llama aAWS Key Management Service(AWS KMS) como CreateGrant, Decrypt, Encrypt y RetireGrant para administrar el cifrado en el clúster. En este caso, registra las llamadas porAWS CloudTrailmediante un identificador de cuenta de Amazon Redshift.

Amazon Redshift utiliza los ID de cuenta de la siguiente tabla cuando llama a otrosAWSServicios de .

Región	Región	ID de cuenta
US East (N. Virginia) Region	us-east-1	368064434614
US East (Ohio) Region	us-east-2	790247189693
US West (N. California) Region	us-west-1	703715109447
US West (Oregon) Region	us-west-2	473191095985
Región de África (Ciudad del Cabo)	af-south-1	420376844563
Región Asia Pacífico (Hong Kong)	ap-east-1	651179539253
Asia Pacific (Mumbai) Region	ap-south-1	408097707231
Región de Asia-Pacífico (Osaka)	ap-northeast-3	398671365691
Asia Pacific (Seoul) Region	ap-northeast-2	713597048934
Región Asia Pacífico (Singapur)	ap-southeast-1	960118270566
Región Asia Pacífico (Sídney)	ap-southeast-2	485979073181
Región Asia Pacífico (Tokio)	ap-northeast-1	615915377779

Región	Región	ID de cuenta
Canada (Central) Region	ca-central-1	764870610256
Europe (Frankfurt) Region	eu-central-1	434091160558
Europe (Ireland) Region	eu-west-1	246478207311
Europe (London) Region	eu-west-2	885798887673
Región Europa (Milán)	eu-south-1	041313461515
Región de Europa (París)	eu-west-3	694668203235
Región de Europa (Estocolmo)	eu-north-1	553461782468
Región Medio Oriente (Baréin)	me-south-1	051362938876
Región América del Sur (São Paulo)	sa-east-1	392442076723

En el ejemplo siguiente se muestra una entrada de registro de CloudTrail para elAWS KMSDescifrar operación que fue llamada por 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"
}
```

Configuración de la auditoría con la consola

Puede configurar Amazon Redshift para que cree archivos de registro de auditoría y los almacene en S3.

Habilitación del registro de auditoría con la consola

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para habilitar el registro de auditoría de un clúster

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLUSTERES) y seleccione el clúster que desee actualizar.
3. Elija la pestaña Properties. A continuación, consulte elRegistro de auditoríaeen laConfiguraciones de basesección.
4. SeleccionarEditar, luegoEdición del registro de auditoría.
5. En la páginaEdición del registro de auditoría, elijaHabilitar registro de auditoríae introduzca sus opciones en función de dónde estén almacenados los registros.
6. SeleccionarGuarde los cambiosPara guardar sus opciones.

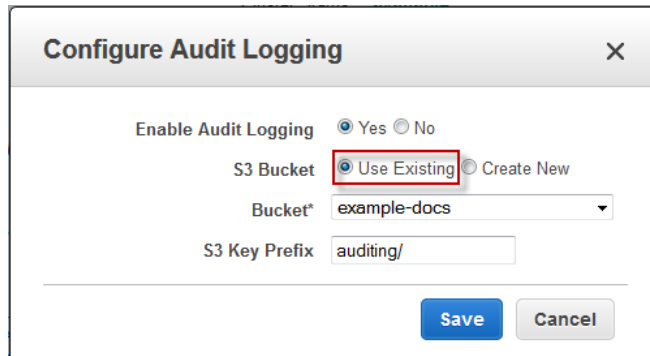
Consola original

Para habilitar el registro de auditoría de un clúster

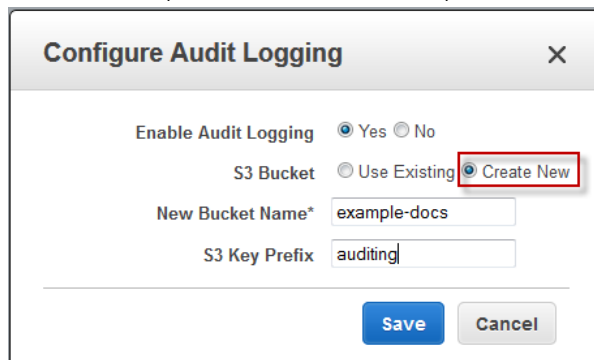
1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En la lista, haga clic en el clúster para el que desea habilitar el registro.
4. En la página de detalles del clúster, seleccione Database (Base de datos) y luego Configure Audit Logging (Configurar registro de auditoría).
5. En el cuadro de diálogo Configure Audit Logging (Configurar registro de auditoría), en el cuadro Enable Audit Logging (Habilitar registro de auditoría), haga clic en Yes (Sí).

6. En S3 Bucket (Bucket de S3), realice alguna de las siguientes operaciones:

- Si ya tiene un bucket de S3 que desee utilizar, seleccione Use Existing (Usar existente) y seleccione el bucket en la lista Bucket.



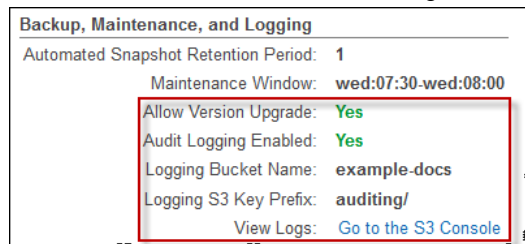
- Si necesita crear un bucket de S3 nuevo, seleccione Create New (Crear nuevo) y, en el cuadro New Bucket Name (Nuevo nombre de bucket), escriba un nombre.



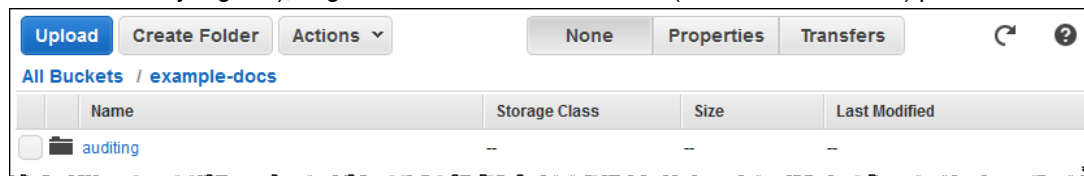
7. Si lo desea, en S3 Key Prefix (Prefijo de clave de S3), escriba un prefijo para añadirlo al bucket de S3.

8. Elija Save (Guardar).

Una vez configurado el registro de auditoría, la página de detalles Cluster (Clúster) se actualiza para mostrar información acerca de la configuración del registro.



En la página de detalles de Cluster (Clúster), en Backup, Maintenance, and Logging (Copia de seguridad, mantenimiento y registro), haga clic en Go to the S3 console (Ir a la consola de S3) para ir al bucket.



Modificación del bucket para el registro de auditoría

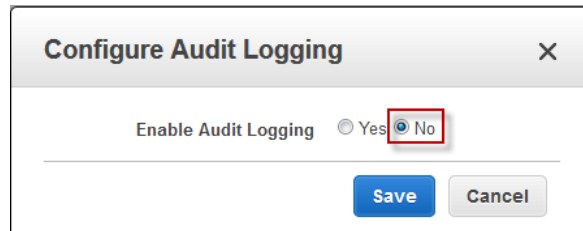
(Consola original) Modificación del bucket de Amazon S3 para el registro de auditoría

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Seleccione el clúster de la lista el que desea modificar el bucket utilizado para el registro de auditoría.
4. En la página de detalles del clúster, seleccione Database (Base de datos) y luego Configure Audit Logging (Configurar registro de auditoría).
5. En S3 Bucket (Bucket de S3), seleccione un bucket existente o cree uno nuevo.
6. Si lo desea, en S3 Key Prefix (Prefijo de clave de S3), escriba un prefijo para añadirlo al bucket de S3.
7. Elija Save (Guardar).

Deshabilitación del registro de auditoría con la consola

(Consola original) Deshabilitación del registro de auditoría

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Seleccione el clúster de la lista en el que desea deshabilitar el registro.
4. En la página de detalles del clúster, seleccione Database (Base de datos) y luego Configure Audit Logging (Configurar registro de auditoría).
5. En el cuadro de diálogo Configure Audit Logging (Configurar registro de auditoría), en el cuadro Enable Audit Logging (Habilitar registro de auditoría), haga clic en No.



6. Elija Save (Guardar).

Configuración del registro mediante elAWS CLIy la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para configurar el registro de auditoría:

- [describe-logging-status](#)
- [disable-logging](#)
- [enable-logging](#)

Puede utilizar las siguientes acciones de la API de Amazon Redshift para configurar el registro de auditoría:

- [DescribeLoggingStatus](#)
- [DisableLogging](#)

- [EnableLogging](#)

Validación de la conformidad para Amazon Redshift

Audidores externos evalúan la seguridad y la conformidad de Amazon Redshift como parte de varios AWS Programas de conformidad. Estos incluyen SOC, PCI, FedRAMP, HIPAA y otros.

Para obtener una lista de los servicios de AWS en el ámbito de programas de conformidad específicos, consulte [Servicios de AWS en el ámbito del programa de conformidad](#). Para obtener información general, consulte [Programas de conformidad de AWS](#).

Puede descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#).

Su responsabilidad de conformidad al utilizar Amazon Redshift se determina en función de la confidencialidad de los datos, los objetivos de conformidad de su organización y la legislación y normativa aplicables. Si su uso de Amazon Redshift está sujeto a conformidad con estándares tales como HIPAA, PCI o FedRAMP, AWS proporciona recursos para ayudar a:

- [Guías de inicio rápido de seguridad y cumplimiento](#) que incluyen consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- [Documento técnico sobre la arquitectura para la seguridad y el cumplimiento de HIPAA](#), que describe cómo las empresas pueden usar AWS para crear aplicaciones que se ajusten al estándar HIPAA.
- [AWS Recursos de conformidad](#), manuales y guías que podrían aplicarse a su sector y ubicación.
- [AWS Config](#), un AWS puede evaluar en qué medida las configuraciones de los recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- [AWS Centro de seguridad de](#), un AWS, proporciona una visión completa del estado de seguridad dentro de AWS que le ayudará a contrariar el grado de conformidad con las prácticas recomendadas y los estándares sectoriales.

En los siguientes documentos de conformidad y seguridad se trata Amazon Redshift y están disponibles bajo demanda a través de AWS Artifact. Para obtener más información, consulte [AWS Artifact](#).

- Catálogo de controles de conformidad de informática en la nube (C5)
- Declaración de aplicabilidad (SoA) de ISO 27001:2013
- Certificación ISO 27001:2013
- Declaración de aplicabilidad (SoA) de ISO 27017:2015
- Certificación ISO 27017:2015
- Declaración de aplicabilidad (SoA) de ISO 27018:2015
- Certificación ISO 27018:2014
- Certificación ISO 9001:2015
- Declaración de conformidad (AOC) PCI DSS y resumen de responsabilidad
- Informe de controles de organizaciones de servicios (SOC) 1
- Informe de controles de organizaciones de servicios (SOC) 2
- Informe de controles de organizaciones de servicios (SOC) 2 para la confidencialidad

Resiliencia en Amazon Redshift

La AWS La infraestructura global de está integrada por AWS Regiones y zonas de disponibilidad (AZ). AWS Las regiones de proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que

se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras de centros de datos tradicionales únicos o múltiples.

Casi todas las regiones de AWS tienen varias zonas de disponibilidad y centros de datos. Puede implementar sus aplicaciones en varias zonas de disponibilidad en la misma región para la tolerancia de errores y la baja latencia.

Para obtener más información acerca de las zonas de disponibilidad y las regiones de AWS, consulte [Infraestructura global de AWS](#).

Seguridad de la infraestructura en Amazon Redshift

Como servicio gestionado, Amazon Redshift está protegido por los procedimientos globales de seguridad de red descritos en el [Amazon Web Services: Información general sobre los procesos de seguridad](#) Documento técnico.

Utiliza AWS Publicado las llamadas a la API de para obtener acceso a Amazon Redshift a través de la red. Los clientes deben ser compatibles con Transport Layer Security (TLS) 1.0 o una versión posterior. Le recomendamos TLS 1.2 o una versión posterior. Los clientes también deben ser compatibles con conjuntos de cifrado con confidencialidad directa total (PFS) tales como Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar [AWS Security Token Service \(AWS STS\)](#) para generar credenciales de seguridad temporales para firmar solicitudes.

Puede llamar a estas operaciones de la API desde cualquier ubicación de red. Además, Amazon Redshift admite políticas de acceso basadas en recursos que pueden incluir restricciones en función de la dirección IP de origen.

Aislamiento de red

Una nube privada virtual (VPC) basada en el servicio de Amazon VPC es su red privada y aislada de manera lógica en la AWS Cloud. Puede implementar un clúster de Amazon Redshift en una VPC siguiendo los siguientes pasos:

- Cree una VPC en una AWS Región . Para obtener más información, consulte [¿Qué es Amazon VPC?](#) en la Guía del usuario de Amazon VPC.
- Cree dos o más subredes de VPC privadas. Para obtener más información, consulte [VPC y subredes](#) en la Guía del usuario de Amazon VPC.
- Implemente un clúster de Amazon Redshift. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#) .

Un clúster de Amazon Redshift está bloqueado de forma predeterminada tras el aprovisionamiento. Para permitir el tráfico de red entrante desde clientes de Amazon Redshift, asocie un grupo de seguridad de la VPC a un clúster de Amazon Redshift. Para obtener más información, consulte [Grupos de subredes del clúster de Amazon Redshift \(p. 80\)](#) .

Para permitir el tráfico solo hacia o desde rangos de direcciones IP específicos, actualice los grupos de seguridad con su VPC. Un ejemplo consiste en permitir el tráfico solo desde o hacia su red corporativa.

Amazon Redshift admite la implementación de clústeres en las VPC de tenencia dedicada. Para obtener más información, consulte [Instancias dedicadas](#) en la Guía del usuario de Amazon EC2.

Grupos de seguridad de clúster de Amazon Redshift

Cuando aprovisiona un clúster de Amazon Redshift, se bloquea de forma predeterminada para que nadie pueda obtener acceso a él. Para conceder a otros usuarios acceso de entrada a un clúster de Amazon Redshift, debe asociar el clúster a un grupo de seguridad. Si está en la plataforma de EC2-VPC, puede utilizar un grupo de seguridad de Amazon VPC de existente o definir uno nuevo y luego asociarlo a un clúster. Para obtener más información acerca de la administración de un clúster en la plataforma de EC2-VPC, consulte [Administración de clústeres en una VPC \(p. 75\)](#).

Si está en la plataforma EC2-Classic, defina un grupo de seguridad de clúster y asócielo a un clúster, como se describe en las siguientes secciones. Le recomendamos que lance el clúster en una plataforma EC2-VPC en lugar de hacerlo en una plataforma EC2-Classic. Sin embargo, puede restaurar una instantánea EC2-Classic en un clúster EC2-VPC con la consola de Amazon Redshift. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 258\)](#).

Temas

- [Overview \(p. 390\)](#)
- [Administración de grupos de seguridad de clúster mediante la consola \(p. 391\)](#)
- [Administración de grupos de seguridad de clúster con la herramientaAWS SDK for Java \(p. 402\)](#)
- [Administración de grupos de seguridad de clúster con la herramientaAWS CLIy Amazon Redshift API \(p. 405\)](#)

Overview

Un grupo de seguridad de clúster está formado por un conjunto de reglas que controlan el acceso al clúster. Las reglas individuales identifican un rango de direcciones IP o un grupo de seguridad de Amazon EC2 al que se permite obtener acceso al clúster de. Cuando asocia un grupo de seguridad de clúster a un clúster, las reglas que están definidas en el grupo de seguridad de clúster controlan el acceso al clúster.

Puede crear grupos de seguridad de clúster independientemente de la provisión de clústeres. Puede asociar un grupo de seguridad de clúster a un clúster de Amazon Redshift cuando aprovisiona el clúster o más adelante. También puede asociar un grupo de seguridad de clúster con varios clústeres.

Amazon Redshift ofrece un grupo de seguridad de clúster denominado default, que se crea automáticamente cuando lanza el primer clúster. Inicialmente, este grupo de seguridad de clúster está vacío. Puede añadir reglas de acceso de entrada al grupo de seguridad de clúster predeterminado y, luego, asociarlo al clúster de Amazon Redshift.

Si el grupo de seguridad de clúster predeterminado es suficiente para el usuario, no es necesario crear uno propio. Sin embargo, de forma opcional, puede crear sus propios grupos de seguridad de clúster adicionales para administrar mejor el acceso de entrada al clúster. Por ejemplo, suponga que está ejecutando un servicio en un clúster de Amazon Redshift y tiene varias empresas como clientes. Si no desea proporcionar el mismo acceso a todos los clientes, se recomienda crear grupos de seguridad de clúster independientes, uno para cada empresa. Puede añadir reglas en cada grupo de seguridad de clúster para identificar los grupos de seguridad de Amazon EC2 y los rangos de dirección IP específicos de una empresa. Luego, puede asociar todos estos grupos de seguridad de clúster al clúster.

Puede asociar un grupo de seguridad de clúster a varios clústeres y puede asociar varios grupos de seguridad de clúster a un clúster, sujeto aAWSlímites del servicio. Para obtener más información, consulte [Límites de Amazon Redshift](#).

Puede administrar grupos de seguridad de clústeres mediante la consola de Amazon Redshift y mediante programación, utilizando la API de Amazon Redshift o laAWSSDK.

Amazon Redshift aplica cambios a un grupo de seguridad de clúster de inmediato. Por lo que si asoció un grupo de seguridad de clúster a un clúster, las reglas de acceso de entrada al clúster en el grupo de seguridad de clúster actualizado se aplican de inmediato.

Administración de grupos de seguridad de clúster mediante la consola

Puede crear, modificar y eliminar grupos de seguridad de clúster utilizando la consola de Amazon Redshift. También puede administrar el grupo de seguridad de clúster predeterminado en la consola de Amazon Redshift. Todas las tareas parten de la lista de grupos de seguridad de clúster. Debe elegir un grupo de seguridad de clúster para administrarlo.

No puede eliminar el grupo de seguridad de clúster predeterminado, pero puede modificarlo mediante la autorización o revocación de acceso.

Creación de un grupo de seguridad de clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG, y seleccione Security groups (Grupos de seguridad) para mostrar la página Grupos de seguridad de clúster.

Note

Solo puede administrar grupos de seguridad de clúster cuando inicie sesión con un EC2-ClassicAWSaccount.

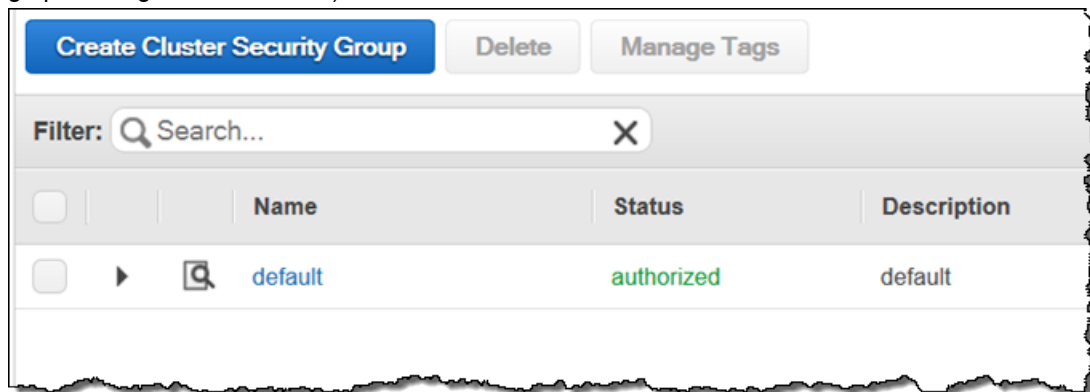
3. Seleccione Create cluster security group (Crear grupo de seguridad de clúster) para mostrar la ventana Create cluster security group (Crear grupo de seguridad de clúster).
4. Para el nuevo grupo de seguridad, introduzca valores para lo siguiente:
 - Nombre
 - Descripción
 - Rango de CIDR/IP que autorizar en el documento `nnn.nnn.nnn.nn/nn`
 - AWSID de cuenta de(sin guiones)
 - EC2 security group name (Nombre de grupo de seguridad EC2)
5. Para crear el grupo de seguridad, haga clic en Create (Crear).

Consola original

Para crear un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).

3. En la pestaña Security Groups (Grupos de seguridad), elija Create Cluster Security Group (Crear grupo de seguridad de clúster).



4. En el cuadro de diálogo Create Cluster Security Group (Crear grupo de seguridad de clúster), especifique un nombre y una descripción para el grupo de seguridad del clúster.



5. Seleccione Create (Crear).

El nuevo grupo se muestra en la lista de grupos de seguridad de clúster.

Etiquetado de un grupo de seguridad de clúster

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para etiquetar un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG, y seleccione Security groups (Grupos de seguridad) para mostrar la página Grupos de seguridad de clúster.

Note

Solo puede administrar grupos de seguridad de clúster cuando inicie sesión con un EC2-ClassicAWSaccount.

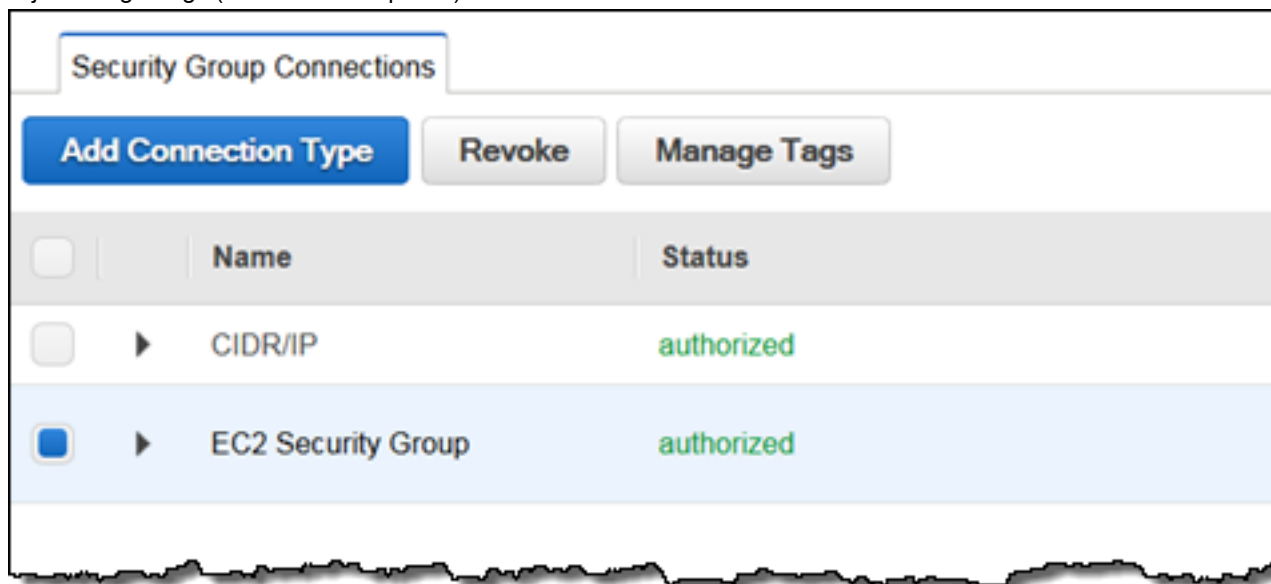
3. Seleccione un grupo de seguridad de clúster, luego elija Manage tags (Administrar etiquetas) para mostrar la página Manage tags (Administrar etiquetas).

4. En la página Manage Tags (Administrar etiquetas), añada nuevas etiquetas y actualice o elimine las etiquetas existentes. Para cada nueva etiqueta, introduzca información de Key (Clave) y Value (Valor).
5. Haga clic en Apply (Aplicar) para guardar las etiquetas.

Consola original

Para etiquetar un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), seleccione el grupo de seguridad de clúster y elija Manage Tags (Administrar etiquetas).



4. En el cuadro de diálogo Manage Tags (Administrar etiquetas), realice una de las acciones siguientes:
 - Elimine una etiqueta.
 - En la sección Applied Tags (Etiquetas aplicadas), elija Delete (Eliminar) junto a la etiqueta que desea quitar.
 - Elija Apply Changes (Aplicar cambios).

Manage Tags

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn More](#) about tagging your resources.

Applied Tags

Key	Value	Delete
owner	admin	☒

Add Tags

Key	Value	
Add key	Empty value	

Cancel

Apply Changes

- Añada una etiqueta.
- En la sección Add Tags (Añadir etiquetas), escriba un par de clave/valor para la etiqueta.
- Elija Apply Changes (Aplicar cambios).

Manage Tags

Apply tags to your resources to help organize and identify them.
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn More](#) about tagging your resources.

Applied Tags

Key	Value	Delete
owner	admin	☐

Add Tags

Key	Value	
sg_type	finance	x
Add key	Empty value	

Para obtener más información acerca del etiquetado de un recurso de Amazon Redshift, consulte [Cómo administrar etiquetas en la consola de Amazon Redshift](#) (p. 504).

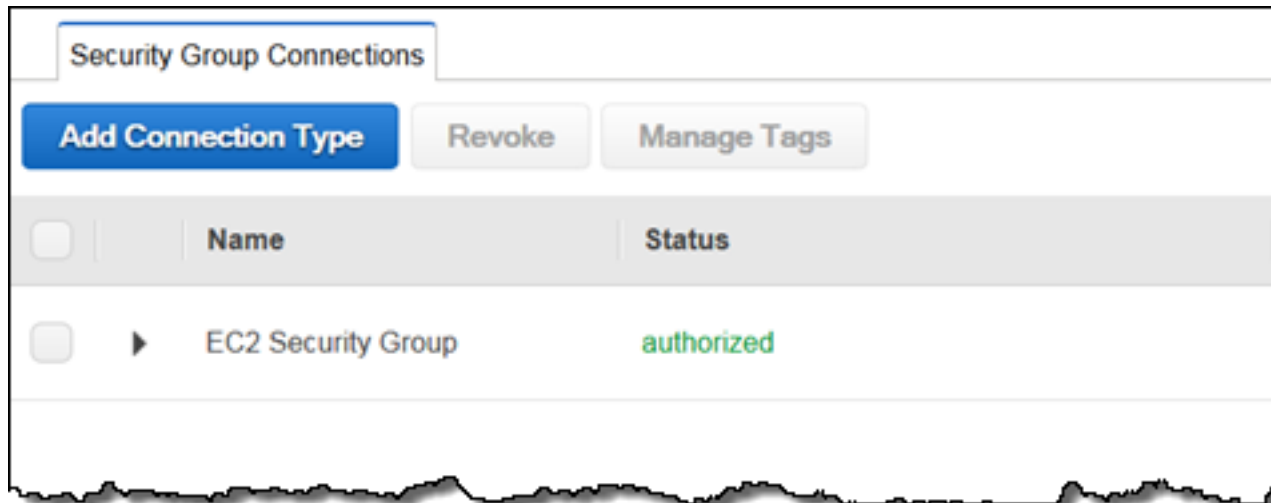
Administración de reglas de entrada para un grupo de seguridad de clúster

(Consola original) [Administrar reglas de entrada para un grupo de seguridad de clúster](#)

Para administrar reglas de entrada para un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.

2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), en la lista de grupos de seguridad del clúster, seleccione el grupo cuyas reglas desee administrar.
4. En la pestaña Security Group Connections (Conexiones del grupo de seguridad), seleccione Add Connection Type (Añadir tipo de conexión).



5. En el cuadro de diálogo Add Connection Type (Añadir tipo de conexión), realice una de las acciones siguientes:
 - Añada una regla de entrada basada en CIDR/IP:
 - En la casilla Connection Type (Tipo de conexión), seleccione CIDR/IP.
 - En el cuadro CIDR/IP to Authorize (CIDR/IP que se va a autorizar), especifique el rango.
 - Elija Authorize.

The screenshot shows the 'Add Connection Type' dialog box. It has a title bar with 'Add Connection Type' and a close button. Inside, there is a 'Connection Type' dropdown menu set to 'CIDR/IP'. Below it is a field for 'CIDR/IP of your current machine' which is empty. Then there is a field for 'CIDR/IP to Authorize*' containing the text '10.0.0.0/16'. At the bottom right, there are two buttons: 'Cancel' and 'Authorize' (highlighted in blue).

- Añada una regla de entrada basada en un grupo de seguridad de EC2:
 - En Connection Type (Tipo de conexión), seleccione EC2 Security Group (Grupo de seguridad de EC2).
 - Elija el iconoAWSPara usar. De forma predeterminada, se utiliza la cuenta con la que ha iniciado sesión en la consola actualmente. Si eligeOtra cuenta, especifique la propiedadAWSID de la cuenta de.
 - Para EC2 Security Group Name (Nombre del grupo de seguridad EC2), introduzca el nombre del grupo de seguridad EC2 que desee.
 - Elija Authorize.

Add Connection Type

Connection Type **EC2 Security Group** ▼

Account ☒ This account ☐ Another account ⓘ

Account ID

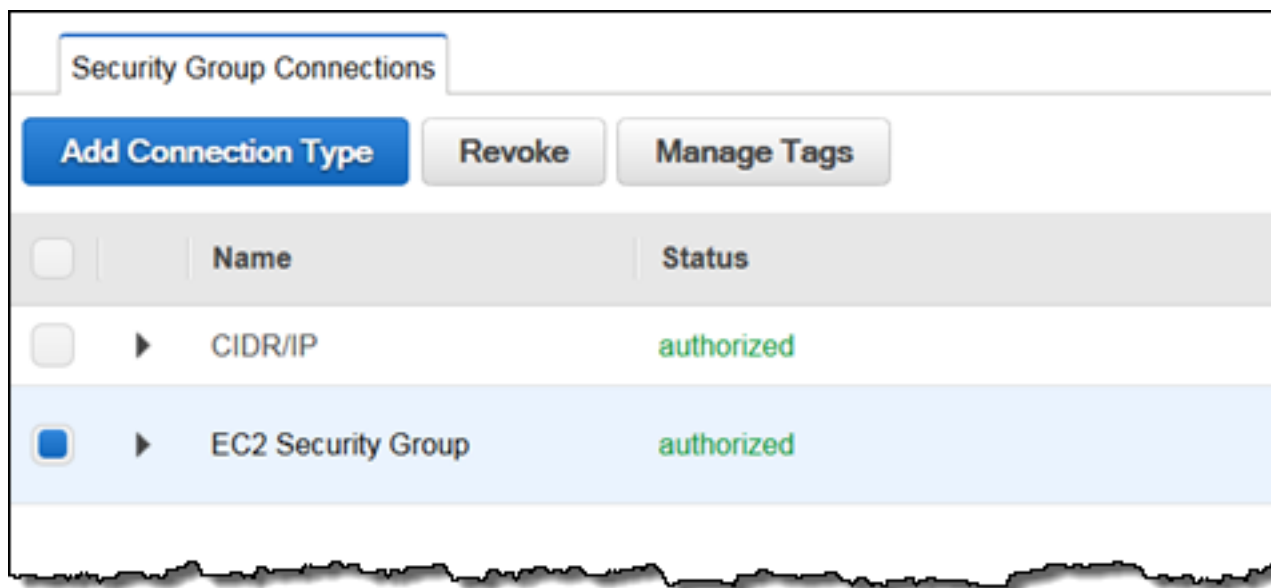
EC2 Security Group Name **default** ▼ ⓘ

Revocación de reglas de entrada para un grupo de seguridad de clúster

(Consola original) Revocar reglas de entrada para un grupo de seguridad de clúster

Para revocar reglas de entrada para un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), en la lista de grupos de seguridad del clúster, seleccione el grupo cuyas reglas desee administrar.
4. En la pestaña Security Group Connections (Conexiones con el grupo de seguridad), elija la regla que desea eliminar y seleccione Revoke (Revocar).

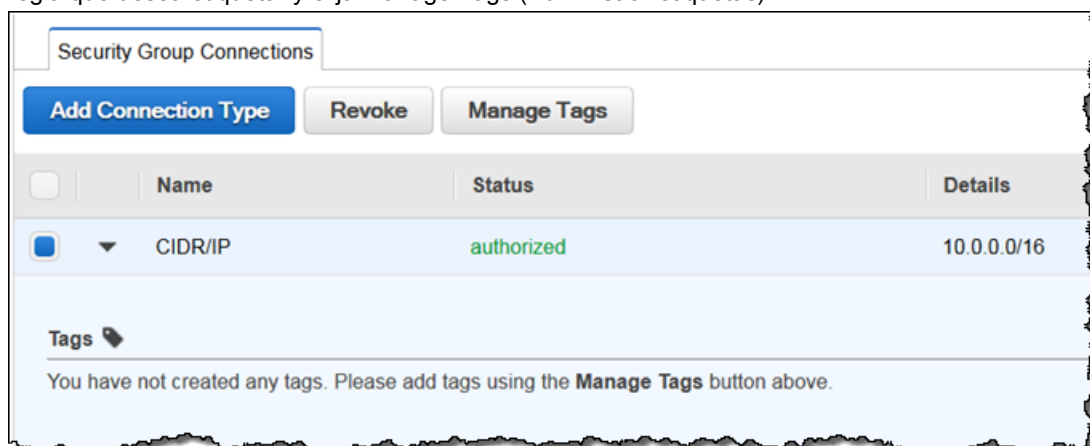


Etiquetado de reglas de entrada para un grupo de seguridad de clúster

(Consola original) Etiquetar reglas de entrada para un grupo de seguridad de clúster

Parar etiquetar reglas de entrada para un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), elija el grupo de seguridad de clúster cuyas reglas desee administrar.
4. En la pestaña Security Group Connections (Conexiones con el grupo de seguridad), seleccione la regla que desea etiquetar y elija Manage Tags (Administrar etiquetas).



5. En el cuadro de diálogo Manage Tags (Administrar etiquetas), realice una de las acciones siguientes:
 - Eliminación de una etiqueta:
 - En la sección Applied Tags (Etiquetas aplicadas), elija Delete (Eliminar) junto a la etiqueta que desea quitar.

- Elija Apply Changes (Aplicar cambios).

Manage Tags

Apply tags to your resources to help organize and identify them.
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn More](#) about tagging your resources.

Applied Tags

Key	Value	Delete
owner	admin	☒

Add Tags

Key	Value
Add key	Empty value

- Añada una etiqueta.

Note

El etiquetado de una regla de grupo de seguridad de EC2 solo etiqueta esa regla, no el grupo de seguridad de EC2 en sí. Si también desea etiquetar el grupo de seguridad de EC2, debe hacerlo por separado.

- En la sección Add Tags (Añadir etiquetas), escriba un par de clave/valor para la etiqueta.
- Elija Apply Changes (Aplicar cambios).

Manage Tags

Apply tags to your resources to help organize and identify them.
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn More](#) about tagging your resources.

Applied Tags

Key	Value	Delete
owner	admin	☐

Add Tags

Key	Value	
sg_type	finance	x
Add key	Empty value	

Para obtener más información acerca del etiquetado de un recurso de Amazon Redshift, consulte [Cómo administrar etiquetas en la consola de Amazon Redshift](#) (p. 504).

Eliminación de un grupo de seguridad de clúster

Si un grupo de seguridad de clúster está asociado a uno o más clústeres, no puede eliminarlo.

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para eliminar un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CONFIG, y seleccione Security groups (Grupos de seguridad) para mostrar la página Grupos de seguridad de clúster.

Note

Solo puede administrar grupos de seguridad de clúster cuando inicie sesión con un EC2-ClassicAWSaccount.

3. Elija el grupo de seguridad que desea eliminar y, a continuación, seleccione Delete (Eliminar).

Consola original

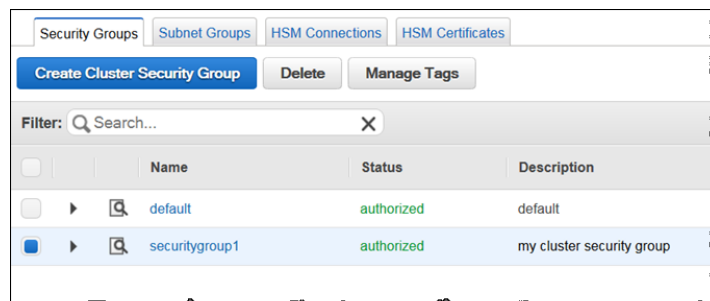
Para eliminar un grupo de seguridad de clúster

1. Inicie sesión en la enAWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Security (Seguridad).
3. En la pestaña Security Groups (Grupos de seguridad), seleccione el grupo de seguridad de clúster que desea eliminar y, a continuación, elija Delete (Eliminar).

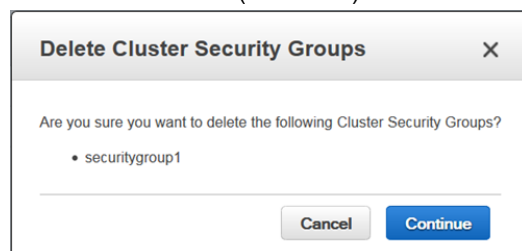
Es necesario seleccionar una fila para que se habilite el botón Delete (Eliminar).

Note

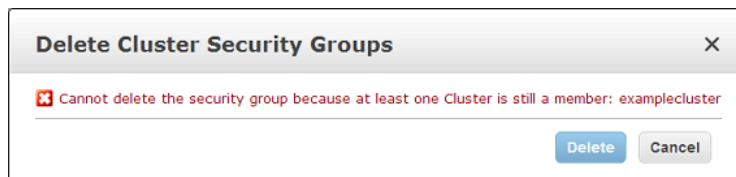
No puede eliminar el grupo de seguridad de clúster default.



4. En el cuadro de diálogo Delete Cluster Security Groups (Eliminar grupos de seguridad del clúster), seleccione Continue (Continuar).



Si el grupo de seguridad de clúster es utilizado por algún clúster, no podrá eliminarlo. En el siguiente ejemplo se muestra que securitygroup1 es utilizado por examplecluster2.



Asociación de un grupo de seguridad de clúster a un clúster

Si utiliza una plataforma EC2-VPC, consulte [Administración de grupos de seguridad de VPC para un clúster \(p. 79\)](#) para obtener más información acerca de cómo asociar grupos de seguridad de la VPC al clúster. Le recomendamos que lance el clúster en una plataforma EC2-VPC. Sin embargo, puede restaurar una instantánea EC2-Classic en un clúster EC2-VPC con la consola de Amazon Redshift. Para obtener más información, consulte [Restauración de un clúster desde una instantánea \(p. 258\)](#).

Cada clúster que aprovisiona en la plataforma EC2-Classic tiene uno o más grupos de seguridad de clúster asociados a él. Puede asociar un grupo de seguridad de clúster a un clúster cuando crea el clúster o puede asociar un grupo de seguridad de clúster más adelante mediante la modificación del clúster. Para obtener más información, consulte [Creación de un clúster mediante un lanzamiento del clúster \(p. 50\)](#) y [Pasos para modificar un clúster \(p. 60\)](#).

Administración de grupos de seguridad de clúster con la herramienta AWS SDK for Java

En el siguiente ejemplo se muestran las operaciones comunes para grupos de seguridad de clúster, incluidas:

- La creación de un nuevo grupo de seguridad de clúster.
- La adición de reglas de entrada a un grupo de seguridad de clúster.
- La asociación de un grupo de seguridad de clúster a un clúster mediante la modificación de la configuración del clúster.

De forma predeterminada, cuando se crea un nuevo grupo de seguridad de clúster, este no tiene reglas de entrada. En este ejemplo se modifica un nuevo grupo de seguridad de clúster añadiendo dos reglas de entrada. Una regla de entrada se añadió mediante la especificación de un intervalo CIDR/IP, la otra mediante la especificación de una combinación del grupo de seguridad de Amazon EC2 y el ID del propietario.

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Debe actualizar el código y proporcionar un identificador de clúster y el número de cuenta de AWS.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
```

```

*/

// snippet-sourcedescription:[CreateAndModifyClusterSecurityGroup demonstrates how to
// create and modify an Amazon Redshift security group.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[CreateClusterSecurityGroup]
// snippet-keyword:[DescribeClusterSecurityGroups]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-02-01]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.CreateAndModifyClusterSecurityGroup.complete]

package com.amazonaws.services.redshift;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

import com.amazonaws.services.redshift.model.*;

public class CreateAndModifyClusterSecurityGroup {

    public static AmazonRedshift client;
    public static String clusterSecurityGroupName = "securitygroup1";
    public static String clusterIdentifier = "****provide a cluster identifier****";
    public static String ownerID = "****provide a 12-digit account number****";

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
com.amazonaws.auth.DefaultAWSCredentialsProviderChain}
        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            createClusterSecurityGroup();
            describeClusterSecurityGroups();
            addIngressRules();
            associateSecurityGroupWithCluster();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void createClusterSecurityGroup() {
        CreateClusterSecurityGroupRequest request = new CreateClusterSecurityGroupRequest()
            .withDescription("my cluster security group")
            .withClusterSecurityGroupName(clusterSecurityGroupName);

        client.createClusterSecurityGroup(request);
        System.out.format("Created cluster security group: '%s'\n",
clusterSecurityGroupName);
    }

    private static void addIngressRules() {

        AuthorizeClusterSecurityGroupIngressRequest request = new
AuthorizeClusterSecurityGroupIngressRequest()
            .withClusterSecurityGroupName(clusterSecurityGroupName)
            .withCIDRIP("192.168.40.5/32");

        ClusterSecurityGroup result = client.authorizeClusterSecurityGroupIngress(request);
    }
}

```

```

        request = new AuthorizeClusterSecurityGroupIngressRequest()
            .withClusterSecurityGroupName(clusterSecurityGroupName)
            .withEC2SecurityGroupName("default")
            .withEC2SecurityGroupOwnerId(ownerID);
        result = client.authorizeClusterSecurityGroupIngress(request);
        System.out.format("\nAdded ingress rules to security group '%s'\n",
clusterSecurityGroupName);
        printResultSecurityGroup(result);
    }

    private static void associateSecurityGroupWithCluster() {

        // Get existing security groups used by the cluster.
        DescribeClustersRequest request = new DescribeClustersRequest()
            .withClusterIdentifier(clusterIdentifier);

        DescribeClustersResult result = client.describeClusters(request);
        List<ClusterSecurityGroupMembership> membershipList =
            result.getClusters().get(0).getClusterSecurityGroups();

        List<String> secGroupNames = new ArrayList<String>();
        for (ClusterSecurityGroupMembership mem : membershipList) {
            secGroupNames.add(mem.getClusterSecurityGroupName());
        }
        // Add new security group to the list.
        secGroupNames.add(clusterSecurityGroupName);

        // Apply the change to the cluster.
        ModifyClusterRequest request2 = new ModifyClusterRequest()
            .withClusterIdentifier(clusterIdentifier)
            .withClusterSecurityGroups(secGroupNames);

        Cluster result2 = client.modifyCluster(request2);
        System.out.format("\nAssociated security group '%s' to cluster '%s'.",
clusterSecurityGroupName, clusterIdentifier);
    }

    private static void describeClusterSecurityGroups() {
        DescribeClusterSecurityGroupsRequest request = new
DescribeClusterSecurityGroupsRequest();

        DescribeClusterSecurityGroupsResult result =
client.describeClusterSecurityGroups(request);
        printResultSecurityGroups(result.getClusterSecurityGroups());
    }

    private static void printResultSecurityGroups(List<ClusterSecurityGroup> groups)
    {
        if (groups == null)
        {
            System.out.println("\nDescribe cluster security groups result is null.");
            return;
        }

        System.out.println("\nPrinting security group results:");
        for (ClusterSecurityGroup group : groups)
        {
            printResultSecurityGroup(group);
        }
    }

    private static void printResultSecurityGroup(ClusterSecurityGroup group) {
        System.out.format("\nName: '%s', Description: '%s'\n",
group.getClusterSecurityGroupName(), group.getDescription());
        for (EC2SecurityGroup g : group.getEC2SecurityGroups()) {
            System.out.format("EC2group: '%s', '%s', '%s'\n", g.getEC2SecurityGroupName(),
g.getEC2SecurityGroupOwnerId(), g.getStatus());
        }
    }

```

```
    }  
    for (IPRange range : group.getIPRanges()) {  
        System.out.format("IPRanges: '%s', '%s'\n", range.getCIDRIP(),  
range.getStatus());  
    }  
}  
}  
// snippet-end:[redshift.java.CreateAndModifyClusterSecurityGroup.complete]
```

Administración de grupos de seguridad de clúster con la herramientaAWS CLIy Amazon Redshift API

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar los grupos de seguridad de clúster.

- [authorize-cluster-security-group-ingress](#)
- [create-cluster-security-group](#)
- [delete-cluster-security-group](#)
- [describe-cluster-security-groups](#)
- [revoke-cluster-security-group-ingress](#)

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar los grupos de seguridad de clúster.

- [AuthorizeClusterSecurityGroupIngress](#)
- [CreateClusterSecurityGroup](#)
- [DeleteClusterSecurityGroup](#)
- [DescribeClusterSecurityGroups](#)
- [RevokeClusterSecurityGroupIngress](#)

Conexión a Amazon Redshift mediante un punto de enlace de la VPC de tipo interfaz

Puede conectarse directamente al servicio API de Amazon Redshift mediante un extremo de VPC de interfaz (AWS PrivateLink) en su nube privada virtual (VPC) en lugar de conectarse a través de Internet. Para obtener información acerca de las acciones de la API de Amazon Redshift, consulte [Acciones](#) en laReferencia de la API de Amazon Redshift. Para obtener más información acerca de AWS PrivateLink , consulte [Puntos de conexión de la VPC de interfaz \(AWS PrivateLink \)](#) en laGuía del usuario de Amazon VPC. Tenga en cuenta que la conexión JDBC/ODBC al clúster no forma parte del servicio API de Amazon Redshift.

Cuando se utiliza un punto de enlace de la VPC de tipo interfaz, la comunicación entre la VPC y Amazon Redshift se realiza en su totalidad dentro delAWS, que puede proporcionar una mayor seguridad. Cada punto de enlace de la VPC está representado por una o varias interfaces de red elástica con direcciones IP privadas en las subredes de la VPC. Para obtener más información acerca de las interfaces de red elásticas, consulte [Interfaces de red elásticas](#) en laGuía del usuario de Amazon EC2 para instancias de Linux.

Un extremo de VPC de interfaz conecta la VPC directamente a Amazon Redshift. No utiliza una gateway de Internet, un dispositivo de conversión de las direcciones de red (NAT), una conexión de red virtual privada (VPN) o una conexión deAWS Direct ConnectConexión de. Las instancias de la VPC no necesitan direcciones IP públicas para comunicarse con la API de Amazon Redshift.

Para utilizar Amazon Redshift a través de su VPC, dispone de dos opciones. Una de ellas es conectarse desde una instancia que está dentro de su VPC. La otra es conectar su red privada a su VPC mediante unAWS VPNoAWS Direct Connect. Para obtener más información acerca deAWS VPN, consulte[Conexiones de VPN](#)en laGuía del usuario de Amazon VPC. Para obtener información acerca deAWS Direct Connect, consulte[Creación de una conexión](#)en laAWS Direct ConnectGuía del usuario.

Puede crear un punto de enlace de la VPC de tipo interfaz para conectarse a Amazon Redshift utilizando laAWS Management ConsoleoAWS Command Line Interface(AWS CLI). Para obtener más información, consulte [Creación de un punto de enlace de interfaz](#).

Después de crear un punto de enlace de la VPC de tipo interfaz, puede habilitar nombres de host DNS privados para el punto de enlace. Cuando lo haga, el extremo predeterminado de Amazon Redshift (<https://redshift.Region.amazonaws.com>) se resuelve en el punto de conexión de la VPC.

Si no habilita nombres de host DNS privados, Amazon VPC proporciona un nombre de punto de enlace de DNS que puede utilizar en el siguiente formato.

`VPC_endpoint_ID.redshift.Region.vpce.amazonaws.com`

Para obtener más información, consulte[Puntos de conexión de la VPC de interfaz \(AWS PrivateLink \)](#)en laGuía del usuario de Amazon VPC.

Amazon Redshift admite realizar llamadas a todas sus[Operaciones de la API](#)dentro de su VPC.

Puede asociar políticas de punto de enlace de la VPC a un punto de enlace de la VPC para controlar el acceso deAWS Identity and Access Management(IAM). También puede asociar grupos de seguridad con un punto de enlace de la VPC para controlar el acceso de entrada y salida en función del origen y el destino del tráfico de red. Un ejemplo es un rango de direcciones IP. Para obtener más información, consulte [Controlar el acceso a servicios con puntos de enlace de la VPC](#) en la Guía del usuario de Amazon VPC.

Creación de una política de puntos de enlace de la VPC para Amazon Redshift

Puede crear una política para los puntos de enlace de la VPC de Amazon Redshift de para especificar lo siguiente:

- La entidad principal que puede o no puede realizar acciones
- Las acciones que se pueden realizar
- Los recursos en los que se pueden llevar a cabo las acciones

Para obtener más información, consulte [Control del acceso a servicios con puntos de enlace de la VPC](#) en la Guía del usuario de Amazon VPC.

A continuación, encontrará ejemplos de políticas de puntos de enlace de la VPC.

Temas

- [Ejemplo: La política de puntos de enlace de la VPC para denegar todo el acceso desde unAWSaccount \(p. 407\)](#)
- [Ejemplo: Directiva de punto final de VPC para permitir el acceso de VPC sólo a una entidad de IAM especificada \(usuario\) \(p. 407\)](#)
- [Ejemplo: Política de puntos de enlace de la VPC para permitir operaciones de Amazon Redshift de solo lectura \(p. 407\)](#)
- [Ejemplo: Directiva de extremo de VPC que deniega el acceso a un clúster especificado \(p. 408\)](#)

Ejemplo: La política de puntos de enlace de la VPC para denegar todo el acceso desde unAWSaccount

La siguiente directiva de extremo de VPC deniega elAWSaccount123456789012todo el acceso a los recursos utilizando este endpoint.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    },
    {
      "Action": "*",
      "Effect": "Deny",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "123456789012"
        ]
      }
    }
  ]
}
```

Ejemplo: Directiva de punto final de VPC para permitir el acceso de VPC sólo a una entidad de IAM especificada (usuario)

La siguiente directiva de extremo de VPC permite el acceso completo sólo al usuario de IAMredshiftadmininAWSaccount123456789012. A las demás entidades principales de IAM se les deniega el acceso mediante el punto de enlace.

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/redshiftadmin"
        ]
      }
    }
  ]
}
```

Ejemplo: Política de puntos de enlace de la VPC para permitir operaciones de Amazon Redshift de solo lectura

La siguiente directiva de punto final de VPC sólo permiteAWSaccount123456789012Para realizar las acciones de Amazon Redshift especificadas.

Las acciones especificadas proporcionan el equivalente al acceso de solo lectura para Amazon Redshift. Las demás acciones en la VPC se deniegan para la cuenta especificada. Además, se deniega el acceso a

las demás cuentas. Para obtener una lista de acciones de Amazon Redshift, consulte [Claves de condición, recursos y acciones de Amazon Redshift](#) en la Guía del usuario de 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"
        ]
      }
    }
  ]
}
```

Ejemplo: Directiva de extremo de VPC que deniega el acceso a un clúster especificado

La siguiente directiva de extremo de VPC permite el acceso completo a todas las cuentas y entidades principales. Al mismo tiempo, niega cualquier acceso a `AWSaccount123456789012` a las acciones realizadas en el clúster de Amazon Redshift con ID de clúster `my-redshift-cluster`. Se siguen permitiendo otras acciones de Amazon Redshift que no admiten permisos de nivel de recursos para clústeres de. Para obtener una lista de acciones de Amazon Redshift y su correspondiente tipo de recurso, consulte [Claves de condición, recursos y acciones de Amazon Redshift](#) en la Guía del usuario de 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"
    ]
  }
}
]
```

Configuración y análisis de vulnerabilidades en Amazon Redshift

AWS gestiona las tareas de seguridad básicas como la aplicación de parches en la base de datos y el sistema operativo (SO) invitado, la configuración del firewall y la recuperación de desastres (DR). Terceros certificados han revisado estos procedimientos. Para obtener más información, consulte [Validación de la conformidad para Amazon Redshift](#) (p. 388), el [Modelo de responsabilidad compartida](#), y [Prácticas recomendadas para la seguridad, identidad y conformidad](#).

Amazon Redshift aplica actualizaciones y parches automáticamente al almacén de datos para que usted pueda centrarse en la aplicación y no en su administración. Las actualizaciones y parches se aplican durante un periodo de mantenimiento configurable. Para obtener más información, consulte [Períodos de mantenimiento](#) (p. 16).

Uso de las interfaces de administración de Amazon Redshift

Amazon Redshift admite diversas interfaces de administración que puede utilizar para crear, administrar y eliminar clústeres de Amazon Redshift: la [AWS SDK](#), el [AWS Command Line Interface \(AWS CLI\)](#) y la [API de administración de Amazon Redshift](#).

La API de Amazon Redshift Para llamar a esta API de gestión de Amazon Redshift, envíe una solicitud de. Las solicitudes son solicitudes HTTPS o HTTP que utilizan los verbos HTTP `GET` o `POST` con un parámetro de consulta denominado `Action`. Llamar a la API de Amazon Redshift es la forma más directa de obtener acceso al servicio de Amazon Redshift. No obstante, esto requiere que la aplicación controle niveles de detalle de bajo nivel, tales como el control de errores y la generación del código hash para firmar la solicitud.

- Para obtener información acerca de la creación y la firma de una solicitud de la API de Amazon Redshift, consulte [Firma de una solicitud HTTP](#) (p. 413).
- Para obtener información sobre las acciones de la API de Amazon Redshift y los tipos de datos de Amazon Redshift, consulte la [Referencia de la API de Amazon Redshift](#).

AWS SDK de— Puede utilizar la herramienta de [AWS SDK](#) para realizar operaciones relacionadas con clústeres de Amazon Redshift. Varias de las bibliotecas del SDK integran la API de Amazon Redshift de subyacente. Los SDK integran la funcionalidad de la API en el lenguaje de programación específico y administran varios de los detalles de bajo nivel, como el cálculo de firmas, el control de reintentos de solicitud y el control de errores. Llamar a las funciones contenedora en las bibliotecas del SDK puede simplificar enormemente el proceso de escritura de una aplicación para administrar un clúster de Amazon Redshift.

- Amazon Redshift es compatible con el [AWS SDK](#) para Java, .NET, PHP, Python, Ruby y Node.js. Las funciones contenedora para Amazon Redshift se documentan en el manual de referencia de cada SDK. Para obtener una lista de los [AWS SDK](#) y enlaces a la documentación, consulte [Herramientas para Amazon Web Services](#).
- En esta guía se proporcionan ejemplos de cómo trabajar con Amazon Redshift mediante el SDK de Java. Para ver ejemplos de código del SDK de AWS más generales, consulte [Código de muestra y bibliotecas](#).

AWS CLI— La CLI proporciona un conjunto de herramientas de línea de comandos de la que puede utilizar para administrar [AWS Servicios de equipos](#) Windows, Mac y Linux. La [AWS CLI](#) contiene comandos relacionados con las acciones de la API de Amazon Redshift.

- Para obtener información acerca de la instalación y configuración de la CLI de Amazon Redshift, consulte [Configuración de la CLI de Amazon Redshift](#) (p. 415).
- Para obtener material de referencia sobre los comandos de la CLI de Amazon Redshift, consulte [Amazon Redshift en la AWS CLI Referencia de](#).

Temas

- [Mediante la AWS SDK for Java en Amazon Redshift](#) (p. 411)
- [Firma de una solicitud HTTP](#) (p. 413)

- [Configuración de la CLI de Amazon Redshift \(p. 415\)](#)

Mediante la AWS SDK for Java en Amazon Redshift

AWS SDK for Java proporciona una clase llamada `AmazonRedshiftClientBuilder`, que puede utilizar para interactuar con Amazon Redshift. Para obtener información sobre la descarga del AWS SDK for Java, consulte [AWS SDK for Java](#).

Note

La AWS SDK for Java proporciona clientes seguros para subprocessos con el fin de obtener acceso a Amazon Redshift. Como práctica recomendada, sus aplicaciones deben crear un cliente y reutilizar el cliente entre subprocessos.

Puede utilizar las clases `AmazonRedshiftClientBuilder` y `AwsClientBuilder` para configurar un punto de enlace y crear un cliente de Amazon Redshift. Puede utilizar el objeto de cliente para crear una instancia del objeto `Cluster`. El objeto `Cluster` contiene métodos que coinciden con las acciones de la API de consulta de Amazon Redshift. (Estas acciones se describen en [Referencia de la API de Amazon Redshift](#)). Cuando llama a un método, debe crear el objeto de solicitud correspondiente. El objeto de solicitud incluye la información que debe transmitirse con la solicitud real. El objeto `Cluster` proporciona la información que devuelve Amazon Redshift en respuesta a la solicitud.

En el ejemplo siguiente, se muestra cómo utilizar la clase `AmazonRedshiftClientBuilder` para configurar un punto de enlace y, a continuación, crear un clúster `ds2.xlarge` de dos nodos.

```
String endpoint = "https://redshift.us-east-1.amazonaws.com/";
String region = "us-east-1";
AwsClientBuilder.EndpointConfiguration config = new
    AwsClientBuilder.EndpointConfiguration(endpoint, region);
AmazonRedshiftClientBuilder clientBuilder = AmazonRedshiftClientBuilder.standard();
clientBuilder.setEndpointConfiguration(config);
AmazonRedshift client = clientBuilder.build();

CreateClusterRequest request = new CreateClusterRequest()
    .withClusterIdentifier("exampleclusterusingjava")
    .withMasterUsername("masteruser")
    .withMasterUserPassword("12345678Aa")
    .withNodeType("ds2.xlarge")
    .withNumberOfNodes(2);

Cluster createResponse = client.createCluster(request);
System.out.println("Created cluster " + createResponse.getClusterIdentifier());
```

Ejecución de ejemplos de Java para Amazon Redshift con Eclipse

Proceso general de ejecución de ejemplos de código Java con Eclipse

1. Creación de un nuevo `AWS Proyecto Java` en Eclipse.

Siga los pasos de [Configuración de la AWS Toolkit for Eclipse](#) en la `AWS Toolkit for Eclipse` Guía de introducción.

2. Copie el código de muestra de la sección de este documento que está leyendo y péguelo en su proyecto como un archivo de clase de Java nuevo.
3. Ejecute el código.

Ejecución de ejemplos de Java para Amazon Redshift desde la línea de comando

Proceso general de ejecución de ejemplos de código Java desde la línea de comando

1. Configure y pruebe su entorno de la siguiente manera:
 - a. Cree un directorio para trabajar y cree en él las subcarpetas `src` `bin` y `sdk`.
 - b. Descargue AWS SDK para Java y descomprímalo en la subcarpeta `sdk` que creó anteriormente. Después de descomprimir el Software Development Kit (SDK, Kit de desarrollo de software) debería tener cuatro subdirectorios en la carpeta `sdk`, que incluyen una carpeta `lib` y una `third-party`.
 - c. Proporcione su AWS para el SDK for Java. Para obtener más información, consulte [Proporcionar AWS en la AWS SDK for Java](#) en la AWS SDK for Java Guía para desarrolladores.
 - d. Asegúrese de poder ejecutar el compilador de programa de Java (`javac`) y el iniciador de aplicaciones de Java (`java`) desde su directorio de trabajo. Puede probarlos ejecutando los siguientes comandos:

```
javac -help
java -help
```

2. Ingrese el código que desea ejecutar en un archivo `.java` y guarde el archivo en la carpeta `src`. Para ilustrar el proceso, utilizamos el código de [Administración de grupos de seguridad de clúster con la herramienta AWS SDK for Java \(p. 402\)](#) para que el archivo del directorio `src` sea `CreateAndModifyClusterSecurityGroup.java`.
3. Compile el código.

```
javac -cp sdk/lib/aws-java-sdk-1.3.18.jar -d bin src
\CreateAndModifyClusterSecurityGroup.java
```

Si usa una versión diferente de la AWS SDK for Java, ajuste la ruta de clase (`-cp`) para su versión.

4. Ejecute el código. En el siguiente comando, se añaden saltos de línea para facilitar la lectura.

```
java -cp "bin;
sdk/lib/*;
sdk/third-party/commons-logging-1.1.1/*;
sdk/third-party/httpcomponents-client-4.1.1/*;
sdk/third-party/jackson-core-1.8/*"
CreateAndModifyClusterSecurityGroup
```

Cambie el separador de la ruta de clases según lo necesite para su sistema operativo. Por ejemplo, para Windows, el separador es ";" (tal y como se muestra) y para Unix es ":". Otros ejemplos de códigos pueden requerir más bibliotecas que las que se muestran en este ejemplo o la versión de la AWS SDK con el que está trabajando puede tener diferentes nombres de carpetas de terceros. Para estos casos, ajuste el classpath (`-cp`) según corresponda.

Para ejecutar muestras en este documento, utilice una versión de la AWS SDK compatible con Amazon Redshift. Para obtener la versión más reciente de la AWS SDK for Java, vaya a [AWS SDK for Java](#).

Configuración del punto de enlace

De forma predeterminada, AWS SDK for Java utiliza el punto de enlace `https://redshift.us-east-1.amazonaws.com/`. Puede configurar el punto de enlace de forma explícita con el método `client.setEndpoint`, tal como se muestra en el siguiente fragmento de código Java.

Example

```
client = new AmazonRedshiftClient(credentials);  
client.setEndpoint("https://redshift.us-east-1.amazonaws.com/");
```

Para obtener una lista de AWS en las que puede aprovisionar un clúster, vaya a [la Regiones y puntos de enlace](#) en la sección [Glosario de Amazon Web Services](#).

Firma de una solicitud HTTP

Amazon Redshift requiere que cada solicitud que envía a la API de administración se autentique con una firma. En este tema, se explica cómo firmar solicitudes.

Si está utilizando uno de los AWS Kits de desarrollo de software (SDK) o el AWS Command Line Interface, la firma de solicitudes se maneja automáticamente y puede omitir esta sección. Para obtener más información acerca del uso de AWS SDK, consulte [Uso de las interfaces de administración de Amazon Redshift \(p. 410\)](#). Para obtener más información acerca del uso de la interfaz de línea de comandos de Amazon Redshift, visite [Referencia de la línea de comandos de Amazon Redshift](#).

Para firmar una solicitud, se calcula una firma digital mediante una función hash criptográfica. Un hash criptográfico es una función que devuelve un valor hash único que se basa en la entrada. La entrada a la función hash incluye el texto de la solicitud y la clave de acceso secreta. La función hash devuelve un valor hash que se incluye en la solicitud como la firma. La firma forma parte del encabezado de la `Authorization` de la solicitud.

Note

Para acceder a la API, necesita un ID de clave de acceso y una clave de acceso secreta. Utilice las claves de acceso de usuario de IAM en lugar de AWS las claves de acceso de usuario de la cuenta de Para obtener más información sobre la creación de claves de acceso, consulte [Administración de las claves de acceso de los usuarios de IAM](#) en la Guía del usuario de IAM

Tras Amazon Redshift solicitud, recalcula la firma utilizando la misma función hash y los datos que ha introducido para firmar la solicitud. Si la firma resultante coincide con la firma de la solicitud, Amazon Redshift procesa la solicitud; de lo contrario, la solicitud se rechaza.

Amazon Redshift admite la autenticación mediante [AWS Signature Version 4](#). El proceso para calcular una firma se compone de tres tareas. Estas se ilustran en el siguiente ejemplo.

- [Tarea 1: Crear una solicitud canónica](#)

Reorganice la solicitud HTTP en forma canónica. Es preciso utilizar un formato canónico, ya que Amazon Redshift utiliza el mismo formato canónico para calcular la firma que compara con la que ha enviado.

- [Tarea 2: Crear una cadena para firmar](#)

Crear una cadena que se utilizará como uno de los valores de entrada de la función hash criptográfica. La cadena, denominada cadena para firmar, es una concatenación del nombre del algoritmo hash, la fecha de la solicitud, una cadena de ámbito de credenciales y la solicitud en formato canónico de la tarea anterior. La cadena del ámbito de credenciales es una concatenación de fecha, región e información del servicio.

- [Tarea 3: Creación de una firma](#)

Cree una firma para la solicitud utilizando una función hash criptográfica que acepte dos cadenas de entrada: la cadena para firmar y una clave derivada. La clave derivada se calcula a partir de la clave de acceso secreta, utilizando el ámbito de credencial para crear una serie de códigos de autenticación de mensajes basados en hash (HMAC-SHA256).

Ejemplo de cálculo de firma

En el siguiente ejemplo, se presentan los detalles de la creación de una firma de una solicitud [CreateCluster](#). Puede utilizar el ejemplo como referencia para comprobar su propio método de cálculo de firmas. Encontrará otros cálculos de referencia en [Conjunto de pruebas de Signature Version 4](#), en el Glosario de Amazon Web Services.

Puede utilizar una solicitud GET o POST para enviar solicitudes a Amazon Redshift. La diferencia entre las dos solicitudes es que con la solicitud GET los parámetros se envían como parámetros de cadena de consulta. Con la solicitud POST, las firmas se incluyen en el cuerpo de la solicitud. En el ejemplo a continuación, se presenta una solicitud POST.

El ejemplo supone lo siguiente:

- La marca temporal de la solicitud es `Fri, 07 Dec 2012 00:00:00 GMT`.
- El punto de enlace es la región EE. UU. Este (Norte de Virginia), `us-east-1`.

La sintaxis general de la solicitud es la siguiente:

```
https://redshift.us-east-1.amazonaws.com/  
  ?Action=CreateCluster  
  &ClusterIdentifier=examplecluster  
  &MasterUsername=masteruser  
  &MasterUserPassword=12345678Aa  
  &NumberOfNode=2  
  &NodeType=ds2.xlarge  
  &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
```

El formato canónico de la solicitud calculado para [Tarea 1: Creación de una solicitud canónica \(p. 413\)](#) es:

```
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
```

La última línea de la solicitud canónica es el hash del cuerpo de la solicitud. La tercera línea de la solicitud canónica se encuentra vacía porque no hay parámetros de consulta para esta API.

La cadena para firmar para [Tarea 2: Creación de una cadena para firmar \(p. 413\)](#) es:

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

La primera línea de la cadena para firmar es el algoritmo, la segunda línea es la marca de tiempo, la tercera línea es el ámbito de las credenciales, y la última línea es un hash de la solicitud canónica de [Tarea 1: Creación de una solicitud canónica \(p. 413\)](#). El nombre del servicio que se va a utilizar en el ámbito de credenciales es `redshift`.

Para [Tarea 3: Creación de una firma \(p. 413\)](#) En la clave derivada se puede representar como sigue:

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

La clave derivada se calcula como series de funciones hash. A partir de la instrucción HMAC interna en la fórmula anterior, concatenar la frase **AWS4** Con su clave de acceso secreta y úsela como la clave para resumir los datos «us-east-1». El resultado de esta hash se convierte en la clave para la siguiente función hash.

Tras calcular la clave derivada, se usa en una función hash que acepte dos cadenas de entrada: la cadena para firmar y la clave derivada. Por ejemplo, si usa la clave de acceso secreta `wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY` y la cadena para firmar provistas anteriormente, la firma calculada es la siguiente:

```
9a6b557aa9f38dea83d9215d8f0eae54100877f3e0735d38498d7ae489117920
```

El último paso consiste en construir el encabezado `Authorization`. Para la clave de acceso de demostración `AKIAIOSFODNN7EXAMPLE`, el encabezado (al que se han agregado saltos de línea para que resulte más legible) es el siguiente:

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

Configuración de la CLI de Amazon Redshift

En esta sección, se explica cómo configurar y ejecutar la herramienta de `AWS CLI` herramientas de línea de comandos para su uso en la gestión de Amazon Redshift. Las herramientas de línea de comandos de Amazon Redshift se ejecutan en el `AWS Command Line Interface (AWS CLI)`, que a su vez usa Python (<https://www.python.org/>). La `AWS CLI` se puede ejecutar en cualquier sistema operativo que admita Python.

Instrucciones de instalación

Para comenzar a utilizar las herramientas de línea de comandos de Amazon Redshift, primero configure la propiedad de `AWS CLI` y añada los archivos de configuración que definen las opciones de la CLI de Amazon Redshift.

Si ya instaló y configuró la `AWS CLI` para otro producto de AWS, puede omitir este procedimiento.

Para instalar `AWS Command Line Interface`

1. Vaya a [Configuración inicial de la interfaz de línea de comandos de AWS](#) y luego siga las instrucciones para instalar la `AWS CLI`.

Para acceder a la CLI de, necesita un ID de clave de acceso de y una clave de acceso secreta de. Utilice las claves de acceso de usuario de IAM en lugar de `AWS` claves de acceso de usuario de la cuenta raíz de IAM le permite controlar de forma segura el acceso a `AWS` Servicios y recursos de su cuenta de `AWS` account. Para obtener más información acerca de la creación de claves de acceso de, consulte [Entender y obtener sus credenciales de seguridad de](#) en la `AWS` Referencia general de.

2. Cree un archivo que contenga la información de configuración, como las claves de acceso, la región predeterminada y el formato de salida de comandos. Luego, establezca la variable de entorno `AWS_CONFIG_FILE` para que haga referencia a ese archivo. Para obtener instrucciones

detalladas, visite [Configuración de la interfaz de línea de comandos de la AWS Command Line Interface](#) Guía del usuario de .

3. Ejecute un comando de prueba para confirmar que la AWS CLI está funcionando. Por ejemplo, el siguiente comando debe mostrar información de ayuda para la AWS CLI:

```
aws help
```

El siguiente comando debe mostrar información de ayuda para Amazon Redshift:

```
aws redshift help
```

Para obtener material de referencia sobre los comandos de la CLI de Amazon Redshift, consulte [Amazon Redshift en la AWS CLI](#) Referencia de .

Introducción al AWS Command Line Interface

Para ayudarle a comenzar a utilizar la herramienta de AWS Command Line Interface (AWS CLI), en esta sección se muestra cómo realizar tareas administrativas básicas para un clúster de Amazon Redshift. Estas tareas son muy similares a las de la lista del [Introducción a Amazon Redshift](#), pero se centran en el AWS CLI en lugar de la consola de Amazon Redshift.

En esta sección se enseñan los procesos de creación de un clúster, creación de tablas de base de datos, carga de datos y prueba de consultas. La AWS CLI se utiliza para aprovisionar un clúster y autorizar los permisos de acceso necesarios. Luego, utilizará el cliente SQL Workbench para conectarse al clúster y crear tablas de ejemplo, cargar datos de ejemplo y ejecutar consultas de prueba.

Paso 1: Antes de empezar

Si aún no tiene una AWS, debe inscribirse para obtener una. A continuación, deberá configurar las herramientas de línea de comandos de Amazon Redshift. Por último, necesitará descargar los controladores y las herramientas del cliente para conectarse al clúster.

Paso 1.1: Inscribirse en una cuenta de AWS

Para obtener información acerca de la inscripción en una AWS, consulte la [Guía de introducción a Amazon Redshift](#).

Paso 1.2: Descargue e instale la AWS CLI

Si no ha instalado la AWS CLI, consulte [Configuración de la CLI de Amazon Redshift \(p. 415\)](#).

Paso 1.3: Descargue los controladores y las herramientas del cliente

Puede utilizar cualquier herramienta de cliente SQL para conectarse a un clúster de Amazon Redshift con los controladores JDBC u ODBC de PostgreSQL. Si no tiene dicho software instalado, puede usar SQL Workbench, una herramienta multiplataforma gratuita para consultar tablas en un clúster de Amazon Redshift. Los ejemplos de esta sección utilizarán el cliente SQL Workbench.

Para descargar SQL Workbench y los controladores de PostgreSQL, consulte la sección de [Guía de introducción a Amazon Redshift](#).

Paso 2: Lance un clúster

Ahora ya está listo para lanzar un clúster mediante la AWS CLI.

Important

El clúster que está por lanzar se ejecutará en un entorno real (no en uno de prueba). Deberá pagar las tarifas de uso estándares por el clúster hasta que lo elimine. Para obtener información acerca de los precios, visite [la página de precios de Amazon Redshift](#).

Si completa el ejercicio descrito aquí de una vez y elimina el clúster cuando finaliza, los cargos totales serán mínimos.

El comando `create-cluster` tiene una gran cantidad de parámetros. Para este ejercicio, utilizará los valores del parámetro que se describen en la siguiente tabla. Antes de crear un clúster en un entorno de producción, le recomendamos revisar todos los parámetros opcionales y obligatorios para que la configuración del clúster cumpla con los requisitos. Para obtener más información, consulte [create-cluster](#).

Nombre del parámetro	Valor del parámetro para este ejercicio
Cluster Identifier (Identificador del clúster)	<code>examplecluster</code>
Master Username (Nombre de usuario maestro)	<code>masteruser</code>
Master Password (Contraseña maestra)	<code>TopSecret1</code>
Node Type	<code>ds2.xlarge</code> o el tamaño de nodo que desea utilizar. Para obtener más información, consulte Clusters y nodos en Amazon Redshift (p. 5)
Cluster Type (Tipo de clúster)	<code>single-node</code>

Escriba el siguiente comando para crear el clúster.

```
aws redshift create-cluster --cluster-identifier examplecluster --master-username
masteruser --master-user-password TopSecret1 --node-type ds2.xlarge --cluster-type single-
node
```

El proceso de creación de clúster tardará varios minutos en completarse. Escriba el siguiente comando para comprobar el estado.

```
aws redshift describe-clusters --cluster-identifier examplecluster
```

El resultado tendrá un aspecto similar al siguiente:

```
{
  "Clusters": [
    {
      ...output omitted...

      "ClusterStatus": "creating",
      "ClusterIdentifier": "examplecluster",

      ...output omitted...
    }
  ]
}
```

Cuando el campo `ClusterStatus` cambia de `creating` a `available`, ya se puede utilizar el clúster.

En el próximo paso, autorizará el acceso para poder conectarse al clúster.

Paso 3: Autorizar tráfico entrante para el acceso al clúster

Debe conceder explícitamente acceso entrante en el cliente para poder conectarse al cluster. Su cliente puede ser una instancia de Amazon EC2 o un equipo externo.

Cuando creó un clúster en el paso anterior, debido a que no especificó un grupo de seguridad, asoció el grupo de seguridad de clúster predeterminado con el clúster. El grupo de seguridad de clúster predeterminado no contiene reglas para autorizar tráfico entrante al clúster. Para obtener acceso al nuevo clúster, debe añadir reglas para el tráfico entrante, que son llamadas reglas de entrada, al grupo de seguridad de clúster.

Reglas de entrada para aplicaciones que se ejecutan en Internet

Si obtiene acceso al clúster desde Internet, necesitará autorizar un rango de dirección IP de enrutamiento entre dominios sin clases (CIDR/IP). Por ejemplo, utilizaremos una regla CIDR/IP de 192.0.2.0/24; necesitará modificar este rango para reflejar la dirección IP y máscara de red reales.

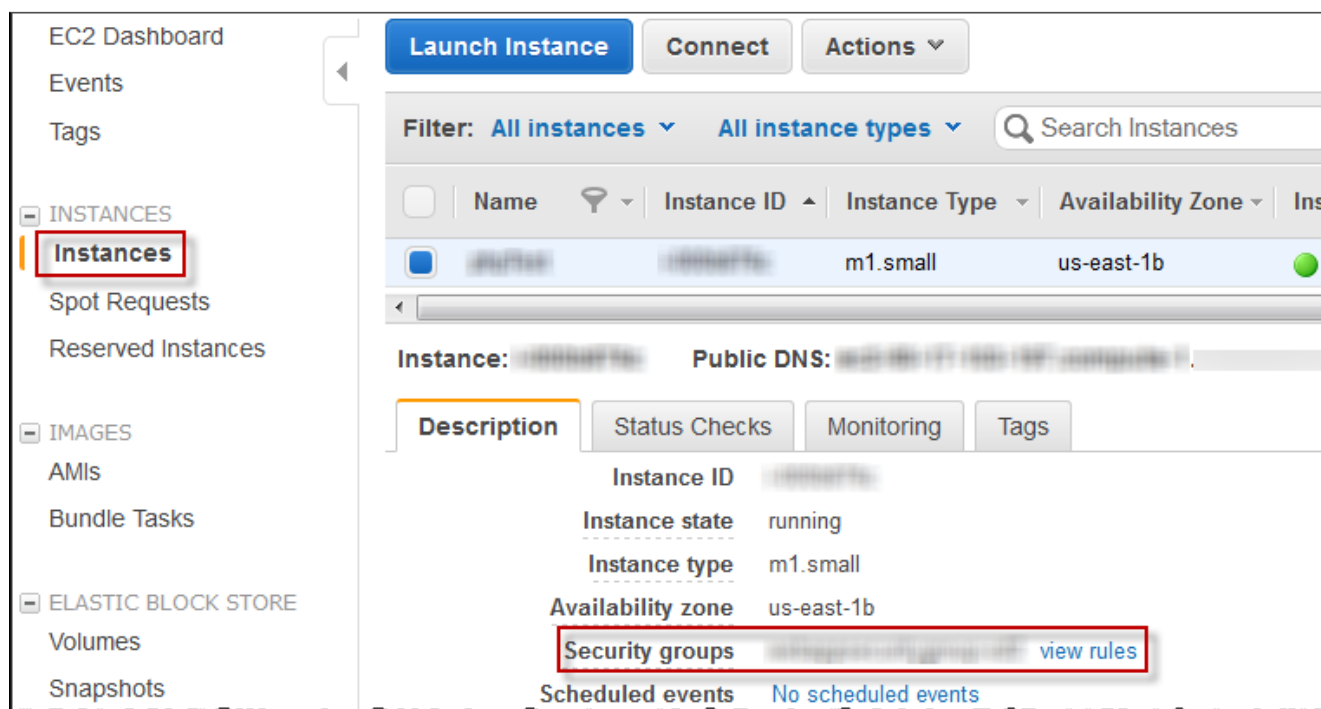
Para habilitar acceso a la red en el clúster, escriba el siguiente comando:

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name default  
--cidrip 192.0.2.0/24
```

Reglas de entrada para instancias EC2

Si obtiene acceso al clúster desde una instancia de Amazon EC2, tendrá que autorizar un grupo de seguridad de Amazon EC2. Para hacerlo, especifique el nombre del grupo de seguridad, junto con el número de cuenta de 12 dígitos del propietario del grupo de seguridad de EC2.

Puede utilizar la consola de Amazon EC2 para determinar el grupo de seguridad de EC2 asociado a la instancia:



Para buscar su AWS número de cuenta, vaya a <https://aws.amazon.com/> e inicie sesión en la página Mi cuenta de. Sus AWS En la esquina superior derecha de esa página, aparece el número de cuenta de.

Para este ejemplo, usaremos `myec2securitygroup` Para obtener el nombre del grupo de seguridad de Amazon EC2, y `123456789012` Para obtener el número de cuenta de. Deberá modificar estos valores en función de sus necesidades.

Para habilitar acceso a la red en el clúster, escriba el siguiente comando:

```
aws redshift authorize-cluster-security-group-ingress --cluster-security-group-name default --ec2-security-group-name myec2securitygroup --ec2-security-group-owner 123456789012
```

Paso 4: Connect al clúster

Ahora que ha añadido una regla de entrada al grupo de seguridad de clúster, se autorizan las conexiones entrantes de una CIDR/IP específica o un grupo de seguridad de EC2 a `examplecluster`.

Ahora ya puede conectarse al clúster.

Para obtener información acerca de cómo conectarse al clúster, visite la página de [Guía de introducción a Amazon Redshift](#).

Paso 5: Crear tablas, cargar datos e intentar consultas de ejemplo

Para obtener información acerca de la creación de tablas, carga de datos y emisión de consultas, diríjase al [Introducción a Amazon Redshift](#).

Paso 6: Elimine el clúster de ejemplo

Después de haber lanzado un clúster y de que esté disponible, se le facturará el tiempo de ejecución del clúster, incluso si no lo está utilizando activamente. Cuando ya no necesite el clúster, puede eliminarlo.

Cuando elimina un clúster, debe decidir si desea crear una instantánea final. Debido a que este es un ejercicio y el clúster de ejemplo no debería contener datos importantes, puede omitir la instantánea final.

Para eliminar el clúster, escriba siguiente comando.

```
aws redshift delete-cluster --cluster-identifier examplecluster --skip-final-cluster-snapshot
```

¡Enhorabuena! Lanzó, autorizó el acceso a, se conectó a y eliminó un clúster correctamente.

Supervisión del rendimiento del clúster de Amazon Redshift

Amazon Redshift proporciona métricas y datos de rendimiento para que pueda registrar el rendimiento y el estado de sus clústeres y bases de datos. En esta sección, analizaremos los tipos de datos con los que puede trabajar en Amazon Redshift, específicamente en la consola de Amazon Redshift.

Temas

- [Overview \(p. 421\)](#)
- [Supervisión de Amazon Redshift mediante las métricas de CloudWatch \(p. 422\)](#)
- [Uso de los datos de rendimiento en la consola de Amazon Redshift \(p. 430\)](#)

Overview

Los datos de rendimiento que puede utilizar en la consola de Amazon Redshift se dividen en dos categorías:

- **Métricas de Amazon CloudWatch** Métricas de Amazon CloudWatch ayudan a monitorear los aspectos físicos del clúster, como la utilización de la CPU, la latencia y el desempeño. Los datos de métricas se muestran directamente en la consola de Amazon Redshift. También puede verlos en la consola de CloudWatch. De modo alternativo, puede consumirlos de cualquier otra forma en la que trabaje con métricas, como en la AWS CLI o una de las AWS SDK.
- **Datos de rendimiento de cargas/consultas:** Los datos de rendimiento le ayudan a supervisar la actividad y el rendimiento de la base. Estos datos se incorporan en la consola de Amazon Redshift para que le resulte fácil correlacionar lo que ve en las métricas de CloudWatch con eventos de carga y consulta específicos de la base de datos. También puede crear sus propias consultas de rendimiento personalizadas y ejecutarlas directamente en la base de datos. Los datos de rendimiento de cargas y consultas se muestran únicamente en la consola de Amazon Redshift. No se publican como métricas de CloudWatch.

Los datos de rendimiento se acumulan en la consola de Amazon Redshift, lo que produce una mejor experiencia de las siguientes maneras:

- Los datos de rendimiento asociados a un clúster se muestran de forma contextual cuando ve un clúster, caso en el que es posible que los necesite para tomar decisiones sobre el clúster, como cambiar el tamaño.
- Algunas métricas de desempeño se muestran en unidades con escalas más adecuadas en la consola de Amazon Redshift que en CloudWatch. Por ejemplo, `WriteThroughput` se muestra en GB/s (mientras que en lo hace en bytes/s de CloudWatch), que es una unidad más pertinente para el espacio de almacenamiento normal de un nodo.
- Puede visualizar fácilmente los datos de rendimiento de los nodos de un clúster conjuntamente en el mismo gráfico. De este modo, podrá monitorear de forma sencilla el rendimiento de todos los nodos de un clúster. También puede ver los datos de rendimiento de cada nodo.

Amazon Redshift proporciona datos de rendimiento (tanto las métricas de CloudWatch como los datos de cargas y consultas) sin ningún cargo adicional. Los datos de rendimiento se registran cada minuto. Puede obtener acceso a los valores históricos de los datos de rendimiento en la consola de Amazon Redshift. Para obtener información detallada acerca del uso de CloudWatch para obtener acceso a los

datos de rendimiento de Amazon Redshift que se exponen como métricas de CloudWatch, consulte [¿Qué es CloudWatch?](#) en la Guía del usuario de Amazon CloudWatch.

Supervisión de Amazon Redshift mediante las métricas de CloudWatch

Mediante las métricas de CloudWatch para Amazon Redshift, puede obtener información sobre el rendimiento y el estado del clúster y ver información en el nivel del nodo. Al trabajar con estas métricas, hay que recordar que cada métrica tiene una o más dimensiones asociadas. Estas dimensiones le indican a qué es aplicable la métrica, es decir, el alcance de la métrica. Amazon Redshift tiene las dos dimensiones siguientes:

- Las métricas que tienen una dimensión `NodeID` son métricas que proporcionan los datos de rendimiento de los nodos de un clúster. Este conjunto de métricas incluye el nodo principal y los de computación. Entre los ejemplos de estas métricas se incluyen `CPUUtilization`, `ReadIOPS` y `WriteIOPS`.
- Las métricas que tienen solo una dimensión `ClusterIdentifier` son métricas que proporcionan datos de rendimiento de los clústeres. Entre los ejemplos de estas métricas se incluyen `HealthStatus` y `MaintenanceMode`.

Note

En algunos casos de métricas, una métrica específica del clúster representa una acumulación del comportamiento de los nodos. En estos casos, hay que prestar especial atención al interpretar el valor de las métricas, ya que el comportamiento del nodo principal se agrega al del nodo de computación.

Para obtener información general acerca de las dimensiones y las métricas de CloudWatch, consulte [Conceptos CloudWatch](#) en la Guía del usuario de Amazon CloudWatch.

Para obtener más detalles sobre las métricas de CloudWatch para Amazon Redshift, consulte las siguientes secciones.

Temas

- [Métricas de Amazon Redshift \(p. 422\)](#)
- [Dimensiones de métricas de Amazon Redshift \(p. 428\)](#)
- [Datos de rendimiento de carga y consultas de Amazon Redshift \(p. 429\)](#)

Métricas de Amazon Redshift

El espacio de nombres de `AWS/Redshift` incluye las siguientes métricas. A menos que se indique lo contrario, las métricas se recopilan en intervalos de 1 minuto.

Title

Métrica	Descripción
<code>CommitQueueLength</code>	El número de transacciones en espera de confirmación en un momento determinado. Unidades: Recuento Dimensiones: <code>ClusterIdentifier</code>

Métrica	Descripción
ConcurrencyScalingActiveClusters	El número de clústeres de escalado de simultaneidad que procesan activamente consultas en un momento dado. Unidades: Recuento Dimensiones: ClusterIdentifier
ConcurrencyScalingSeconds	El número de segundos usados por los clústeres de escalado de simultaneidad que tienen actividad de procesamiento de consultas activas. Unidades: Sum Dimensiones: ClusterIdentifier
CPUUtilization	El porcentaje de utilización de CPU. Para los clústeres, esta métrica representa la suma de los valores de utilización de CPU de todos los nodos (principales y de computación). Unidades: Porcentaje Dimensiones: ClusterIdentifier, NodeID Dimensiones: ClusterIdentifier
DatabaseConnections	El número de conexiones de base de datos a un clúster. Unidades: Recuento Dimensiones: ClusterIdentifier
HealthStatus	Indica el estado del clúster. Cada minuto el clúster se conecta a su base de datos y realiza una consulta sencilla. Si puede realizar esta operación correctamente, se considera que el clúster está en buen estado. De lo contrario, se considera que el clúster está en mal estado. Un estado incorrecto se puede producir cuando la base de datos del clúster está sobrecargada en exceso o cuando hay un problema de configuración con una base de datos del clúster. Note En Amazon CloudWatch, esta métrica se registra como 1 o 0, mientras que en la consola de Amazon Redshift se muestra con las palabras HEALTHY o UNHEALTHY para mayor comodidad. Cuando esta métrica se muestra en la consola de Amazon Redshift, se omiten los promedios de muestreo y solo HEALTHY o UNHEALTHY se muestran. En Amazon CloudWatch, pueden aparecer otros valores además de 0 y 1 por cuestiones de muestreo. Cualquier valor inferior a 1 para HealthStatus se registra como 0 (UNHEALTHY). Unidades: Recuento (1/0) (HEALTHY/UNHEALTHY en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier

Métrica	Descripción
MaintenanceMode	Indica si los datos del clúster se encuentran en modo de mantenimiento. Note En Amazon CloudWatch, esta métrica se registra como 1 o 0, mientras que en la consola de Amazon Redshift se muestra con las palabras ON o OFF para mayor comodidad. Cuando esta métrica se muestra en la consola de Amazon Redshift, se omiten los promedios de muestreo y solo ON o OFF se muestran. En Amazon CloudWatch, pueden aparecer otros valores además de 0 y 1 por cuestiones de muestreo. Cualquier valor mayor que 0 para MaintenanceMode se registra como 1 (ON). Unidades: Recuento (1/0) (ON/OFF en la consola de Amazon Redshift). Dimensiones: ClusterIdentifier
MaxConfiguredConcurrencyScale	El número máximo de clústeres de escalado de simultaneidad configurados desde el grupo de parámetros. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift (p. 210). Unidades: Recuento Dimensiones: ClusterIdentifier
NetworkReceiveThroughput	La velocidad a la que el nodo o el clúster reciben datos. Unidades: Bytes/segundo (MB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier, NodeID Dimensiones: ClusterIdentifier
NetworkTransmitThroughput	La velocidad a la que el nodo o el clúster escriben datos. Unidades: Bytes/segundo (MB/s en la consola de Amazon Redshift) Dimensiones: ClusterIdentifier, NodeID Dimensiones: ClusterIdentifier
PercentageDiskSpaceUsed	El porcentaje del espacio en disco usado. Unidades: Porcentaje Dimensiones: ClusterIdentifier
QueriesCompletedPerSecond	Promedio de consultas completadas por segundo. La información se envía en intervalos de 5 minutos. Unidades: Recuento/segundo Dimensiones: ClusterIdentifier, latency Dimensiones: ClusterIdentifier, wlmid

Métrica	Descripción
<code>QueryDuration</code>	Tiempo medio que tarda en completarse una consulta. La información se envía en intervalos de 5 minutos. Unidades: Microsegundos Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code>, <code>latency</code> Dimensiones: <code>ClusterIdentifier</code>, <code>latency</code> Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code>, <code>wlmid</code>
<code>QueryRuntimeBreakdown</code>	El tiempo total que las consultas dedican a ejecutarse por etapa de consulta. La información se envía en intervalos de 5 minutos. Unidades: Milisegundos Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code>, <code>etapa</code> Dimensiones: <code>ClusterIdentifier</code>, <code>etapa</code>
<code>ReadIOPS</code>	El número medio de operaciones de lectura en disco por segundo. Unidades: Recuento/segundo Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>
<code>ReadLatency</code>	Tiempo medio de cada operación de E/S de lectura en disco. Unidades: Segundos Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>
<code>ReadThroughput</code>	El número medio de bytes leídos del disco por segundo. Unidades: Bytes/segundo (GB/s en la consola de Amazon Redshift) Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>
<code>TotalTableCount</code>	Número de tablas de usuario abiertas en un momento determinado. Este total no incluye tablas de Amazon Redshift Spectrum. Unidades: Recuento Dimensiones: <code>ClusterIdentifier</code>
<code>WLMQueueLength</code>	El número de consultas en la cola para una cola de administración de carga de trabajo (WLM). Unidades: Recuento Dimensiones: <code>ClusterIdentifier</code>, <code>service class</code> Dimensiones: <code>ClusterIdentifier</code>, <code>QueueName</code>

Métrica	Descripción
WLMQueueWaitTime	El tiempo de consultas invertido en esperar en la cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Unidades: Milisegundos. Dimensiones: <code>ClusterIdentifier</code>, <code>QueryPriority</code> Dimensiones: <code>ClusterIdentifier</code>, <code>wlmid</code> Dimensiones: <code>ClusterIdentifier</code>, <code>QueueName</code>
WLMQueriesCompletedPerSecond	Número medio de consultas completadas por segundo en una cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Unidades: Recuento/segundo Dimensiones: <code>ClusterIdentifier</code>, <code>wlmid</code> Dimensiones: <code>ClusterIdentifier</code>, <code>QueueName</code>
WLMQueryDuration	Tiempo medio que tarda en completarse una consulta en una cola de administración de carga de trabajo (WLM). La información se envía en intervalos de 5 minutos. Unidades: Microsegundos Dimensiones: <code>ClusterIdentifier</code>, <code>wlmid</code> Dimensiones: <code>ClusterIdentifier</code>, <code>QueueName</code>
WLMRunningQueries	El número de consultas que se ejecutan desde el clúster principal y el clúster de escalado de simultaneidad por cola de WLM. Unidades: Recuento Dimensiones: <code>ClusterIdentifier</code>, <code>wlmid</code> Dimensiones: <code>ClusterIdentifier</code>, <code>QueueName</code>
WriteIOPS	El número medio de operaciones de escritura en disco por segundo. Unidades: Recuento/segundo Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>
WriteLatency	Tiempo medio de cada operación de E/S de escritura en disco. Unidades: Segundos Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>

Métrica	Descripción
<code>WriteThroughput</code>	Número medio de bytes que se escriben en el disco por segundo. Unidades: Bytes/segundo (GB/s en la consola de Amazon Redshift) Dimensiones: <code>ClusterIdentifier</code>, <code>NodeID</code> Dimensiones: <code>ClusterIdentifier</code>
<code>SchemaQuota</code>	La cuota configurada para un esquema. Unidades: Megabytes Dimensiones: <code>ClusterIdentifier</code>, <code>DatabaseName</code>, <code>SchemaName</code> Periódica/Push: <code>Periodic</code> : <code>Frequency5 minutes</code> Criterios de parada: Esquema eliminado o cuota eliminada
<code>NumExceededSchemaQuotas</code>	Número de esquemas con cuotas superadas. Unidades: Recuento Dimensiones: <code>ClusterIdentifier</code> Periódica/Push: <code>Periodic</code> : <code>Frequency5 minutes</code> Criterios de parada: N/A
<code>StorageUsed</code>	El disco o el espacio de almacenamiento utilizado por un esquema. Unidades: Megabytes Dimensiones: <code>ClusterIdentifier</code>, <code>DatabaseName</code>, <code>SchemaName</code> Periódica/Push: <code>Periodic</code> : <code>Frequency5 minutes</code> Criterios de parada: Esquema eliminado o cuota eliminada
<code>PercentageQuotaUsed</code>	Porcentaje de espacio de almacenamiento o disco utilizado en relación con la cuota de esquema configurada. Unidades: Porcentaje Dimensiones: <code>ClusterIdentifier</code>, <code>DatabaseName</code>, <code>SchemaName</code> Periódica/Push: <code>Periodic</code> : <code>Frequency5 minutes</code> Criterios de parada: Esquema eliminado o cuota eliminada

Dimensiones de métricas de Amazon Redshift

Los datos de Amazon Redshift se pueden filtrar en alguna de las dimensiones de la tabla siguiente.

Dimensión	Descripción
latency	Los valores posibles son los siguientes: • corto — menos de 10 segundos • medio: entre 10 segundos y 10 minutos • largo — más de 10 minutos
NodeID	Filtra los datos solicitados que son específicos de los nodos de un clúster. <code>NodeID</code> puede ser "Leader (Principal)", "Shared (Compartido)", o "Compute-N (N-computación)", donde N puede ser 0, 1, etc. en función del número de nodos del clúster. "Shared" significa que el clúster tiene un solo nodo, es decir, que el nodo principal y el nodo de computación están combinados. Las métricas de <code>CPUUtilization</code>, <code>NetworkTransmitThroughput</code> y <code>ReadIOPS</code> se registran únicamente para el nodo principal y los nodos de computación. Otras métricas que usan la dimensión <code>NodeId</code> se registran solo para los nodos de computación.
ClusterIdentifier	Filtra los datos solicitados que son específicos del clúster. Las métricas específicas del clúster son <code>HealthStatus</code>, <code>MaintenanceMode</code> y <code>DatabaseConnections</code>. Las métricas generales de esta dimensión (por ejemplo, <code>ReadIOPS</code>), que también son métricas de nodos, representan el total acumulado de datos de métricas de nodos. Preste especial atención cuando interprete estas métricas, ya que incluyen el comportamiento acumulado tanto del nodo principal como de los nodos de computación.
service class	El identificador de una clase de servicio WLM.
stage	Fases de ejecución de una consulta. Los valores posibles son los siguientes: • <code>QueryPlanning</code>: Tiempo invertido en procesar y optimizar instrucciones SQL. • <code>QueryWaiting</code>: tiempo invertido en esperar en la cola de WLM. • <code>QueryExecutingRead</code>: tiempo invertido en ejecutar consultas de lectura. • <code>QueryExecutingInsert</code>: tiempo invertido en ejecutar consultas de inserción. • <code>QueryExecutingDelete</code>: tiempo invertido en ejecutar consultas de eliminación. • <code>QueryExecutingUpdate</code>: tiempo invertido en ejecutar consultas de actualización. • <code>QueryExecutingCtas</code>: Tiempo invertido en ejecutar consultas de creación de tabla como. • <code>QueryExecutingUnload</code>: tiempo invertido en ejecutar consultas de descarga.

Dimensión	Descripción
	- QueryExecutingCopy: tiempo invertido en ejecutar consultas de copia. - QueryCommit: tiempo invertido en comprometerse.
wlmid	Es el identificador de una cola de administración de carga de trabajo.
QueryPriority	La prioridad de la consulta. Los valores posibles son CRITICAL, HIGHEST, HIGH, NORMAL, LOW y LOWEST.
QueueName	El nombre de la cola de administración de cargas de trabajo.

Datos de rendimiento de carga y consultas de Amazon Redshift

Además de las métricas de CloudWatch, Amazon Redshift proporciona datos sobre el desempeño de las cargas y las consultas. Los datos de rendimiento de cargas y consultas se pueden utilizar para ayudarle a comprender la relación entre el rendimiento de la base de datos y las métricas de clúster. Por ejemplo, si observa que la CPU de un clúster alcanza su pico, puede encontrar el pico en el gráfico de CPU del clúster y ver las consultas que se estaban ejecutando en ese momento. De igual forma, si está revisando una consulta específica, los datos de métricas (como los de CPU) se muestran en contexto para que pueda comprender el impacto de la consulta en las métricas de clúster.

Los datos de desempeño de las cargas y las consultas no se publican como las métricas de CloudWatch y solo pueden verse en la consola de Amazon Redshift. Los datos de desempeño de las cargas y las consultas se generan a partir de consultas de las tablas de sistema de la base de datos (para saber más, consulte [Referencia de las tablas de sistema](#) en la Guía para desarrolladores de Amazon Redshift). También puede generar sus propias consultas personalizadas de rendimiento de la base de datos, pero recomendamos comenzar con los datos de rendimiento de cargas y consultas que se presentan en la consola. Para obtener más información acerca de la medición y el monitoreo del rendimiento de la base de datos, consulte [Administración del rendimiento](#) en la Guía para desarrolladores de Amazon Redshift.

En la tabla siguiente se describen los diferentes aspectos de los datos de cargas y consultas a los que puede obtener acceso en la consola de Amazon Redshift.

Datos de cargas/consultas	Descripción
Resumen de consultas	Lista de consultas en un período de tiempo específico. La lista se puede ordenar por valores como el ID de consulta, tiempo de ejecución de la consulta y el estado. Consulte estos datos en la pestaña Monitoreo de consultas de la página de detalles del clúster.
Detalle de consulta	Proporciona detalles de una consulta en particular, incluidos: - Las propiedades de la consulta como el ID de consulta, el tipo, el clúster en el que se ejecutó la consulta y el tiempo de ejecución. - Detalles como el estado de consulta y el número de errores. - La instrucción SQL que se ejecutó. - Un plan de explicación, si está disponible. - Datos de rendimiento del clúster durante la ejecución de la consulta (para obtener más información, consulte Visualización de datos del historial de consultas (p. 438)).

Datos de cargas/ consultas	Descripción
Resumen de cargas	Muestra todas las cargas en un período de tiempo específico. La lista se puede ordenar por valores como el ID de consulta, tiempo de ejecución de la consulta y el estado. Consulte estos datos en la pestaña Monitoreo de consultas de la página de detalles del clúster.
Detalle de carga	Proporciona detalles de una operación de carga en particular, incluidos: • Las propiedades de la carga, como el ID de consulta, el tipo, el clúster en el que se ejecutó la consulta y el tiempo de ejecución. • Detalles como el estado de carga y el número de errores. • La instrucción SQL que se ejecutó. • Una lista de archivos cargados. • Datos de rendimiento del clúster durante la operación de carga (para obtener más información, consulte Visualización de datos del historial de consultas (p. 438)).

Uso de los datos de rendimiento en la consola de Amazon Redshift

En esta sección, encontrará cómo ver los datos de rendimiento en la consola de Amazon Redshift, que incluye información acerca del rendimiento del clúster y de las consultas. Además, puede crear alarmas en las métricas de clúster directamente desde la consola de Amazon Redshift.

Cuando ve los datos de rendimiento en la consola de Amazon Redshift, los ve por clúster. Los gráficos de datos de rendimiento para un clúster están diseñados para brindarle acceso a los datos para responder a las preguntas de rendimiento más comunes. Para obtener algunos datos de rendimiento (consulte [Supervisión de Amazon Redshift mediante las métricas de CloudWatch \(p. 422\)](#)), también puede utilizar CloudWatch para personalizar aún más los gráficos de métricas. Por ejemplo, puede elegir tiempos más largos o combinar métricas entre clústeres. Para obtener más información acerca del uso de la consola de CloudWatch, consulte [Uso de métricas de rendimiento en la consola de CloudWatch \(p. 469\)](#).

Vea el siguiente vídeo para obtener información sobre cómo monitorear, aislar y optimizar las consultas mediante las características del monitoreo de consultas de la consola de Amazon Redshift: [Monitoreo de consultas con Amazon Redshift](#).

Temas

- [Visualización de datos de rendimiento del clúster \(p. 431\)](#)
- [Visualización de datos del historial de consultas \(p. 438\)](#)
- [Visualización de datos de rendimiento de la base de datos \(p. 441\)](#)
- [Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo \(p. 445\)](#)
- [Visualización de consultas y cargas \(p. 448\)](#)
- [Visualización de métricas de clúster durante las operaciones de carga \(p. 460\)](#)
- [Análisis del rendimiento de las cargas de trabajo \(p. 462\)](#)
- [Creación de una alarma \(p. 466\)](#)
- [Uso de métricas de rendimiento en la consola de CloudWatch \(p. 469\)](#)

Visualización de datos de rendimiento del clúster

Al utilizar las métricas de clúster en Amazon Redshift, puede realizar las siguientes tareas de rendimiento comunes:

- Determinar si las métricas de clúster están fuera de lo normal en un intervalo de tiempo especificado y, si es así, identificar las consultas responsables de este error en el rendimiento.
- Comprobar si las consultas actuales o históricas están impactando en el rendimiento del clúster. Si identifica una consulta problemática, puede ver sus detalles incluyendo el rendimiento del clúster durante la ejecución de la consulta. Puede utilizar esta información a la hora de diagnosticar el motivo por el que la consulta es lenta y lo que se puede hacer para mejorar su rendimiento.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para ver los datos de desempeño

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y haga clic en el nombre de un clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluir Rendimiento del clúster, Supervisión de consultas, Bases de datos, Comparticiones de datos, Schedules, Mantenimiento, y Propiedades pestañas.
3. Elija la pestaña Cluster performance (Rendimiento del clúster) para ver la información del rendimiento, incluido:
 - Utilización de la CPU
 - Porcentaje de espacio del disco usado
 - Conexiones a base de datos
 - Estado
 - Query duration
 - Query throughput
 - Actividad de escalado de simultaneidad

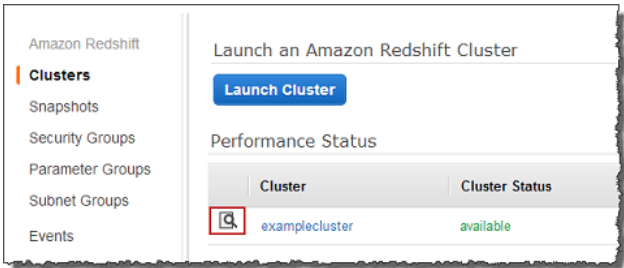
Hay muchas más métricas disponibles. Para ver las métricas disponibles y elegir cuáles se muestran, seleccione el icono Preferencias.

Consola original

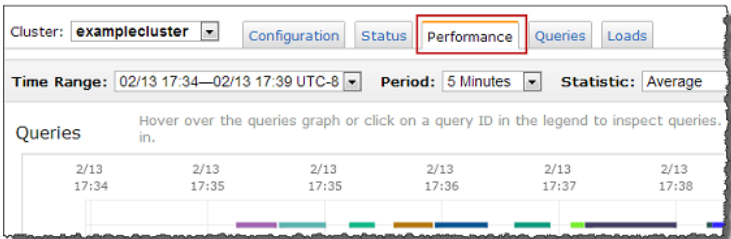
En la vista predeterminada del clúster se muestran todos los nodos representados juntos en un gráfico, una estadística `Average` y los datos de la última hora. Puede cambiar esta vista según sea necesario. Algunas métricas, como `HealthStatus`, solo son aplicables al nodo principal, mientras que otras, como `WriteOps`, solo son aplicables a los nodos de computación. Cambiar el modo de visualización del nodo restablece todos los filtros.

Visualización de datos de rendimiento del clúster

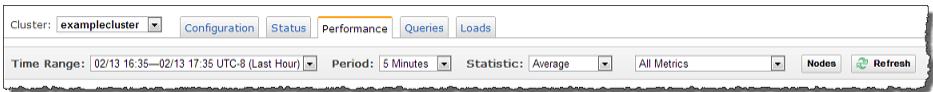
1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), seleccione el icono de lupa situado junto al clúster cuyos datos de desempeño desee ver.



4. Seleccione la pestaña Performance (Desempeño).



De forma predeterminada, en la vista de rendimiento se muestra el rendimiento del clúster durante la última hora. Si necesita ajustar la vista de una forma más precisa, puede utilizar filtros, tal y como se describe en la siguiente tabla.



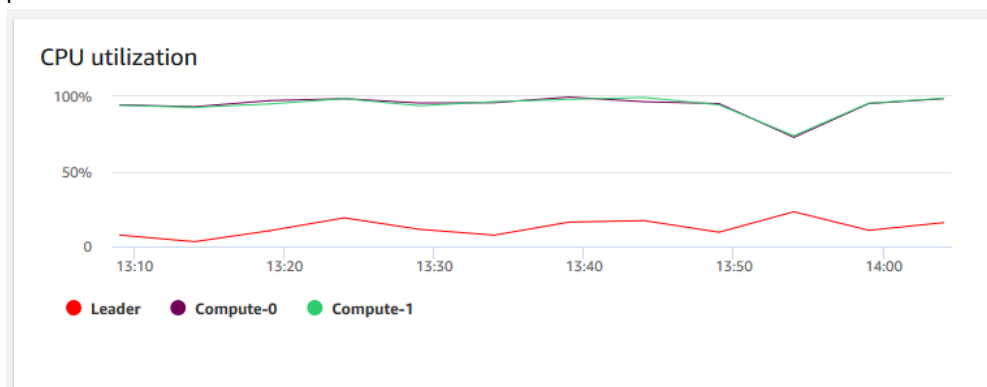
Para ello	Use este filtro
Cambiar el intervalo de tiempo en el que se muestran los datos	Seleccione un intervalo de tiempo en la lista Time Range (Intervalo). De forma predeterminada, se muestra la última hora.
Cambiar el período de tiempo en el que se muestran los datos	Seleccione un periodo en la lista Period (Periodo). De forma predeterminada, se muestra un período de cinco minutos. Utilice un período menor a cinco minutos si necesita ver más detalles cuando investigue una métrica (en profundidad) y visualice las métricas en un breve período de tiempo, por ejemplo, diez minutos. Del mismo modo, utilice un período mayor a cinco minutos cuando visualice las métricas en un período de tiempo extenso, por ejemplo, días.
Cambiar la estadística que se muestra para las métricas	Seleccione una estadística en la lista Statistic (Estadística). De forma predeterminada, se utiliza la estadística Average.

Para ello	Use este filtro
Cambiar qué métricas se muestran, todas o una métrica específica	Seleccione una métrica en la lista Metrics (Métricas). De forma predeterminada, se muestran todas las métricas.
Cambiar las métricas de un nodo para que se muestren por separado o juntas en el mismo gráfico	Seleccione Nodes (Nodos). De forma predeterminada, los datos de nodos para algunas métricas se muestran en un gráfico combinado. Si elige visualizar los datos de nodos en gráficos separados, puede, adicionalmente, mostrar u ocultar los nodos individuales.

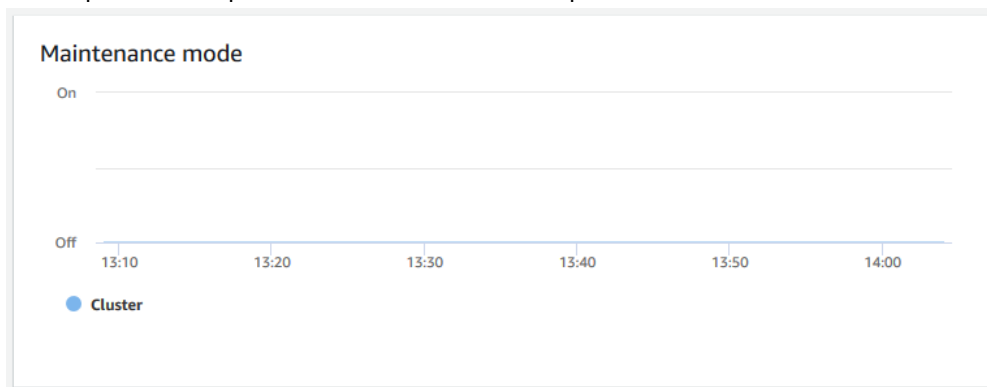
Gráficos de rendimiento del clúster

En los siguientes ejemplos se muestran algunos de los gráficos que se muestran en la nueva consola de Amazon Redshift.

- **Utilización de la CPU**— Muestra el porcentaje de utilización de CPU para todos los nodos (principales y de computación). Para encontrar un momento en el que el uso del clúster sea inferior antes de programar la migración del clúster u otras operaciones que consumen recursos, monitoree este gráfico para ver la utilización de la CPU en cada uno de los nodos o en todos ellos.

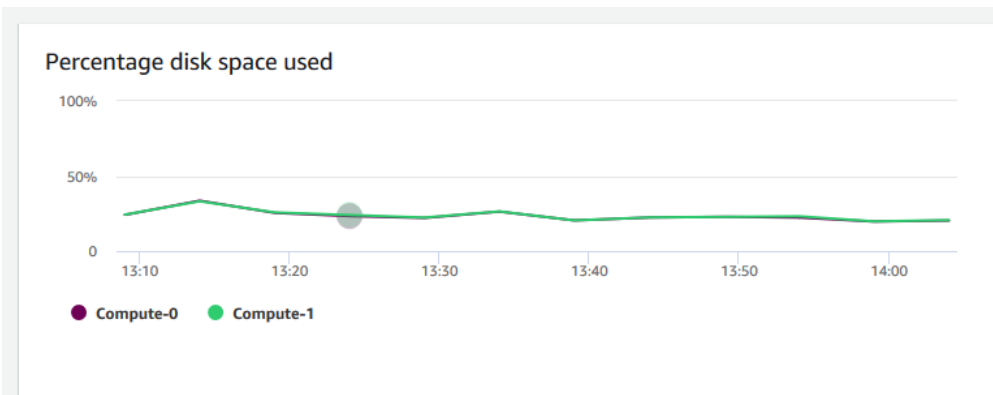


- **Modo de mantenimiento**— Muestra si el clúster está en el modo de mantenimiento en un momento elegido mediante el uso de `on/off` indicadores. Puede ver la hora en que el clúster está en proceso de mantenimiento. A continuación, puede correlacionar esta hora con las operaciones que se realizan en el clúster para estimar períodos de inactividad futuros para eventos recurrentes.

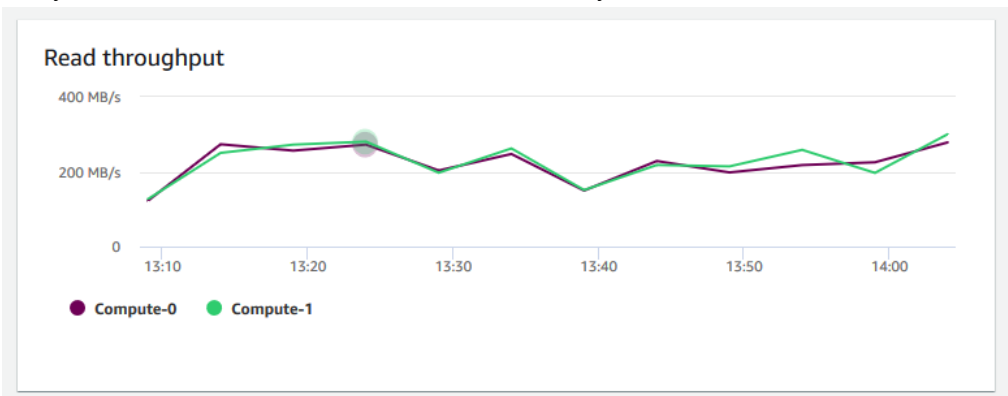


- **Porcentaje de espacio del disco usado**: muestra el porcentaje de uso de espacio en disco por cada nodo informático, y no para el clúster como un todo. Puede explorar este gráfico para monitorear la

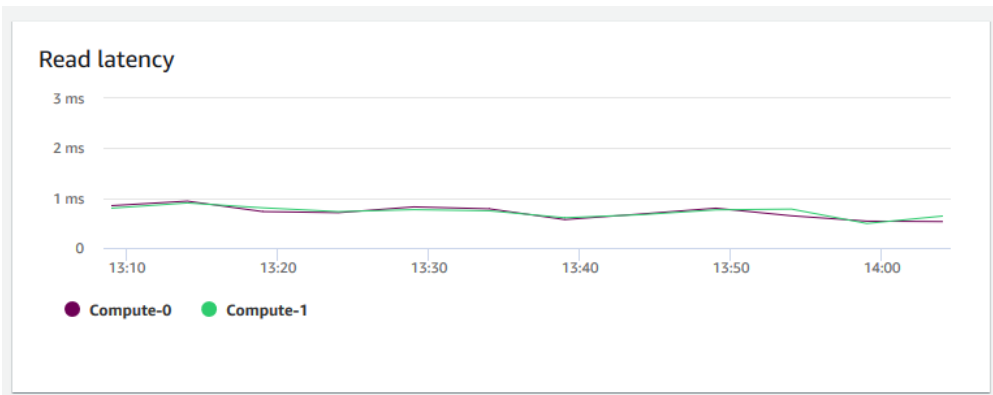
utilización del disco. Las operaciones de mantenimiento como VACUUM y COPY utilizan espacio de almacenamiento temporal intermedio para sus operaciones de clasificación, por lo que se espera un aumento en el uso del disco.



- **Velocidad de lectura:** muestra el número medio de megabytes leídos del disco por segundo. Puede evaluar este gráfico para monitorear el aspecto físico correspondiente del clúster. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y su volumen.



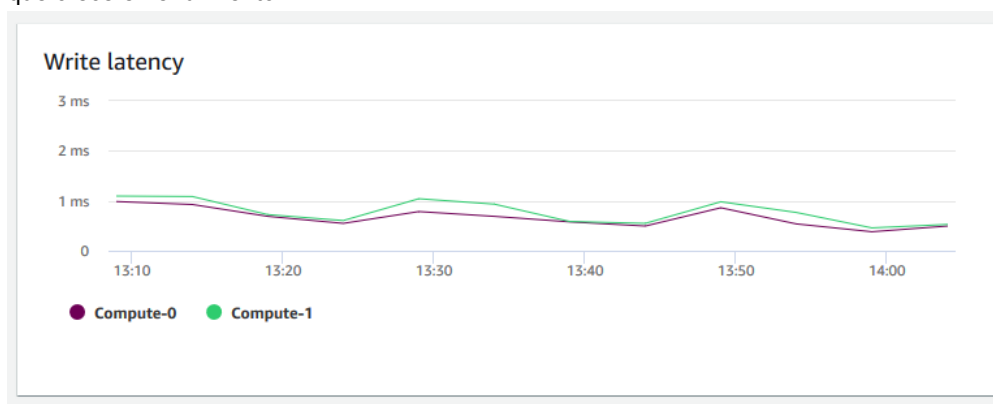
- **Read Latency—** Muestra el tiempo medio de cada operación de E/S de lectura en disco por milisegundo. Puede ver los tiempos de respuesta para que se devuelvan los datos. Cuando la latencia es alta, significa que el remitente pasa más tiempo inactivo (sin enviar paquetes nuevos), lo que reduce la rapidez con que crece el rendimiento.



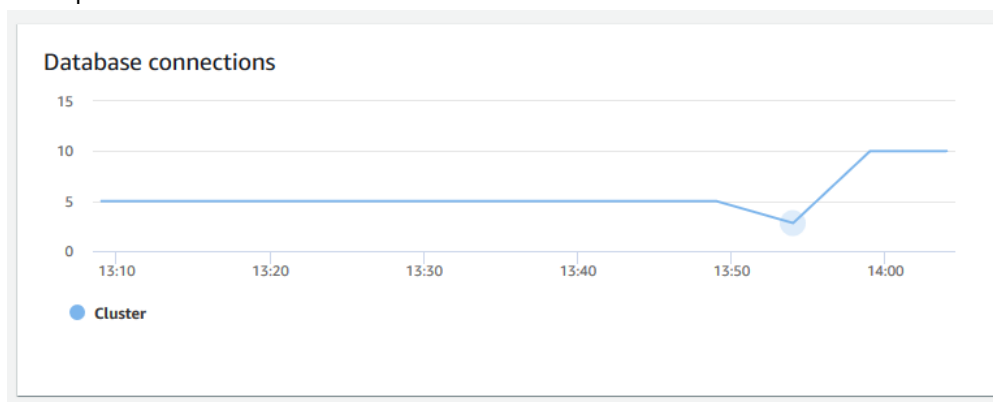
- **Velocidad de escritura:** muestra el número medio de megabytes que se escriben en el disco por segundo. Puede evaluar esta métrica para monitorear el aspecto físico correspondiente del clúster. Este rendimiento no incluye el tráfico de red entre las instancias del clúster y su volumen.



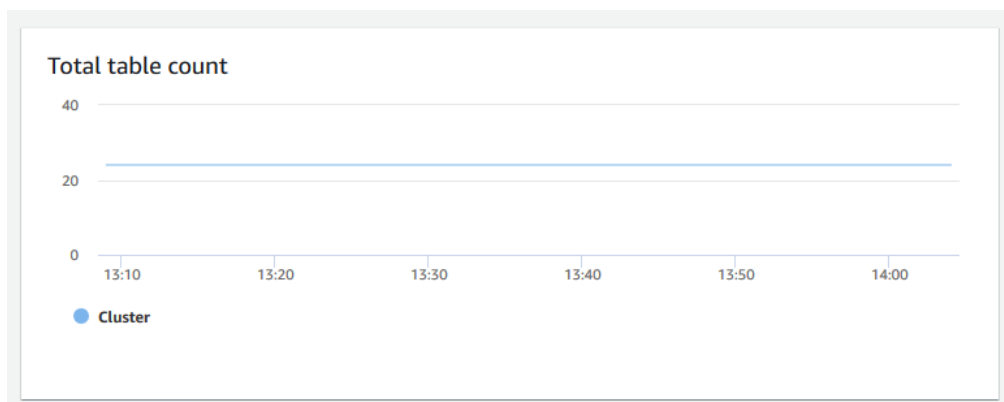
- **Write Latency**— Muestra el tiempo medio de cada operación de E/S de escritura en disco. Puede evaluar el tiempo para que se devuelva el reconocimiento de la escritura. Cuando la latencia es alta, significa que el remitente pasa más tiempo inactivo (sin enviar paquetes nuevos), lo que reduce la rapidez con que crece el rendimiento.



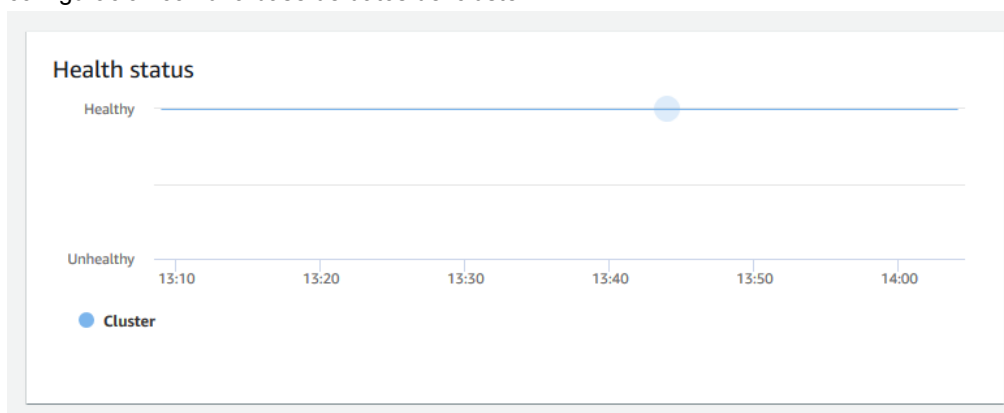
- **Conexiones a base de datos**: muestra el número de conexiones de base de datos a un clúster. Puede utilizar este gráfico para ver cuántas conexiones se establecen a la base de datos y encontrar una hora en la que el uso del clúster es menor.



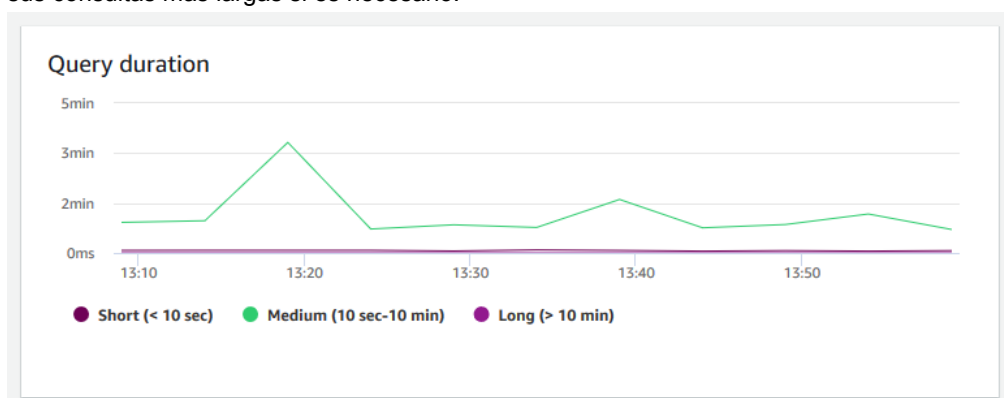
- **Recuento total de tablas**— Muestra el número de tablas de usuario abiertas en un momento determinado dentro de un clúster. Puede monitorear el rendimiento del clúster cuando el recuento de tablas abiertas es alto.



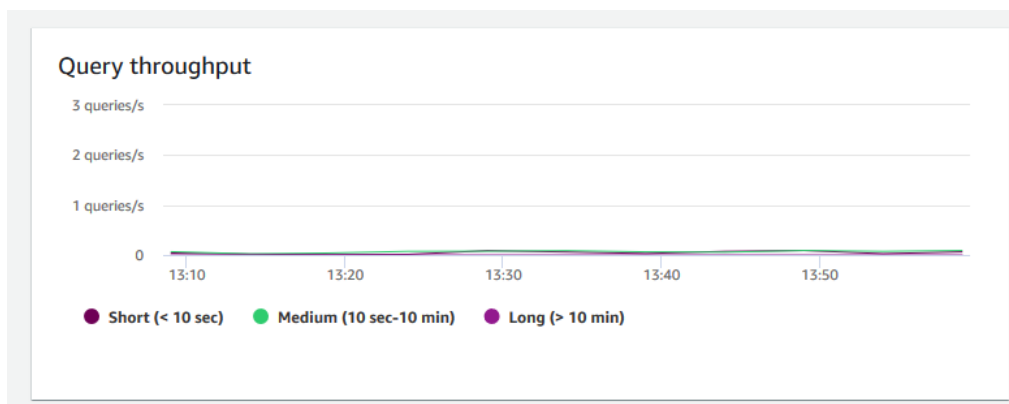
- Estado— Indica el estado del clúster como `Healthy` or `Unhealthy`. Si el clúster puede conectarse a su base de datos y realiza correctamente una consulta sencilla, se considera que el clúster está en buen estado. De lo contrario, se considera que el clúster está en mal estado. Un estado incorrecto se puede producir cuando la base de datos del clúster está sobrecargada en exceso o cuando hay un problema de configuración con una base de datos del clúster.



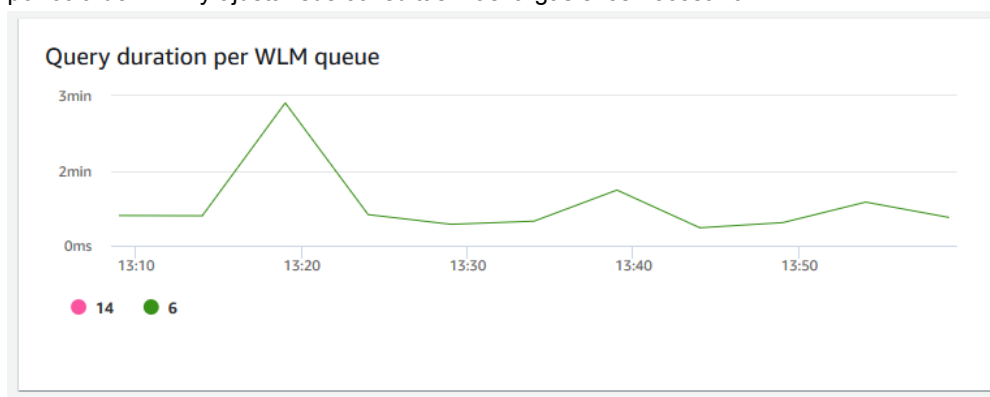
- Query duration— Muestra el tiempo medio que tarda en completarse una consulta en microsegundos. Puede comparar los datos de este gráfico para medir el rendimiento de E/S dentro del clúster y ajustar sus consultas más largas si es necesario.



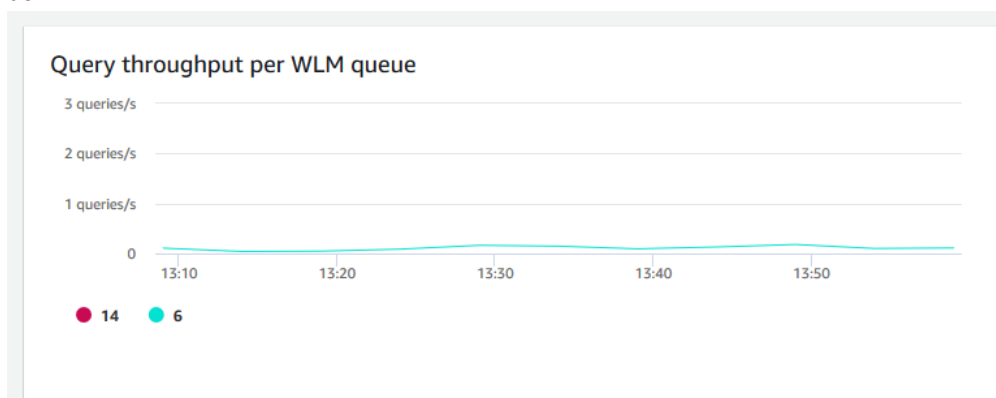
- Query throughput: muestra el número medio de consultas completadas por segundo. Puede analizar los datos de este gráfico para medir el rendimiento de la base de datos y caracterizar la capacidad del sistema para admitir una carga de trabajo multiusuario de manera equilibrada.



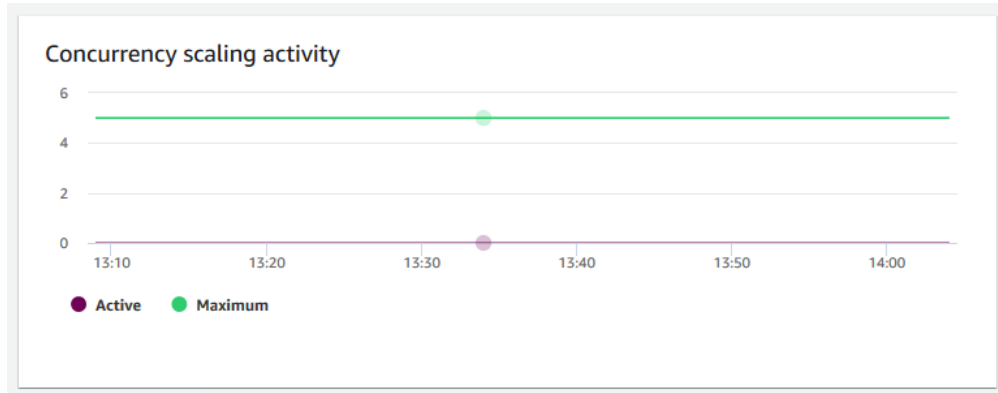
- Duración de la consulta por cola WLM— Muestra el tiempo medio que tarda en completarse una consulta en microsegundos. Puede comparar los datos de este gráfico para medir el rendimiento de E/S por cola de WLM y ajustar sus consultas más largas si es necesario.



- Rendimiento de consulta por cola WLM: muestra el número medio de consultas completadas por segundo. Puede analizar los datos de este gráfico para medir el rendimiento de la base de datos por cola de WLM.



- Actividad de escalado de simultaneidad: muestra el número de clústeres de escalado de simultaneidad activos. Cuando el escalado de simultaneidad está habilitado, Amazon Redshift añade automáticamente capacidad del clúster cuando se necesita para procesar un aumento de las consultas de lectura simultáneas.



Visualización de datos del historial de consultas

Puede utilizar las métricas del historial de consultas en Amazon Redshift para hacer lo siguiente:

- Aislar y diagnosticar problemas de rendimiento de consultas.
- Comparar las métricas de tiempo de ejecución de la consulta y las métricas de rendimiento del clúster en la misma línea temporal para ver cómo pueden estar relacionadas ambas. Al hacerlo, podrá identificar consultas con mal rendimiento, buscar consultas con cuellos de botella y determinar si necesita cambiar el tamaño del clúster para la carga de trabajo.
- Acceda a los detalles de una consulta específica eligiéndola en la línea temporal. Cuando el ID de consulta y otras propiedades se muestran en una fila debajo del gráfico, puede elegir la consulta para ver los detalles de la consulta. Los detalles incluyen, por ejemplo, la instrucción SQL de la consulta, los detalles de ejecución y el plan de consulta. Para obtener más información, consulte [Visualización de detalles de consultas](#) (p. 450).
- Determine si los trabajos de carga se realizan correctamente y cumplen los acuerdos de nivel de servicio (SLA).

Para mostrar datos del historial de consultas

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluirRendimiento del clúster,Supervisión de consultas,Bases de datos,Comparticiones de datos,Schedules,Mantenimiento, yPropiedadespestañas.
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Historial de consultas.

Mediante los controles de la ventana, puede alternar entre Lista de consultas y Métricas de clúster.

Al elegir Lista de consultas, la pestaña incluye los siguientes gráficos:

- Tiempo de ejecución de consultas— La actividad de consulta en una línea de tiempo. Utilice este gráfico para ver qué consultas se están ejecutando en el mismo periodo de tiempo. Elija una consulta para ver más detalles de ejecución de la consulta. El eje x muestra el periodo seleccionado. Puede filtrar las consultas gráficas por: en ejecución, finalizadas, cargadas, etc. Cada barra representa una consulta y la longitud de la barra representa su tiempo de ejecución desde el principio de la barra hasta el final. Las consultas pueden incluir instrucciones de manipulación de

datos SQL (como SELECT, INSERT, DELETE) y cargas (como COPY). De forma predeterminada, las 100 consultas en ejecución más largas se muestran para el periodo de tiempo seleccionado.

- Consultas y cargas— Lista de consultas y cargas que se ejecutaron en el clúster. La ventana incluye una opción para Terminar la consulta si una consulta se está ejecutando actualmente.

Al elegir Métricas de clúster, la pestaña incluye los siguientes gráficos:

- Tiempo de ejecución de consultas— La actividad de consulta en una línea de tiempo. Utilice este gráfico para ver qué consultas se están ejecutando en el mismo periodo de tiempo. Elija una consulta para ver más detalles de ejecución de la consulta.
- Utilización de la CPU— La utilización de CPU del clúster por nodo directivo y el promedio de nodos informáticos.
- Capacidad de almacenamiento utilizada— El porcentaje de la capacidad de almacenamiento utilizada.
- Conexiones de base de datos activas: número de conexiones activas a base de datos en el clúster.

Tenga en cuenta lo siguiente al trabajar con los gráficos del historial de consultas:

- Elija una barra que represente una consulta específica en el gráfico Tiempo de ejecución de consultas para ver detalles sobre esa consulta. También puede elegir un ID de consulta en la lista de Consultas y cargas para ver sus detalles.
- Puede seleccionar una sección del gráfico Tiempo de ejecución de consultas para ampliar y mostrar un periodo de tiempo específico.
- En el gráfico Tiempo de ejecución de consultas, para que el filtro elegido considere todos los datos y pase por todas las páginas mostradas en la lista Consultas y cargas.
- Puede cambiar las columnas y el número de filas que se muestran en la lista Consultas y cargas mediante la ventana de preferencias mostrada por el icono de engranaje de configuración.
- La lista de Consultas y cargas también se puede mostrar navegando desde el icono de Consultas del navegador izquierdo, Consultas y cargas. Para obtener más información, consulte [Visualización de consultas y cargas \(p. 448\)](#).

Gráficos de historial de consultas

En los siguientes ejemplos se muestran gráficos que se muestran en la nueva consola de Amazon Redshift.

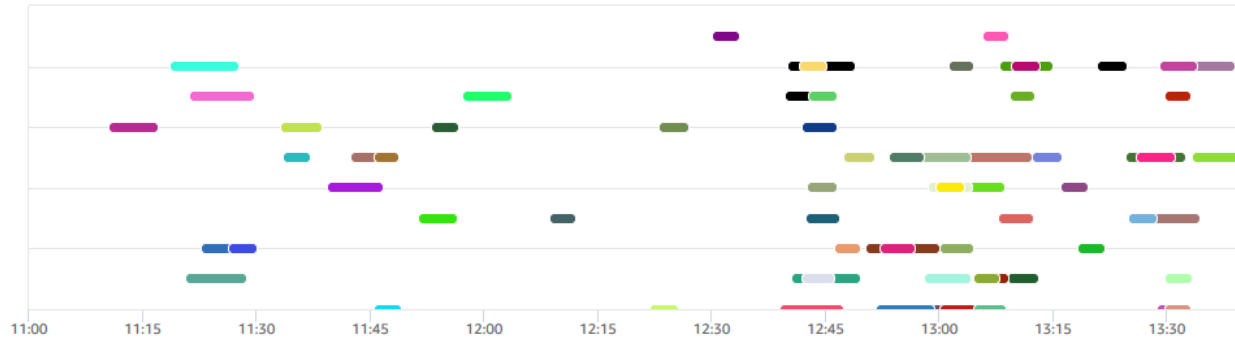
Note

Los gráficos de la consola de Amazon Redshift solo contienen datos de las 100 000 consultas más recientes.

- Tiempo de ejecución de consultas

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



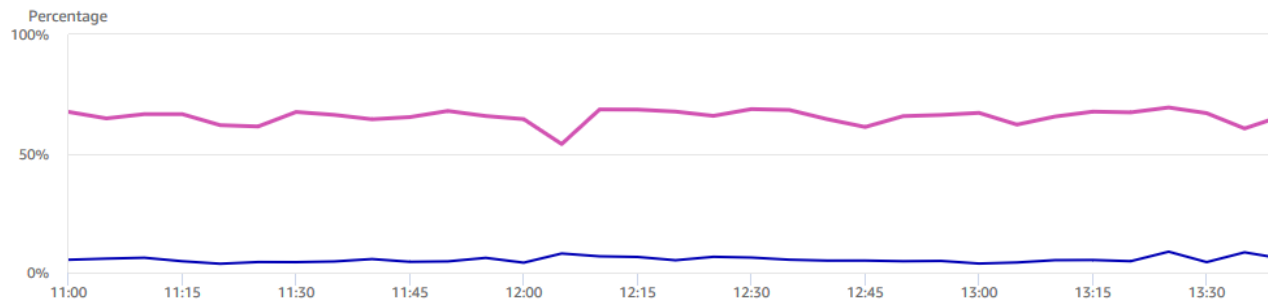
- Consultas y cargas

Queries and loads(100)						
Filter queries						
☐	Start time	Query	Status	Duration	SQL	
☐	Apr 13th, 2020 01:00:55 PM 8 days ago	69248	Completed	11 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_10cu_	
☐	Apr 13th, 2020 12:58:07 PM 8 days ago	69199	Completed	11 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_10cu_	
☐	Apr 13th, 2020 12:54:15 PM 8 days ago	69111,69265,69253	Completed	10 min	with /* query_templates/query22.tpl a-8047-06872b3fecc8.stream_10cu_	
☐	Apr 13th, 2020 12:50:17 PM 8 days ago	68976	Completed	10 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_10cu_	
☐	Apr 13th, 2020 01:29:23 PM 8 days ago	70089	Completed	10 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_10cu_	
☐	Apr 13th, 2020 11:18:35 AM 8 days ago	65543	Completed	9 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_05cu_	
☐	Apr 13th, 2020 12:40:30 PM 8 days ago	68729	Completed	9 min	with /* query_templates/query67.tpl a-8047-06872b3fecc8.stream_10cu_	

- Utilización de la CPU

CPU utilization

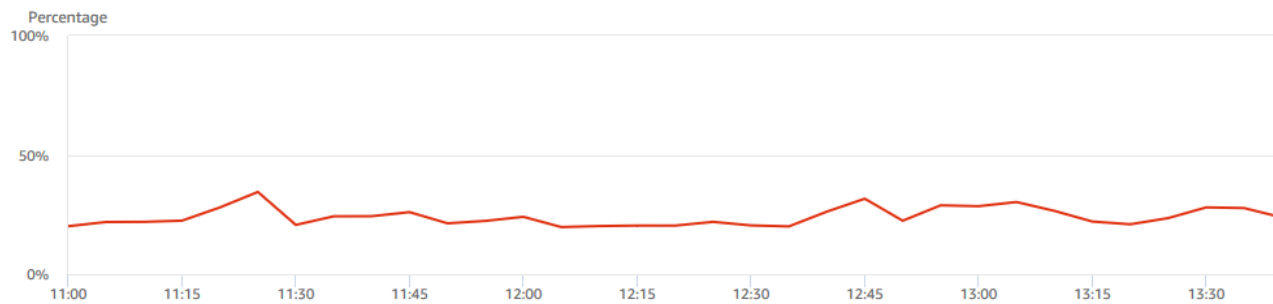
The CPU utilization of the cluster by leader node and average of compute nodes.



- Capacidad de almacenamiento utilizada

Storage capacity used

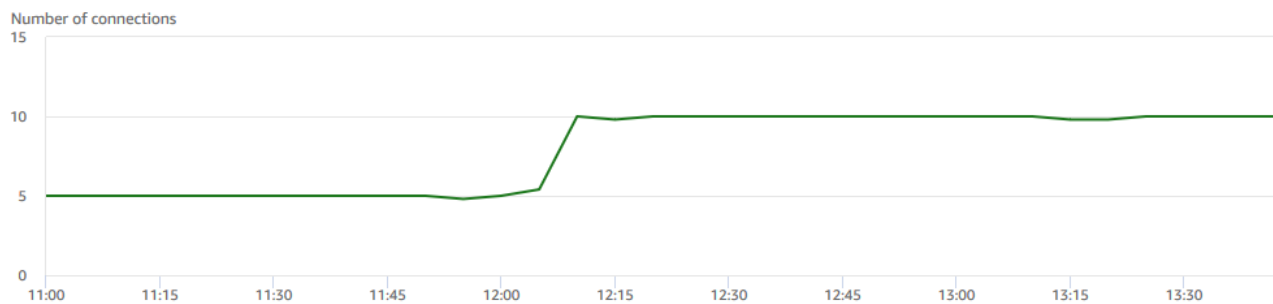
The percent of the storage capacity used.



- Conexiones de base de datos activas

Active database connections

The number of active database connections to the cluster.



Visualización de datos de rendimiento de la base de datos

Puede utilizar las métricas de rendimiento de la base de datos en Amazon Redshift para hacer lo siguiente:

- Analizar el tiempo empleado por las consultas por etapas de procesamiento. Puede buscar tendencias inusuales en el tiempo que pasa en una etapa.
- Analizar el número de consultas, la duración y el rendimiento de las consultas por intervalos de duración (corto, medio y largo).
- Buscar tendencias acerca del tiempo de espera de la consulta por prioridad de la consulta (más baja, baja, normal, alta, más alta, crítica).
- Buscar tendencias acerca de la duración de la consulta, el rendimiento o el tiempo de espera de la cola de WLM.

Para mostrar los datos de rendimiento de la base de datos

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija CLUSTERS y elija el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, incluyendoRendimiento del clúster,Supervisión de consultas,Bases de datos,Comparticiones de datos,Schedules,Mantenimiento, yPropiedadespestañas.
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Rendimiento de la base de datos.

Mediante los controles de la ventana, puede alternar entre Métricas de clúster y Métricas de cola de WLM.

Al elegir Métricas de clúster, la pestaña incluye los siguientes gráficos:

- Desglose de la ejecución de las cargas de trabajo— El tiempo utilizado en las etapas de procesamiento de consultas.
- Consultas por intervalo de duración: número de consultas cortas, medianas y largas.
- Query throughputNúmero medio de consultas completadas por segundo.
- Query duration: tiempo medio que tarda en completarse una consulta.
- Tiempo medio de espera de cola por prioridadEl tiempo de consultas invertido en esperar en la cola de WLM por prioridad de consulta.

Al elegir Métricas de cola de WLM, la pestaña incluye los siguientes gráficos:

- Duración de la consulta por cola— La duración media de la consulta por cola de WLM.
- Rendimiento de la consulta por colaNúmero medio de consultas completadas por segundo por la cola de WLM.
- Tiempo de espera de consulta por cola— La duración media de las consultas pasadas en espera de la cola de WLM.

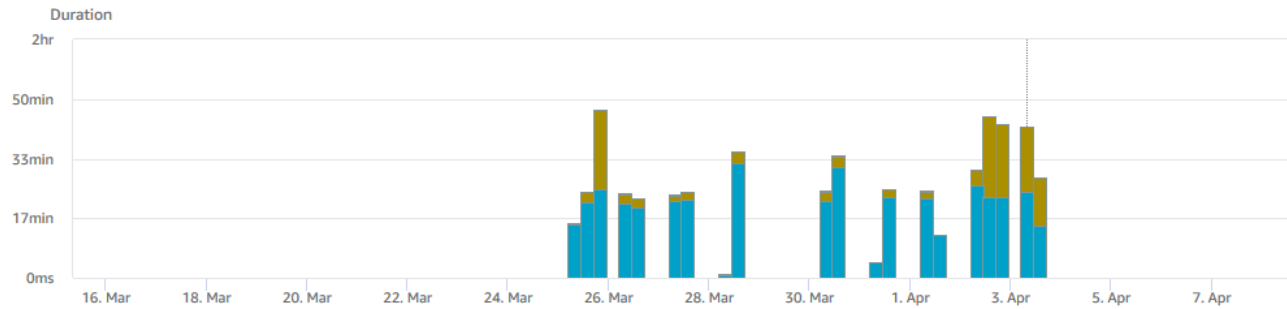
Gráficos de rendimiento de la base de datos

En los siguientes ejemplos se muestran gráficos que se muestran en la nueva consola de Amazon Redshift.

- Desglose de la ejecución de las cargas de trabajo

Workload execution breakdown

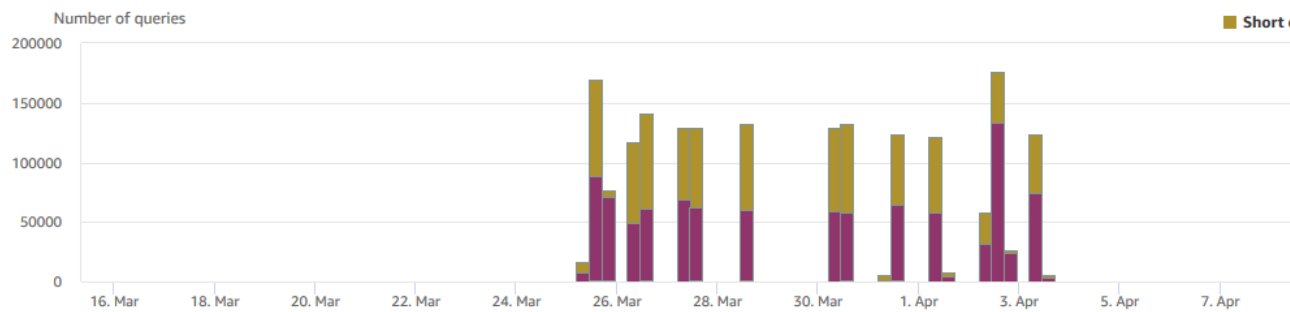
The time used in query processing stages.



- Consultas por intervalo de duración

Queries by duration range

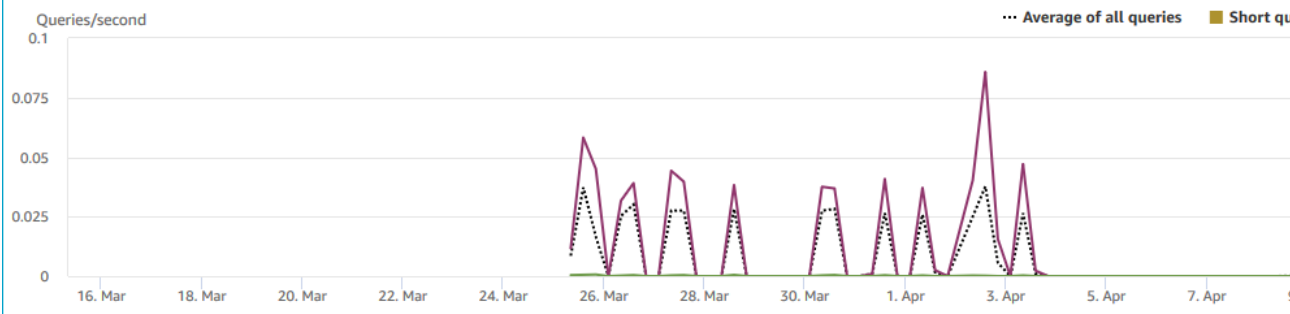
The number of short, medium and long queries.



- Query throughput

Query throughput

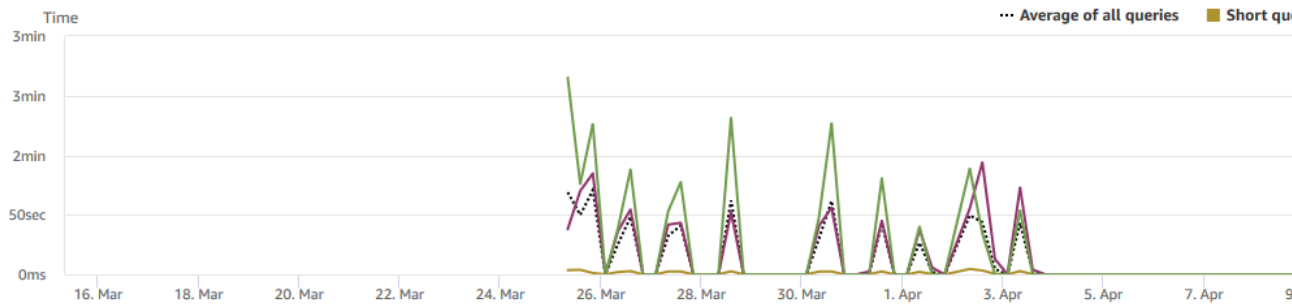
The average number of queries completed per second.



- Query duration

Query Duration

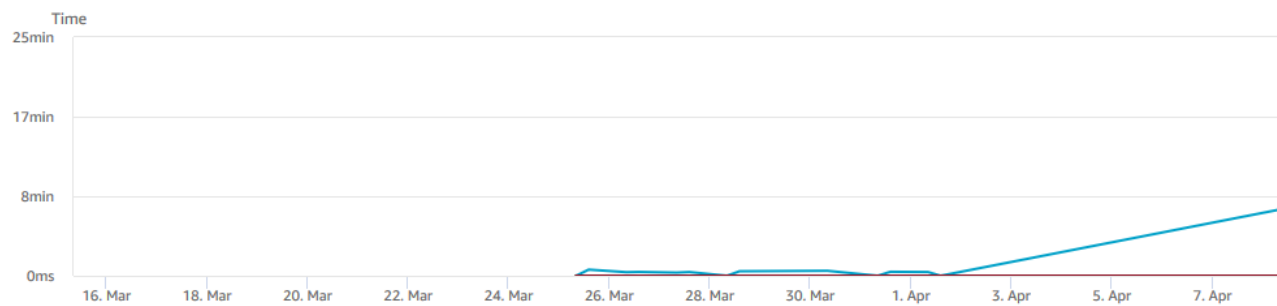
The average amount of time to complete a query.



- Tiempo medio de espera de cola por prioridad

Average queue wait time by priority

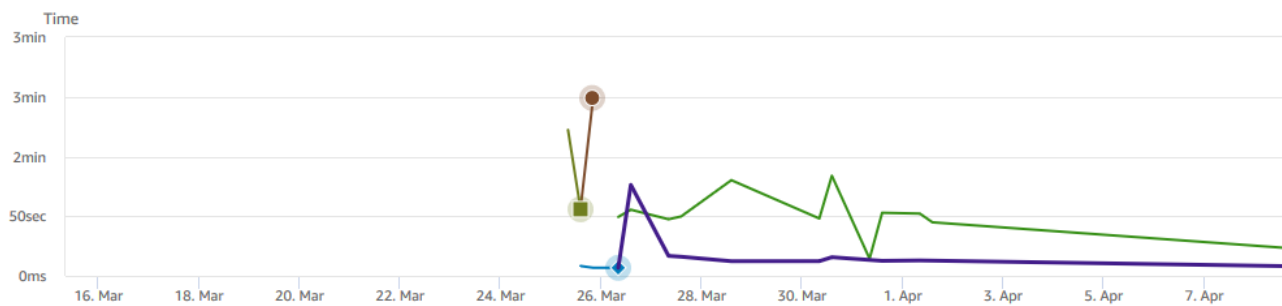
The total time queries spent waiting in the WLM queue by query priority.



- Duración de la consulta por cola

Query Duration by queue

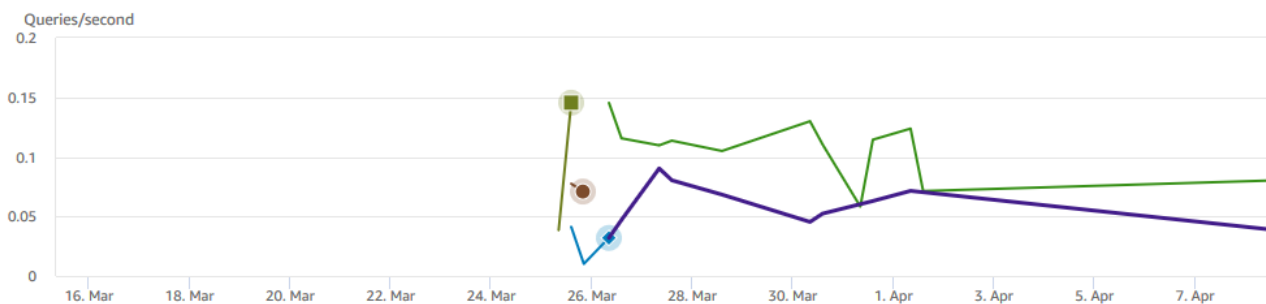
The average query duration by WLM queue.



- Rendimiento de la consulta por cola

Query throughput by queue

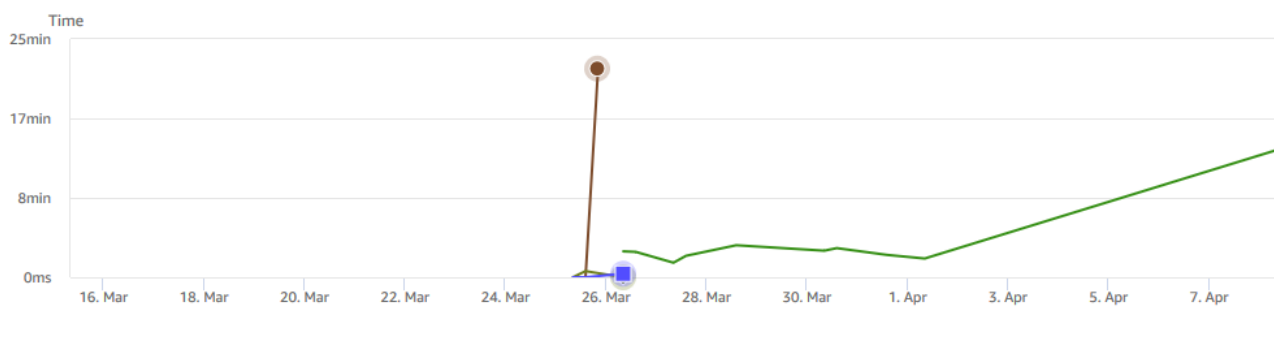
The average number of queries completed per second by WLM queue.



- Tiempo de espera de consulta por cola

Query wait time by queue

The average duration of queries spent waiting by WLM queue.



Visualización de datos de escalado de simultaneidad y simultaneidad de cargas de trabajo

Al utilizar las métricas de escalado de simultaneidad en Amazon Redshift, puede hacer lo siguiente:

- Analice si puede reducir el número de consultas en cola habilitando el escalado de simultaneidad. Puede comparar por cola de WLM o para todas las colas de WLM.
- Ver la actividad de escalado de simultaneidad en clústeres de escalado de simultaneidad. Esto le puede indicar si el escalado de simultaneidad está limitado por el valor de `max_concurrency_scaling_clusters`. En tal caso, puede elegir aumentar el valor `max_concurrency_scaling_clusters` en el parámetro de base de datos.
- Ver el uso total de escalado de simultaneidad de todos los clústeres de escalado de simultaneidad.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para mostrar los datos de escalado de simultaneidad

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluirRendimiento del clúster,Supervisión de consultas,Bases de datos,Comparticiones de datos,Schedules,Mantenimiento, yPropiedadespestañas.
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija la pestaña Simultaneidad de cargas de trabajo.

La pestaña incluye los siguientes gráficos:

- Consultas en cola frente a ejecución en el clúster— El número de consultas que se ejecutan (desde el clúster principal y el clúster de escalado de simultaneidad) en comparación con el número de consultas que esperan en todas las colas WLM del clúster.
- consultas en cola frente a ejecución por cola— El número de consultas que se ejecutan (desde el clúster principal y el clúster de escalado de simultaneidad) en comparación con el número o las consultas que esperan en cada cola de WLM.
- Actividad de escalado de simultaneidad— Número de clústeres de escalado de simultaneidad que procesan activamente consultas.
- Uso de escalado de simultaneidad— El uso de clústeres de escalado de simultaneidad que tienen actividad de procesamiento de consultas activa.

Consola original

Para ver los datos de escalado de simultaneidad

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. Elija el clúster para el que desea ver los datos de escalado de simultaneidad.
4. Seleccione la pestaña Database Performance (Desempeño de la base de datos).

De forma predeterminada, en la vista de rendimiento se muestran los datos de escalado de simultaneidad durante la última hora. Si necesita ajustar la vista de una forma más precisa, puede utilizar filtros para cambiar el alcance de los datos.

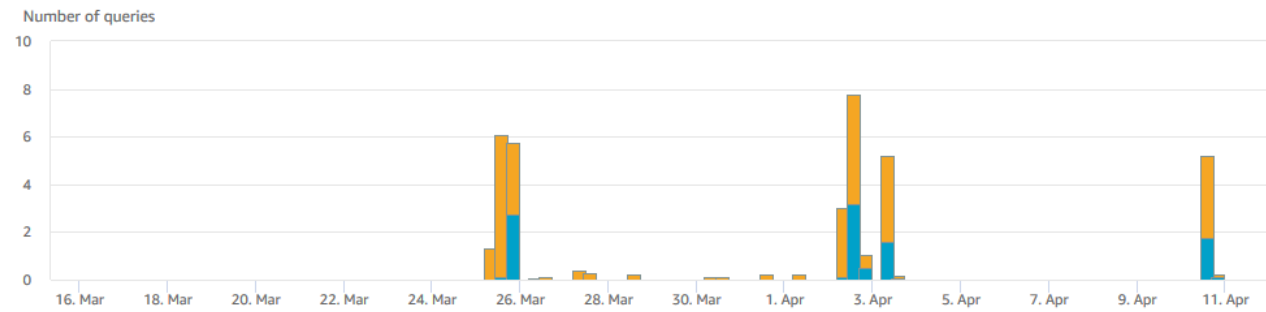
Gráficos de simultaneidad de carga de trabajo

En los siguientes ejemplos se muestran gráficos que se muestran en la nueva consola de Amazon Redshift.

- Consultas en cola frente a ejecución en el clúster)

Queued vs. Running queries on the cluster

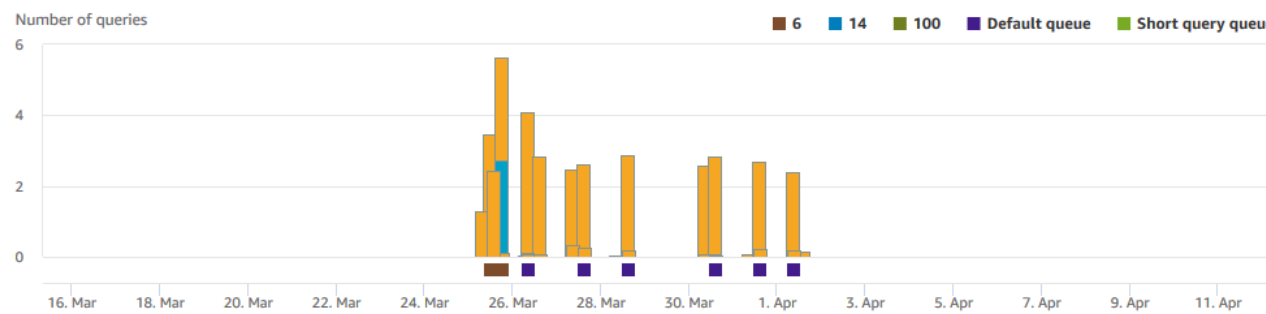
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in all WLM queues in the cluster.



- consultas en cola frente a ejecución por cola)

Queued vs. Running queries per queue

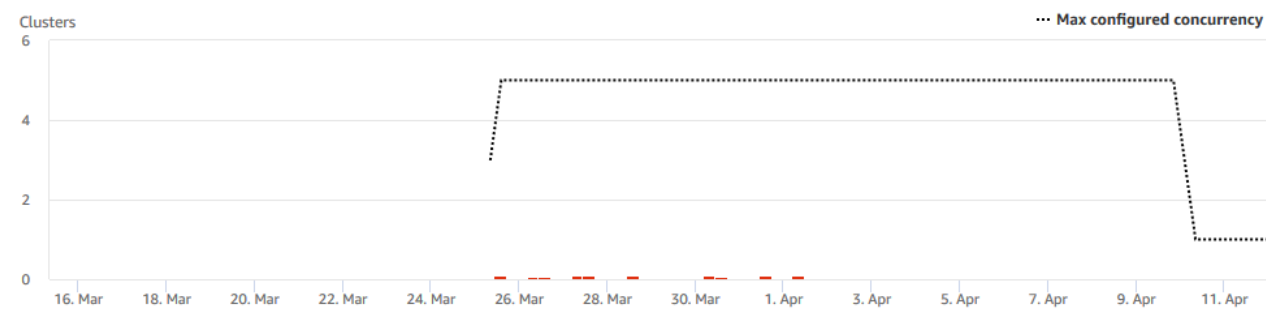
The number of queries running (from the main cluster and concurrency scaling cluster) compared to the number of queries waiting in each WLM queue.



- Actividad de escalado de simultaneidad

Concurrency scaling activity

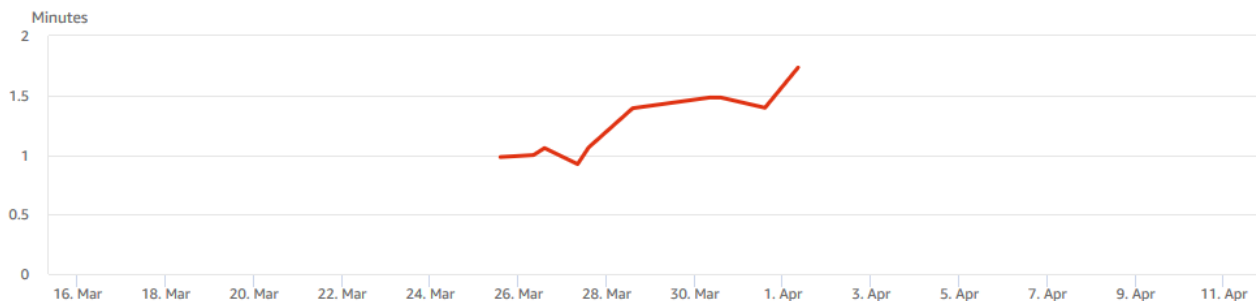
The number of concurrency scaling clusters that are actively processing queries.



- Uso de escalado de simultaneidad

Concurrency scaling usage

The usage of concurrency scaling clusters that have active query processing activity.



Visualización de consultas y cargas

La consola de Amazon Redshift proporciona información acerca de las consultas y cargas que se ejecutan en la base de datos. Puede utilizar esta información para identificar y solucionar problemas de las consultas que tardan demasiado tiempo para procesarse y provocan cuellos de botella que impiden que las otras consultas se procesen de forma eficaz. Puede utilizar la información de consultas de la consola de Amazon Redshift para supervisar el procesamiento de consultas.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para mostrar datos de rendimiento de consultas

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione QUERIES (Consultas) y luego seleccione Queries and loads (Consultas y cargas) para mostrar la lista de consultas de su cuenta.

Por defecto, la lista muestra consultas de todos sus clústeres durante las últimas 24 horas. Puede cambiar el alcance de los datos mostrados en la consola.

Important

La pestaña Queries and loads (Consultas y cargas) muestra las consultas que han tardado más tiempo en ejecutarse en el sistema (hasta 100 consultas).

Consola original

Visualización de datos de rendimiento de consultas

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).

3. Elija el clúster para el que desea ver los datos de rendimiento.
4. De forma predeterminada, en la lista de Consultas se muestra el rendimiento de las consultas durante las últimas 24 horas. Si desea modificar los datos que aparecen en la vista, use la lista Filter (Filtro) para seleccionar el periodo de tiempo de las consultas que quiere ver. También puede escribir una palabra clave en la casilla Buscar para buscar consultas que coincidan con sus criterios de búsqueda.

Finalizar una consulta en ejecución

También puede utilizar la página Queries (Consultas) para finalizar una consulta que esté en proceso.

Note

La función para terminar consultas y cargas en la consola de Amazon Redshift requiere un permiso específico. Si desea que los usuarios puedan terminar consultas y cargas, asegúrese de añadir la acción `redshift:CancelQuerySession` a la política de AWS Identity and Access Management (IAM). Este requisito se aplica tanto si selecciona la opción Sólo lectura de Amazon Redshift AWS o cree una directiva personalizada en IAM. Los usuarios que tienen el Acceso completo a Amazon Redshift ya cuentan con los permisos necesarios para terminar las consultas y las cargas. Para obtener más información acerca de las acciones de las políticas de IAM para Amazon Redshift, consulte [Administración del acceso a los recursos \(p. 307\)](#).

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para finalizar una consulta en ejecución

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione QUERIES (Consultas) y luego seleccione Queries and loads (Consultas y cargas) para mostrar la lista de consultas de su cuenta.
3. Seleccione la consulta en ejecución que quiera finalizar en la lista, y luego seleccione Terminate query (Finalizar consulta).

Consola original

Para finalizar una consulta en ejecución

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), seleccione el clúster que desee abrir.
4. Seleccione la pestaña Queries (Consultas).
5. Aplique alguna de las siguientes acciones:
 - En la lista, seleccione la consulta o consultas que desee terminar y haga clic en Terminate Query (Terminar consulta).
 - En la lista, abra una consulta si primero desea revisar su información y luego haga clic en Terminate Query (Terminar consulta).
6. En el cuadro de diálogo Terminate Queries (Terminar consultas), seleccione Confirm (Confirmar).

Visualización de detalles de consultas

Puede analizar los detalles de la consulta en la consola de Amazon Redshift. Con un identificador de consulta, puede consultar los detalles de una consulta. Los detalles pueden incluir, por ejemplo, el estado de finalización de la consulta, la duración, la instrucción SQL y si se trata de una consulta de usuario o una que ha sido reescrita por Amazon Redshift. A consulta de usuario es una consulta que se envía a Amazon Redshift, ya sea desde un cliente de SQL o generada por una herramienta de inteligencia empresarial. Es posible que Amazon Redshift reescriba la consulta para optimizarla, y esto puede dar lugar a varias consultas reescritas. Aunque realiza el proceso mediante Amazon Redshift, verá las consultas reescritas en la página de detalles de la consulta junto con la consulta de usuario.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para ver una consulta

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione QUERIES (Consultas) y luego seleccione Queries (Consultas) para mostrar la lista de consultas de su cuenta. Es posible que necesite cambiar los ajustes de esta página para encontrar su consulta.
3. Seleccione el identificador Query (Consulta) en la lista para mostrar los Query details (Detalles de la consulta).

La página Query details (Detalles de la consulta) incluye las pestañas Query details (Detalles de la consulta) y Query plan (Plan de la consulta) con métricas sobre la consulta.

Las métricas incluyen detalles sobre una consulta, como la hora de inicio, el ID de consulta, el estado y la duración. Otros detalles incluyen si una consulta se ejecutó en un clúster principal o en un clúster de escalado de simultaneidad y si se trata de una consulta primaria o reescrita.

Consola original

Puede ver los detalles de una consulta en particular haciendo clic en una consulta específica de la tabla de la página Queries (Consultas) para abrir la vista del **ID** de consulta. En la siguiente lista se describe la información disponible para consultas individuales:

- Query Properties (Propiedades de la consulta). Muestra un resumen de la información de la consulta, como el ID de consulta, el usuario de la base de datos que ejecutó la consulta, la duración y su estado. La propiedad Executed on (Ejecutado en) indica si la consulta se ejecutó en un clúster principal o en un clúster de escalado de simultaneidad.
- SQL. Muestra el texto de la consulta en un formato fácil de leer.
- Query Execution Details (Detalles de ejecución de la consulta). Muestra información acerca de cómo se procesó la consulta. Esta sección incluye los datos de ejecución reales y planificados de la consulta. La información de ejecución de la consulta no está disponible para las consultas que se ejecutan en un clúster de escalado de simultaneidad. Para obtener información acerca del uso de la sección Query Execution Details (Detalles de ejecución de la consulta), consulte [Análisis de ejecución de consulta](#) (p. 451).
- Cluster Performance During Query Execution (Desempeño del clúster durante la ejecución de la consulta). Muestra las métricas de rendimiento de CloudWatch. Para obtener información acerca del uso de la sección Cluster Performance During Query Execution (Desempeño del clúster durante la ejecución de la consulta), consulte [Visualización del rendimiento del clúster como consultas ejecutadas](#) (p. 458).

Cuando se abre, la vista Query (Consulta) tiene un aspecto similar al siguiente.

Cluster: -stcs
Configuration
Status
Cluster Performance
Database Performance
Queries
Loads
Table restore

Query 935623
Terminate Query

Query properties

Cluster	-stcs	Run time	6m 16.76s
Query ID	935623	Start time	Mon Mar 18 18:45:07 GMT-700 2019
Type	Query	End time	Mon Mar 18 18:51:23 GMT-700 2019
User	rsperf	Status	Completed
Executed on	Concurrency Scaling		

▼ SQL
Start time: Mon Mar 18 18:45:07 GMT-700 2019

```

with /* query_templates/query04.tpl.0 !CF:IR- */ stream_run_1.stream-
query.streams-0014.i0004.1.0:CF! */ year_total as ( select
  c_customer_id customer_id ,
  c_first_name customer_first_name ,
  c_last_name customer_last_name ,
  c_preferred_cust_flag customer_preferred_cust_flag ,
  c_birth_country customer_birth_country ,
  c_login customer_login ,
  c_email_address customer_email_address ,
  d_year dyear ,
  sum(((ss_ext_list_price-ss_ext_wholesale_cost-ss_ext_discount_amt)+ss_ext_sales_price)/2) year_total , 's'
sale_type from public.customer , public.store_sales , public.date_dim where c_customer_sk = ss_customer_sk and
ss_sold_date_sk = d_date_sk group by c_customer_id , c_first_name , c_last_name , c_preferred_cust_flag
, c_birth_country , c_login , c_email_address , d_year union all select c_customer_id customer_id , c_first_name
customer_first_name , c_last_name customer_last_name , c_preferred_cust_flag customer_preferred_cust_flag
, c_birth_country customer_birth_country , c_login customer_login , c_email_address customer_email_address , d_year
dyear , sum(((cs_ext_list_price-cs_ext_wholesale cost-cs_ext_discount_amt)+cs_ext_sales_price)/2) ) year_total
, 'c' sale_type from public.customer , public.catalog_sales , public.date_dim where c_customer_sk =
cs_bill_customer_sk and cs_sold_date_sk = d_date_sk group by c_customer_id , c_first_name , c_last_name
, c_preferred_cust_flag , c_birth_country , c_login , c_email_address , d_year union all select c_customer_id
customer_id , c_first_name customer_first_name , c_last_name customer_last_name , c_preferred_cust_flag
customer_preferred_cust_flag , c_birth_country customer_birth_country , c_login customer_login , c_email_address
customer_email_address , d_year dyear , sum(((ws_ext_list_price-ws_ext_wholesale cost-
ws_ext_discount_amt)+ws_ext_sales_price)/2) ) year_total , 'w' sale_type from public.customer , public.web_sales
, public.date_dim where c_customer_sk = ws_bill_customer_sk and ws_sold_date_sk = d_date_sk group by c_customer_id
, c_first_name , c_last_name , c_preferred_cust_flag , c_birth_country , c_login , c_email_address , d_year ) select
t_s_secyear.customer_id , t_s_secyear.customer_first_name , t_s_secyear.customer_last_name
, t_s_secyear.customer_email_address from year_total t_s_firstyear , year_total t_s_secyear , year_total
t_c_firstyear , year_total t_c_secyear , year_total t_w_firstyear , year_total t_w_secyear where
t_s_secyear.customer_id = t_s_firstyear.customer_id and t_s_firstyear.customer_id = t_c_secyear.customer_id and
t_s_firstyear.customer_id = t_c_firstyear.customer_id and t_s_firstyear.sale_type = 's' and
t_c_firstyear.sale_type = 'c' and t_w_firstyear.sale_type = 'w' and t_s_secyear.sale_type = 's' and
t_c_secyear.sale_type = 'c' and t_w_secyear.sale_type = 'w' and t_s_firstyear.dyear = 1999 and t_s_secyear.dyear =
1999+1 and t_c_firstyear.dyear = 1999 and t_c_secyear.dyear = 1999+1 and t_w_firstyear.dyear = 1999 and
t_w_secyear.dyear = 1999+1 and t_s_firstyear.year_total > 0 and t_c_firstyear.year_total > 0 and
t_w_firstyear.year_total > 0 and case when t_c_firstyear.year_total > 0 then t_c_secyear.year_total /
t_c_firstyear.year_total else null end > case when t_s_firstyear.year_total > 0 then t_s_secyear.year_total /
t_s_firstyear.year_total else null end and case when t_c_firstyear.year_total > 0 then t_c_secyear.year_total /
t_c_firstyear.year_total else null end > case when t_w_firstyear.year_total > 0 then t_w_secyear.year_total /
t_w_firstyear.year_total else null end order by t_s_secyear.customer_id , t_s_secyear.customer_first_name
, t_s_secyear.customer_last_name , t_s_secyear.customer_email_address limit 100;

```

► Query execution details

Análisis de ejecución de consulta

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para analizar una consulta

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione QUERIES (Consultas) y luego seleccione Queries and loads (Consultas y cargas) para mostrar la lista de consultas de su cuenta. Es posible que necesite cambiar los ajustes de esta página para encontrar su consulta.
3. Seleccione el identificador Query (Consulta) en la lista para mostrar los Query details (Detalles de la consulta).

La página Query details (Detalles de la consulta) incluye las pestañas Query details (Detalles de la consulta) y Query plan (Plan de la consulta) con métricas sobre la consulta.

Note

También puede desplazarse a la página Detalles de la consulta desde una página de Detalles del clúster, pestaña Historial de consultas al profundizar en una consulta en un gráfico Tiempo de ejecución de consultas.

La página Detalles de la consulta contiene las siguientes secciones:

- Una lista de Consultas reescritas, como se muestra en la siguiente captura de pantalla.

Rewritten queries(5)					
This query was rewritten by Amazon Redshift for optimization					
	Start time	Query	Status	Duration	
☐	Apr 15th, 2020 01:44:44 PM 6 days ago	122927,122928,122929...	✓ Completed	5 min	
☒	Apr 15th, 2020 01:44:44 PM 6 days ago	122927	✓ Completed	4 sec	
☐	Apr 15th, 2020 01:44:48 PM 6 days ago	122928	✓ Completed	22 ms	
☐	Apr 15th, 2020 01:44:48 PM 6 days ago	122929	✓ Completed	19 ms	
☐	Apr 15th, 2020 01:44:48 PM 6 days ago	122931	✓ Completed	5 min	

- Una sección de Detalles de la consulta, como se muestra en la siguiente captura de pantalla.

Query details		
Query ID	Cluster	User
122927	✓ dnd-sudhare-qa	
From April 15, 2020 at 01:44:44 PM To April 15, 2020 at 01:44:48 PM		

- Una pestaña Detalles de la consulta que contiene el SQL que se ejecutó y Detalles de ejecución sobre la ejecución.
- Una pestaña Plan de consulta que contiene los pasos del Plan de consulta y otra información sobre el plan de consulta. Esta tabla también contiene gráficos sobre el clúster cuando se ejecutó la consulta.
- Estado del clúster

Cluster health status

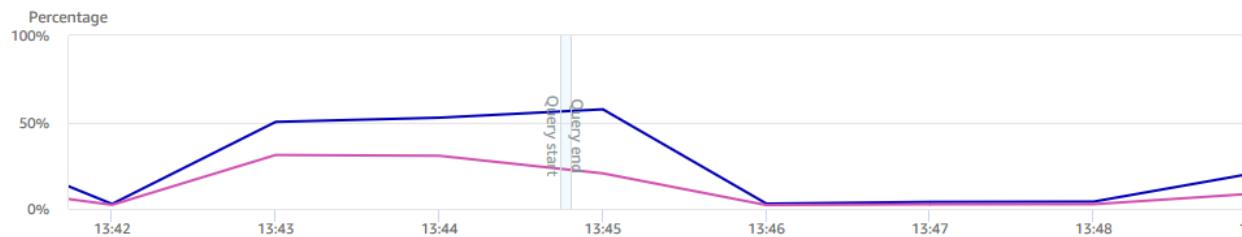
Cluster health during the workload.



- Utilización de la CPU

CPU utilization

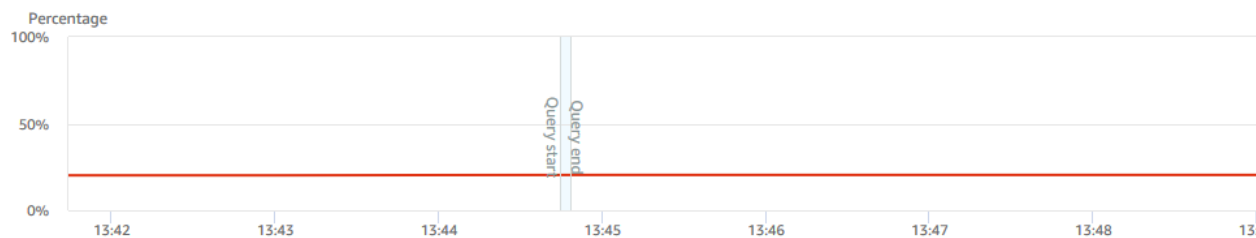
The CPU utilization of the cluster by leader node and average of compute nodes.



- Capacidad de almacenamiento utilizada

Storage capacity used

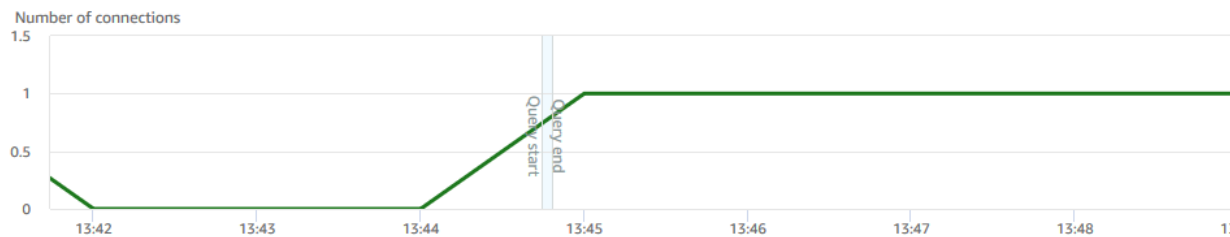
The percent of the storage capacity used.



- Conexiones de base de datos activas

Active database connections

The number of active database connections to the cluster.



Consola original

Visualización de detalles de ejecución de consultas

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), seleccione el clúster cuyos detalles de ejecución de consultas desee ver.
4. Seleccione la pestaña Queries (Consultas) y abra la consulta cuyos datos de desempeño desee ver.
5. Amplíe la sección Query Execution Details (Detalles de ejecución de la consulta) y realice las siguientes operaciones:
 - a. En la pestaña Plan, revise el plan de explicación de la consulta. En algunos casos, verá que el plan de explicación difiere de la ejecución real de la consulta de la pestaña Actual (Real). De ser así, es posible que deba ejecutar ANALYZE para actualizar las estadísticas o realizar otro mantenimiento en la base de datos para optimizar las consultas que ejecute. Para obtener más información acerca de la optimización de consultas, consulte [Ajuste del rendimiento de las consultas](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.
 - b. En la pestaña Actual (Real), revise los datos de desempeño asociados a cada uno de los nodos del plan de la ejecución de la consulta. Puede elegir un nodo individual del plan en la jerarquía para ver los datos de rendimiento asociados a ese nodo específico del plan. Estos datos incluyen los datos de rendimiento reales y estimados.
 - c. En la pestaña Metrics (Métricas), revise las métricas de cada uno de los nodos del clúster.

La sección Query Execution Details (Detalles de ejecución de la consulta) de la vista Query (Consulta) contiene información sobre el modo en que se procesó la consulta. Esta sección combina datos de [SVL_QUERY_REPORT](#), [STL_EXPLAIN](#) y otras vistas y tablas del sistema.

La sección Query Execution Details (Detalles de ejecución de la consulta) tiene tres pestañas:

- Plan. En esta pestaña se muestra el plan de explicación de la consulta que se visualiza.

▼ Query execution details

Plan Actual Metrics

```
XN Merge (cost=2000001005655.84..2000001005655.86 rows=10 width=27)
-> XN Network (cost=2000001005655.84..2000001005655.86 rows=10 width=27)
-> XN Sort (cost=2000001005655.84..2000001005655.86 rows=10 width=27)
-> XN Hash Join DS_DIST_INNER (cost=1000000004530.79..1000001005655.67 rows=10 width=27)
-> XN Seq Scan on users (cost=0.00..499.90 rows=49990 width=23)
-> XN Hash (cost=1000000004530.77..1000000004530.77 rows=10 width=12)
-> XN Subquery Scan q (cost=1000000004530.64..1000000004530.77 rows=10 width=12)
-> XN Limit (cost=1000000004530.64..1000000004530.67 rows=10 width=6)
-> XN HashAggregate (cost=2586.84..2651.00 rows=25665 width=6)
-> XN Seq Scan on sales (cost=0.00..1724.56 rows=172456 width=6)
```

La información de la pestaña Plan es la misma que se obtiene al ejecutar el comando EXPLAIN en la base de datos. El comando EXPLAIN examina el texto de la consulta y devuelve el plan de consulta. Utilice esta información para evaluar consultas y revisarlas para su eficacia y rendimiento si es necesario. El comando EXPLAIN no ejecuta propiamente la consulta.

En el ejemplo siguiente se muestra una consulta que devuelve los cinco mejores vendedores de San Diego. El resultado se basa en el número de tickets vendidos en 2008 y el plan de consulta para esa consulta.

```
explain
```

```
select sellerid, username, (firstname || ' ' || lastname) as name,  
city, sum(qtysold)  
from sales, date, users  
where sales.sellerid = users.userid  
and sales.dateid = date.dateid  
and year = 2008  
and city = 'San Diego'  
group by sellerid, username, name, city  
order by 5 desc  
limit 5;
```

QUERY PLAN
XN HashAggregate (cost=10347367091.97..10347367466.90 rows=49990 width=24)
-> XN Hash Join DS_DIST_OUTER (cost=624.88..10347366229.69 rows=172456 width=24)
Outer Dist Key: s.buyerid
Hash Cond: ("outer".buyerid = "inner".userid)
-> XN Seq Scan on sales s (cost=0.00..1724.56 rows=172456 width=16)
-> XN Hash (cost=499.90..499.90 rows=49990 width=16)
-> XN Seq Scan on users u (cost=0.00..499.90 rows=49990 width=16)

Para obtener más información acerca de cómo entender el plan de explicación, consulte [Análisis del plan de explicación](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

Cuando ejecuta la consulta (omitiendo el comando EXPLAIN), el motor puede encontrar formas de optimizar el rendimiento de la consulta y cambiar el modo en el que la procesa. Los datos de desempeño real de la consulta se almacenan en las vistas del sistema, como [SVL_QUERY_REPORT](#) y [SVL_QUERY_SUMMARY](#).

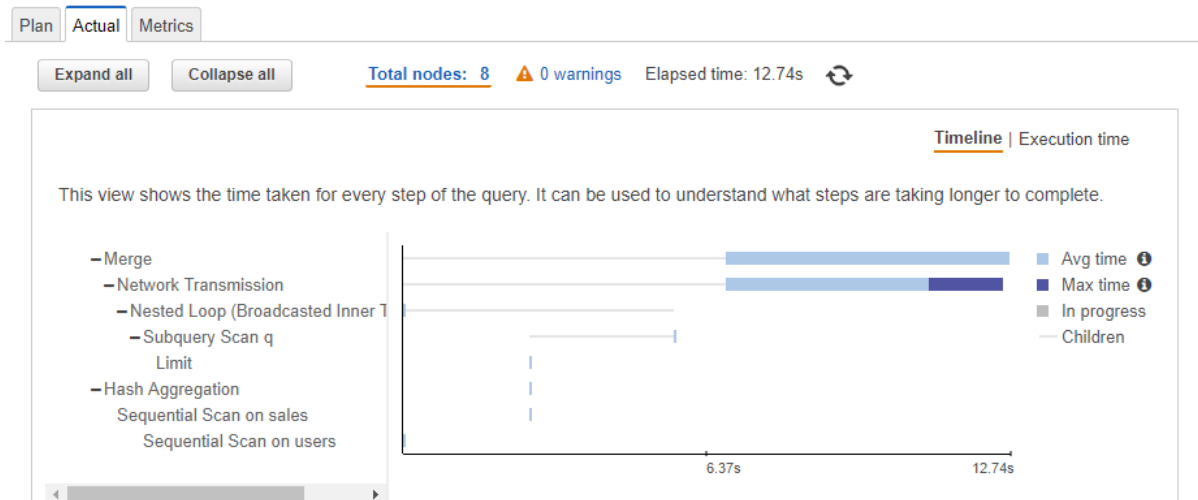
La consola de Amazon Redshift utiliza una combinación de [STL_EXPLAIN](#), [SVL_QUERY_REPORT](#) y otras tablas y vistas del sistema para presentar el desempeño real de la consulta y compararlo con el plan de explicación de la consulta. Esta información aparece en la pestaña Actual (Real). En algunos casos, verá que el plan de explicación y los pasos de ejecución reales de la consulta difieren. De ser así, es posible que deba realizar algunas operaciones en la base de datos, como [ANALYZE](#), para actualizar las estadísticas y hacer que el plan de explicación sea más eficaz.

Además, a veces el optimizador de consultas separa en partes las consultas complejas de SQL y crea tablas temporales con la convención de nomenclatura `volt_tt_guid` para procesar la consulta con más eficacia. En este caso, tanto el plan de explicación como el resumen de ejecución real de la consulta aplican a la última instrucción que se ejecutó. Puede revisar los ID de consultas anteriores para ver el plan de explicación y el resumen de ejecución real de la consulta para cada una de las partes correspondientes de la consulta.

Para obtener más información acerca de la diferencia entre el plan de explicación y las vistas y registros del sistema, consulte [Análisis del resumen de consultas](#) en la Guía para desarrolladores de bases de datos Amazon Redshift.

- Actual (Real). En esta pestaña se muestran los pasos y estadísticas reales de la consulta que se ejecutó. Estos datos se muestran en una jerarquía textual y en los diagramas visuales de Timeline (Línea temporal) y Execution time (Tiempo de ejecución).

▼ Query execution details



En la vista Timeline (Línea temporal), se muestra la secuencia en la que se ejecutan los pasos reales de la consulta.

En la vista Execution time (Tiempo de ejecución), se muestra el tiempo que tarda cada paso de la consulta. Este dato se puede utilizar para saber qué pasos tardan más en completarse.

En cada vista, aparece Avg time (Tiempo medio) y Max time (Tiempo máximo).

La estadística Avg (Promedio) muestra el tiempo medio de ejecución de este paso en los sectores de datos y el porcentaje de tiempo total de ejecución de la consulta que representa. La estadística Max muestra el tiempo de ejecución más largo de este paso en cualquiera de los sectores de datos y la desviación. El valor de skew (desviación) es la diferencia entre el tiempo medio y el tiempo máximo del paso.

Le recomendamos que investigue un paso si ambas condiciones son verdaderas. Una condición es que el tiempo de ejecución máximo es claramente más del doble del tiempo de ejecución medio a lo largo de varias ejecuciones de la consulta. La otra condición es que el paso también requiere una cantidad importante de tiempo. Un ejemplo es que es uno de los tres primeros pasos en tiempo de ejecución en una consulta grande.

Note

En la medida de lo posible, debe ejecutar una consulta dos veces para ver cuáles es su información de ejecución habitual. La compilación añade un trabajo adicional a la primera ejecución de la consulta que no estará presente en las ejecuciones posteriores.

Puede elegir cualquier barra del gráfico para comparar los datos estimados del plan de explicación con el rendimiento real de la consulta, como se muestra a continuación.

Hash				
Plan Node Hash				
Estimated		Actual		
Cost	624.88 (0.00% of total)	Time including children	86ms (21% of total)	
Rows	48	Own Time (Avg)	83ms (20% of total)	
Width	47 bytes	Own Time (Max)	121ms (45% skew)	
Step	Rows scanned	Rows returned	Bytes returned	Working memory
Project	-	188	0 bytes	0 bytes
Hash	-	188	13.92 KB	685.77 MB

Si el optimizador de consultas publicó alertas para la consulta en la tabla de sistema [STL_ALERT_EVENT_LOG](#), los nodos del plan asociados a las alertas se marcan con un icono de alerta.

▼ Query execution details

Plan Actual Metrics

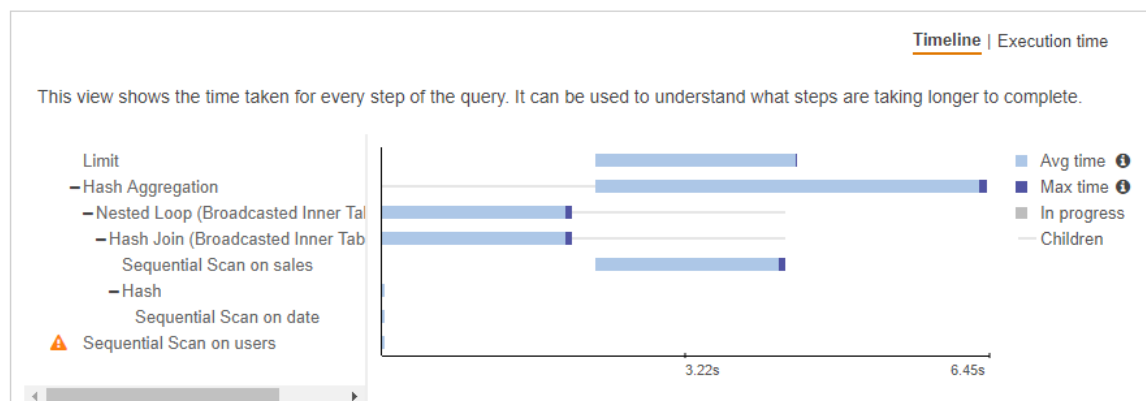
Expand all

Collapse all

Total nodes: 8

2 warnings

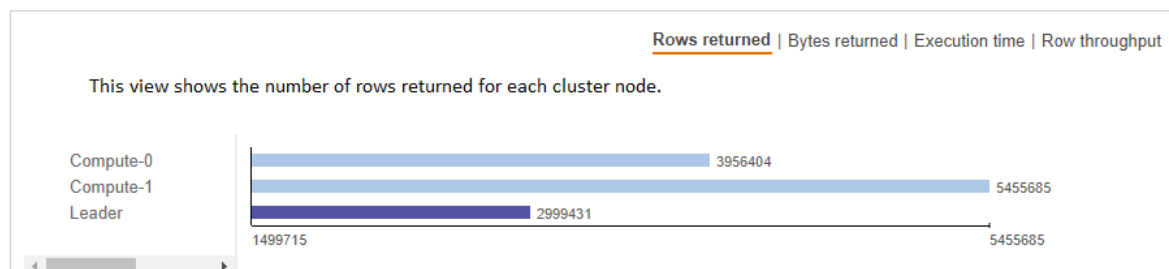
Elapsed time: 6.45s



- Metrics (Métricas). En esta pestaña se muestran las métricas de la consulta que se ejecutó.

▼ Query execution details

Plan Actual Metrics



La métrica Rows returned (Filas devueltas) es la suma del número de filas generadas durante cada paso de la consulta.

La métrica Bytes returned (Bytes devueltos) muestra el número de bytes devuelto por cada nodo del clúster.

La métrica Execution time (Tiempo de ejecución) muestra el tiempo de ejecución de la consulta en cada nodo del clúster.

La métrica Row throughput (Velocidad de fila) muestra el número de filas devuelto dividido por el tiempo de ejecución de la consulta de cada nodo del clúster.

Si la ejecución de una consulta es más lenta de lo esperado, puede utilizar la pestaña Metrics (Métricas) para solucionar el problema. Consulte la métrica Row throughput (Velocidad de fila). Si uno de los nodos del clúster parece tener una velocidad de fila mucho mayor que los otros nodos, esto indica que la carga de trabajo no está distribuida uniformemente entre los nodos del clúster. Una posible causa podría ser que los datos no están distribuidos uniformemente o están descompensados entre los sectores del nodo. Para obtener más información, consulte [Identificación de tablas con sesgo de datos o con filas desordenadas](#).

Si los datos están distribuidos uniformemente, la consulta podría estar utilizando como filtro filas que se encuentran principalmente en ese nodo. Para solucionar este problema, analice los estilos de distribución de las tablas de la consulta y determine si se puede hacer alguna mejora. Recuerde comparar el rendimiento de esta consulta con el rendimiento de otras consultas importantes y con el sistema en general antes de implementar cualquier cambio. Para obtener más información, consulte [Selección de un estilo de distribución de datos](#).

Note

La pestaña de métricas no está disponible para un clúster de un solo nodo.

Visualización del rendimiento del clúster como consultas ejecutadas

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para mostrar el rendimiento del clúster como consultas ejecutadas

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluir Rendimiento del clúster, Supervisión de consultas, Bases de datos, Comparticiones de datos, Schedules, Mantenimiento, y Propiedades pestañas.
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver más detalles.

Para obtener más información, consulte [Visualización de datos del historial de consultas \(p. 438\)](#).

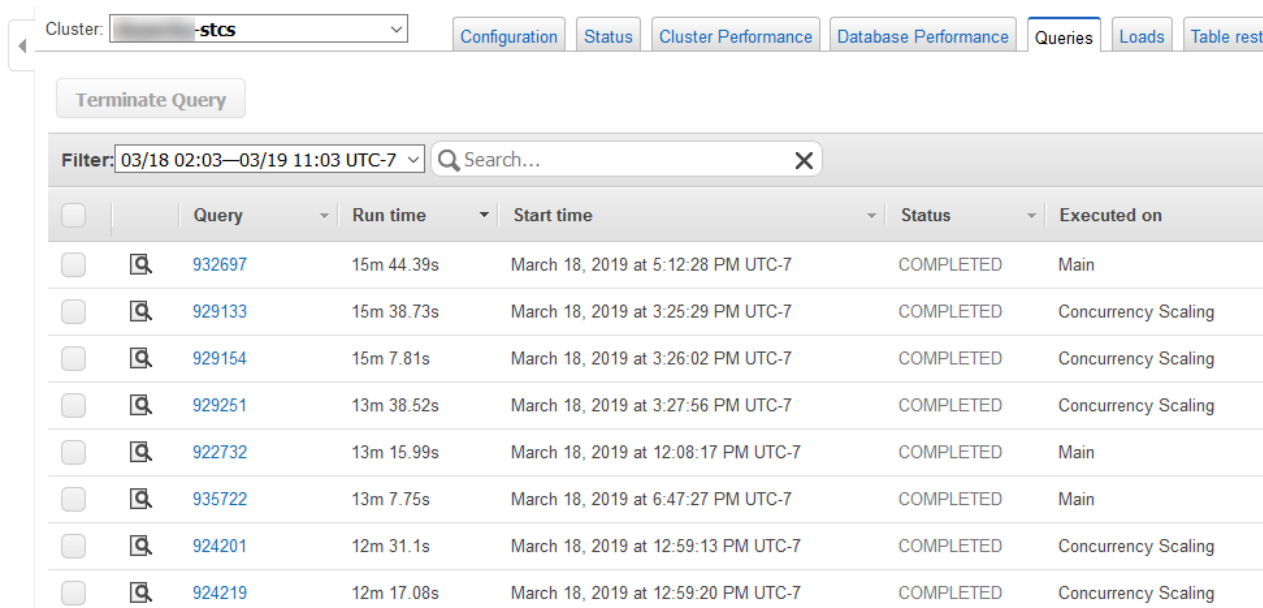
Consola original

En la vista Query puede utilizar la sección Cluster Performance During Query Execution para ver las métricas de clúster durante la ejecución de la consulta. Al hacerlo, podrá identificar consultas con mal rendimiento, buscar consultas con cuellos de botella y determinar si necesita cambiar el tamaño del clúster para la carga de trabajo.

Visualización de métricas de clúster durante la ejecución de consultas

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), elija el clúster cuyo desempeño durante la ejecución de consultas desee ver.
4. Seleccione la pestaña Queries (Consultas).
5. En la lista de consultas, busque la consulta con la que desea trabajar y elija el ID de la consulta en la columna Query (Consulta).

En el siguiente ejemplo, las consultas están ordenadas por Run time (Tiempo de ejecución) para buscar aquellas con el máximo tiempo de ejecución.



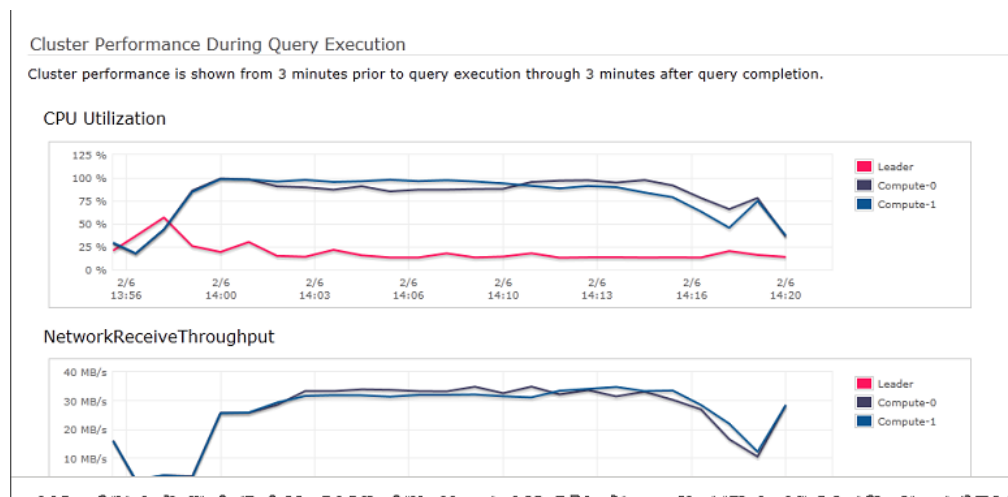
Cluster: stcs		Configuration	Status	Cluster Performance	Database Performance	Queries	Loads	Table rest
Terminate Query								
Filter: 03/18 02:03—03/19 11:03 UTC-7		Search...						
	Query	Run time	Start time	Status	Executed on			
☐	 932697	15m 44.39s	March 18, 2019 at 5:12:28 PM UTC-7	COMPLETED	Main			
☐	 929133	15m 38.73s	March 18, 2019 at 3:25:29 PM UTC-7	COMPLETED	Concurrency Scaling			
☐	 929154	15m 7.81s	March 18, 2019 at 3:26:02 PM UTC-7	COMPLETED	Concurrency Scaling			
☐	 929251	13m 38.52s	March 18, 2019 at 3:27:56 PM UTC-7	COMPLETED	Concurrency Scaling			
☐	 922732	13m 15.99s	March 18, 2019 at 12:08:17 PM UTC-7	COMPLETED	Main			
☐	 935722	13m 7.75s	March 18, 2019 at 6:47:27 PM UTC-7	COMPLETED	Main			
☐	 924201	12m 31.1s	March 18, 2019 at 12:59:13 PM UTC-7	COMPLETED	Concurrency Scaling			
☐	 924219	12m 17.08s	March 18, 2019 at 12:59:20 PM UTC-7	COMPLETED	Concurrency Scaling			

6. En la página Query (Consulta) que se abre, desplácese hasta la sección Cluster Performance During Query Execution (Desempeño del clúster durante la ejecución de la consulta) para ver las métricas del clúster.

En el siguiente ejemplo, las métricas `CPUtilization` y `NetworkReceiveThroughput` se muestran por el tiempo que esta consulta estuvo en ejecución.

Tip

Puede cerrar los detalles de las secciones Query Execution Details (Detalles de ejecución de la consulta) o SQL para administrar la cantidad de información que se muestra en el panel.



Visualización de métricas de clúster durante las operaciones de carga

Cuando observa el rendimiento del clúster durante las operaciones de carga, puede identificar consultas que estén consumiendo recursos y tomar medidas para mitigar su efecto. Puede terminar una carga si no desea que se complete su ejecución.

Note

La función para terminar consultas y cargas en la consola de Amazon Redshift requiere un permiso específico. Si desea que los usuarios puedan terminar consultas y cargas, asegúrese de añadir la acción `redshift:CancelQuerySession` a la política de AWS Identity and Access Management (IAM). Este requisito se aplica tanto si selecciona la opción **Sólo lectura de Amazon Redshift AWS** o cree una directiva personalizada en IAM. Los usuarios que tienen el **Acceso completo a Amazon Redshift** ya cuentan con los permisos necesarios para terminar las consultas y las cargas. Para obtener más información acerca de las acciones de las políticas de IAM para Amazon Redshift, consulte [Administración del acceso a los recursos](#) (p. 307).

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de **New console** (Nueva consola) o **Original console** (Consola original) en función de la consola que utilice. Las instrucciones de **New console** (Nueva consola) están abiertas de forma predeterminada.

New console

Para mostrar el rendimiento del clúster durante operaciones de carga

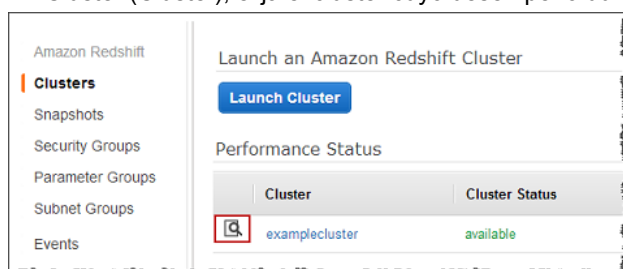
1. Inicie sesión en **AWS Management Console** y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, seleccione **CLUSTERS (CLÚSTERES)** y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluir **Rendimiento del clúster**, **Supervisión de consultas**, **Bases de datos**, **Comparticiones de datos**, **Schedules**, **Mantenimiento**, y **Propiedades** pestañas.
3. Seleccione la pestaña **Query monitoring (Supervisión de consultas)** para ver más detalles.

- En la sección Queries and loads (Consultas y cargas), seleccione Loads (Cargas) para ver las operaciones de carga de un clúster. Si se está ejecutando una carga, puede terminarla seleccionando Terminate query (Terminar consulta).

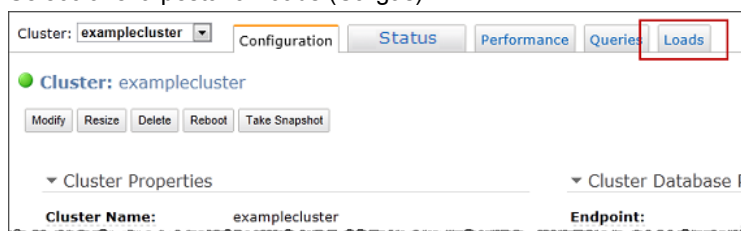
Consola original

Visualización de métricas de clúster durante las operaciones de carga

- Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
- En el panel de navegación, elija Clusters (Clústeres).
- En Cluster (Clúster), elija el clúster cuyo desempeño durante la ejecución de consultas desee ver.



- Seleccione la pestaña Loads (Cargas).



- En la lista de cargas, busque la operación de carga con la que desea trabajar y elija el ID de la carga en la columna Load (Carga).

Cluster:	examplecluster	Configuration	Status	Performance	Queries	Loads
Time Range: 02/05 14:49—02/06 14:49 UTC-8 (Last 24 Hours)						
Load	Run time	Start time	Status	Completion	User	SQL
79679	8.61s	Tue Feb 05 16:25:17 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE users
79738	4.77s	Tue Feb 05 16:26:40 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE venue
79759	6.84s	Tue Feb 05 16:27:08 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE catego
79779	7.31s	Tue Feb 05 16:27:35 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE date
79810	9.08s	Tue Feb 05 16:28:14 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE event
79839	8.3s	Tue Feb 05 16:28:46 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE listing
79874	4.64s	Tue Feb 05 16:29:32 GMT-800	COMPLETED	100%	masterus	COPY ANALYZE sales

- En la nueva pestaña Query (Consulta) que se abre, puede ver los detalles de la operación de carga.

En este momento, puede trabajar con la pestaña Query (Consulta), tal y como se muestra en [Visualización de consultas y cargas \(p. 448\)](#). Puede revisar los detalles de la consulta y ver los valores de las métricas de clúster durante la operación de carga.

Terminación de una carga en ejecución

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), seleccione el clúster que desee abrir.
4. Seleccione la pestaña Loads (Cargas).
5. Aplique alguna de las siguientes acciones:
 - En la lista, seleccione la carga o las cargas que desee terminar y haga clic en Terminate Load (Terminar carga).
 - En la lista, abra una carga si primero desea revisar su información y luego haga clic en Terminate Load (Terminar carga).
6. En el cuadro de diálogo Terminate Loads (Terminar cargas), seleccione Confirm (Confirmar).

Análisis del rendimiento de las cargas de trabajo

Puede obtener una vista detallada del rendimiento de las cargas de trabajo consultando el gráfico de desglose de ejecuciones de cargas de trabajo en la consola. El gráfico se crea con datos proporcionados por la métrica QueryRuntimeBreakdown. Con este gráfico, puede ver cuánto tiempo pasan las consultas en las distintas fases de procesamiento, como la espera y la planificación.

Note

El gráfico de desglose de ejecuciones de cargas de trabajo no se muestra para clústeres de un nodo.

En la siguiente lista de métricas, se describen las distintas fases de procesamiento:

- `QueryPlanning`: tiempo invertido en analizar y optimizar instrucciones SQL.
- `QueryWaiting`: tiempo invertido en esperar en la cola de administración de carga de trabajo (WLM).
- `QueryExecutingRead`: tiempo invertido en ejecutar consultas de lectura.
- `QueryExecutingInsert`: tiempo invertido en ejecutar consultas de inserción.
- `QueryExecutingDelete`: tiempo invertido en ejecutar consultas de eliminación.
- `QueryExecutingUpdate`: tiempo invertido en ejecutar consultas de actualización.
- `QueryExecutingCtas`: tiempo invertido en ejecutar consultas CREATE TABLE AS.
- `QueryExecutingUnload`: tiempo invertido en ejecutar consultas de descarga.
- `QueryExecutingCopy`: tiempo invertido en ejecutar consultas de copia.

Por ejemplo, el gráfico siguiente de la consola de Amazon Redshift muestra la cantidad de tiempo que las consultas han dedicado a las fases de planificación, espera, lectura y escritura. Puede combinar los resultados de este gráfico con otras métricas para ampliar el análisis. En algunos casos, el gráfico podría mostrar que las consultas con una duración corta (medida con la métrica `QueryDuration`) están esperando mucho tiempo en la fase de espera. En estos casos, puede aumentar la tasa de simultaneidad de WLM para una cola determinada con el fin de aumentar el rendimiento.

Note

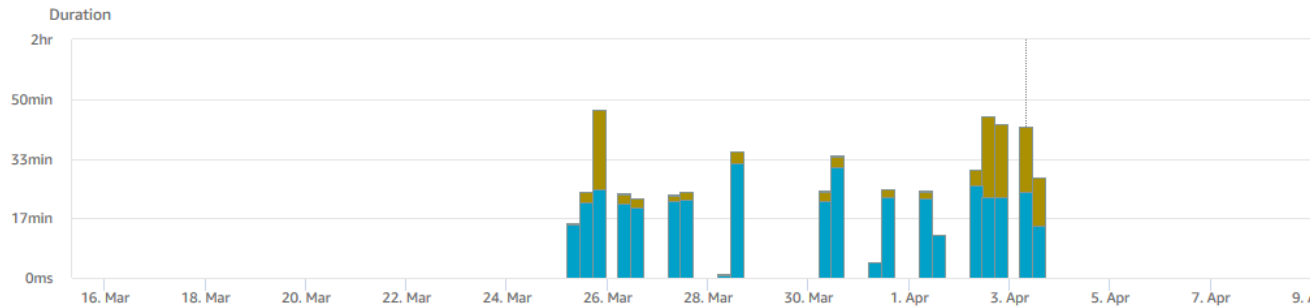
Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

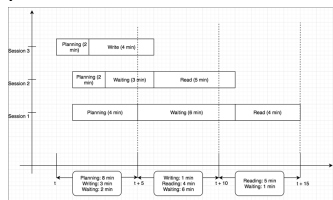
A continuación, se muestra un ejemplo del gráfico de desglose de la ejecución de la carga de trabajo. En el gráfico, el valor del eje Y es la duración media de cada etapa en el tiempo especificado que se muestra como gráfico de barras apiladas.

Workload execution breakdown

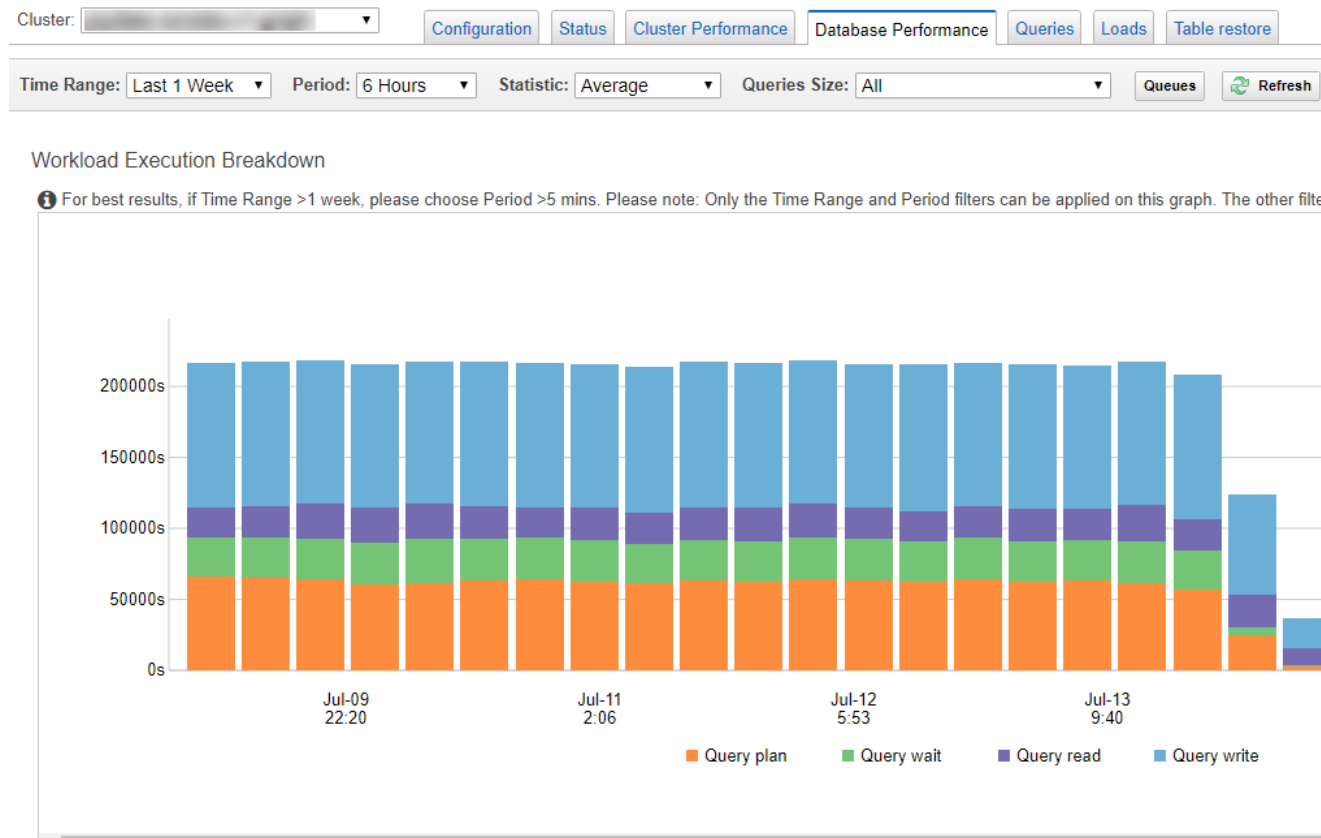
The time used in query processing stages.



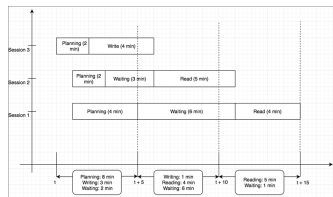
En el diagrama siguiente se ilustra el modo en que Amazon Redshift agrega el procesamiento de consultas para las sesiones simultáneas.



Consola original

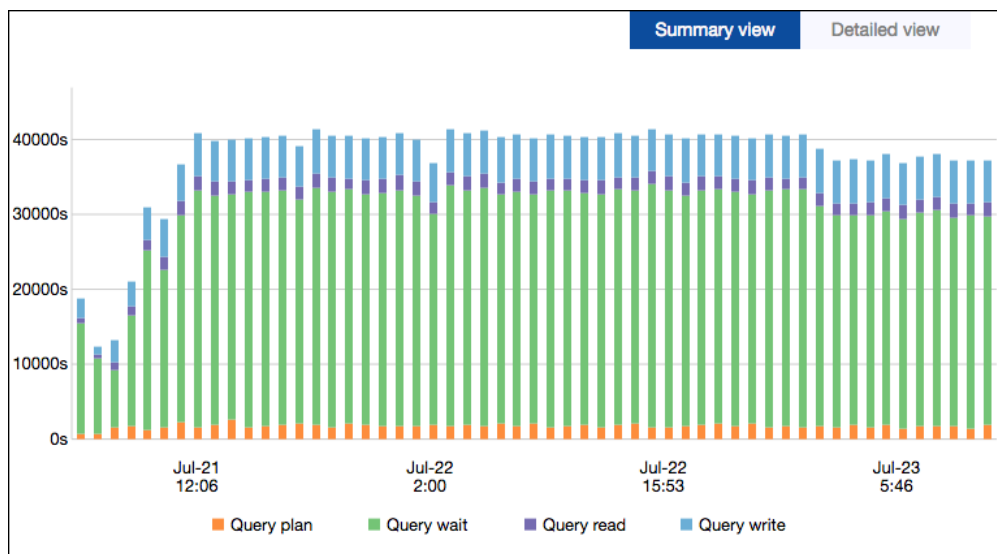


El eje Y del diagrama es acumulativo para todas las sesiones que se ejecutan durante el periodo de tiempo seleccionado. En el diagrama siguiente se ilustra el modo en que Amazon Redshift agrega el procesamiento de consultas para las sesiones simultáneas.

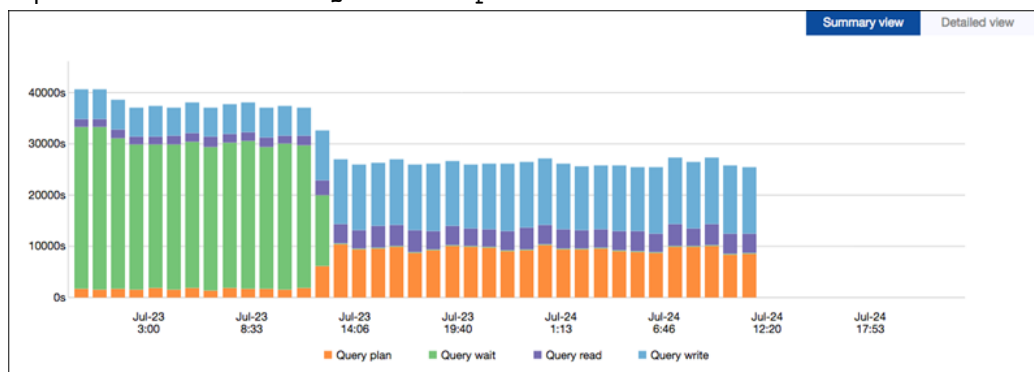


Ejemplo de análisis con el gráfico de desglose de ejecuciones de cargas de trabajo

Los diagramas siguientes ilustran cómo se puede utilizar el gráfico de desglose de ejecuciones de cargas de trabajo para optimizar el rendimiento del clúster. En el primer gráfico de ejemplo, se puede ver que la mayoría del tiempo de las consultas se empleó en la fase `queryWaiting`. Este efecto se debió a un valor bajo de simultaneidad de WLM.



El gráfico siguiente ilustra el desglose del tiempo de ejecución de las consultas después de ajustar la simultaneidad a un valor más alto. En el gráfico actualizado, se puede observar que la mayor parte del tiempo utilizado ha pasado de la fase `QueryWaiting` a las fases `QueryExecutingRead` y `QueryPlanning`. En este caso, se emplea una mayor proporción de tiempo en la fase de planificación, porque ahora se están ejecutando más consultas durante el intervalo de tiempo después de ajustar la simultaneidad. Puede comprobar el número de consultas que se ejecutan durante un periodo de tiempo específico con la métrica `WLMQueriesCompletedPerSecond`.



Estos gráficos demuestran cómo el cambio en la configuración del clúster afecta la cantidad de tiempo que pasan las consultas en las distintas fases. En el caso anterior, las consultas pasaban inicialmente un tiempo relativamente largo esperando, porque la configuración de simultaneidad era baja. Después de aumentar la simultaneidad, se procesan más consultas en paralelo, por lo que disminuye el tiempo de espera y aumenta el rendimiento de las consultas.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para mostrar el gráfico de desglose de la carga de trabajo del clúster

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.

2. En el menú de navegación, seleccione CLUSTERS (CLÚSTERES) y seleccione el nombre del clúster de la lista para abrir sus detalles. Se muestran los detalles del clúster, que pueden incluir Rendimiento del clúster, Supervisión de consultas, Bases de datos, Comparticiones de datos, Schedules, Mantenimiento, y Propiedades pestañas.
3. Seleccione la pestaña Query monitoring (Supervisión de consultas) para ver las métricas de sus consultas.
4. En la sección Monitoreo de consultas, elija Rendimiento de la base de datos y elija Métricas del clúster.

Las siguientes métricas muestran gráficos para el rango de tiempo seleccionado como un gráfico de barras apilado:

- Tiempo de planificación
- Tiempo de espera
- Hora de confirmación
- Hora de ejecución

Consola original

Visualización del gráfico de desglose de cargas de trabajo

Puede ver el gráfico de desglose de cargas de trabajo en la consola.

Para ver el gráfico de desglose de ejecuciones de cargas de trabajo

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. Seleccione Clusters (Clústeres) en el panel de navegación.
3. Elija el clúster que desea analizar.
4. Seleccione la pestaña Database Performance (Desempeño de la base de datos).

Creación de una alarma

Las alarmas que crea en la consola de Amazon Redshift son alarmas de CloudWatch. Las alarmas son útiles porque le ayudan a tomar decisiones proactivas sobre el clúster y las bases de datos. Puede establecer una o más alarmas en cualquiera de las métricas enumeradas en [Supervisión de Amazon Redshift mediante las métricas de CloudWatch \(p. 422\)](#). Por ejemplo, establecer una alarma para una `CPUtilization` alta en un nodo del clúster ayuda a indicar los momentos en los que el nodo está sobrecargado. Del mismo modo, establecer una alarma para una `CPUtilization` baja en un nodo del clúster ayuda a indicar los momentos en los que el nodo está infrautilizado.

En esta sección se explica cómo crear una alarma mediante la consola de Amazon Redshift. Puede crear una alarma mediante la consola de CloudWatch o mediante cualquier otra forma en la que trabaje con métricas, como en la AWS CLI o un AWSSDK. Para eliminar una alarma, debe utilizar la consola de CloudWatch.

Note

Una nueva consola está disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

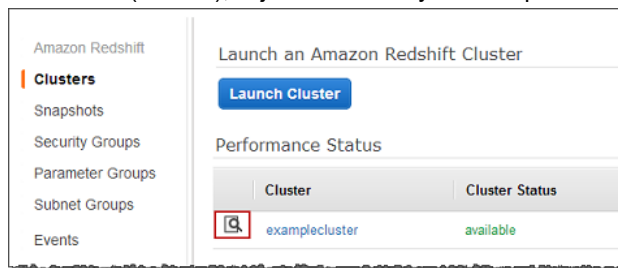
Para crear una alarma de CloudWatch con la consola de Amazon Redshift

1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija ALARMS (Alarmas). A continuación, elija Create alarm (Crear alarma).
3. En la páginaCreación de alarma, introduzca las propiedades para crear una alarma de CloudWatch.
4. Elija Create alarm (Crear alarma).

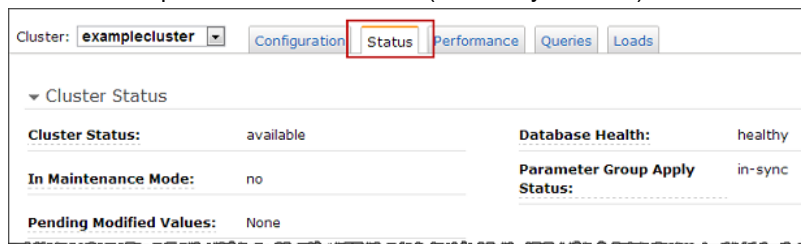
Consola original

Creación de una alarma en una métrica de clúster en la consola de Amazon Redshift

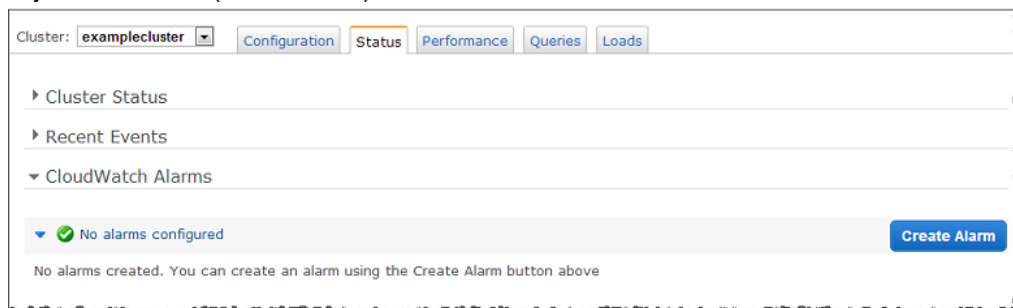
1. Inicie sesión enAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, elija Clusters (Clústeres).
3. En Cluster (Clúster), elija el clúster cuyo desempeño durante la ejecución de consultas desee ver.



4. Seleccione la pestaña Events+Alarms (Eventos y alarmas).



5. Elija Create Alarm (Crear alarma).



6. En el cuadro de diálogo Create Alarm (Crear alarma), configure una alarma y seleccione Create (Crear).

Note

Las notificaciones que se muestran Enviar una notificación a Los temas de Amazon Simple Notification Service (Amazon SNS). Para obtener más información acerca de Amazon SNS y la creación de temas, consulte [Crear un tema](#) en la Amazon Simple Notification Service. Si no tiene temas en Amazon SNS, puede crear uno en el cuadro de diálogo Create Alarm (Crear alarma) haciendo clic en la casilla [Crear tema](#) Enlace a.

Los detalles de la alarma variarán según sus circunstancias. A continuación se incluye un ejemplo de la utilización media de la CPU de un nodo (Compute-0) que tiene una alarma establecida. Si la CPU supera el 80 por ciento durante cuatro períodos consecutivos de cinco minutos, esta alarma envía una notificación al tema redshift-example-cluster-alarms.

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define. To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☒ **Send a notification to:** redshift-example-cluster-alarms [create topic](#)

Whenever: Average of CPUUtilization-Compute-0

Is: >= 80 %

For at least: 4 consecutive period(s) of 5 Minutes

Name of alarm:

[Cancel](#) [Create](#)

CPUUtilization-Compute-0 (%)

100
80
60
40
20
0

2/7 18:00 2/7 20:00 2/7 22:00

7. En la lista de alarmas, busque la alarma nueva.

Es posible que deba esperar unos instantes hasta que se recopilen los datos suficientes para determinar el estado de la alarma, tal como se muestra en el siguiente ejemplo.

CloudWatch Alarms

1 of 1 in INSUFFICIENT_DATA [Create Alarm](#)

Below are your CloudWatch alarms for the selected resources. Click on an alarm to edit it or click 'view' to see additional options and details in Amazon CloudWatch. [View all CloudWatch alarms](#)

State	Name	More Options
INSUFFICIENT_DATA	awsredshift-examplecluster-High-CPUUtilization-Compute-0	view

Poco después, el estado debería cambiar a OK.

CloudWatch Alarms

1 of 1 in OK [Create Alarm](#)

Below are your CloudWatch alarms for the selected resources. Click on an alarm to edit it or click 'view' to see additional options and details in Amazon CloudWatch. [View all CloudWatch alarms](#)

State	Name	More Options
OK		view

8. (Opcional) Elija `NombrePara` que la alarma cambie su configuración o seleccione el enlace «view (ver)» situado bajo `Más opciones` para ir a esta alarma en la consola de CloudWatch.

Uso de métricas de rendimiento en la consola de CloudWatch

Cuando trabaje con métricas de Amazon Redshift en la consola de CloudWatch, hay algunas cosas que debe tener en cuenta:

- Los datos de rendimiento de cargas y consultas están disponibles únicamente en la consola de Amazon Redshift.
- Algunas métricas de CloudWatch tienen unidades diferentes a las que se utilizan en la consola de Amazon Redshift. Por ejemplo, `writeThroughput` se muestra en GB/s (mientras que en lo hace en bytes/s de CloudWatch), que es una unidad más pertinente para el espacio de almacenamiento normal de un nodo.

Cuando trabaje con métricas de Amazon Redshift en la consola de CloudWatch, las herramientas de línea de comandos o un SDK de Amazon, tenga en cuenta estos conceptos:

1. Primero, especifique la dimensión de la métrica con la que va a trabajar. Una dimensión es un par de nombre-valor que le ayuda a identificar una métrica de forma inequívoca. Las dimensiones de Amazon Redshift son `ClusterIdentifier` y `NodeID`. En la consola de CloudWatch, seleccione `Redshift Cluster` y `Redshift Node` para seleccionar fácilmente dimensiones específicas de nodos y clústeres. Para obtener más información acerca de las dimensiones, consulte [Dimensiones](#) en la Guía para desarrolladores de CloudWatch.
2. Luego, especifique el nombre de métrica, como `ReadIOPS`.

En la tabla siguiente se resumen los tipos de dimensiones de métricas de Amazon Redshift que están disponibles para usted. En función de la métrica, los datos estarán disponibles en intervalos de 1 minuto o de 5 minutos sin ningún cargo adicional. Para obtener más información, consulte [Métricas de Amazon Redshift \(p. 422\)](#).

espacio de nombres de CloudWatch	Dimensión	Descripción
AWS/Redshift	NodeID	Filtra los datos solicitados que son específicos de los nodos de un clúster. <code>NodeID</code> puede ser "Leader (Principal)", "Shared (Compartido)", o "Compute-N (N-computación)", donde N puede ser 0, 1, etc. en función del número de nodos del clúster. "Shared" significa que el clúster tiene un solo nodo, es decir, que el nodo principal y el nodo de computación están combinados.
	ClusterIdentifier	Filtra los datos solicitados que son específicos del clúster. Las métricas específicas del clúster son <code>HealthStatus</code> , <code>MaintenanceMode</code> y <code>DatabaseConnections</code> . Las métricas generales de esta dimensión (por ejemplo, <code>ReadIOPS</code>), que también son métricas de nodos, representan el total acumulado de datos de métricas de nodos. Preste especial atención cuando interprete estas métricas, ya que incluyen el comportamiento acumulado tanto del nodo principal como de los nodos de computación.

Trabajar con métricas de gateway y de volumen es similar a trabajar con otras métricas de servicio. Muchas de las tareas comunes se describen en la documentación de CloudWatch, incluidas las siguientes:

- [Ver métricas disponibles](#)
- [Obtener estadísticas de una métrica](#)
- [Creación de alarmas de CloudWatch](#)

Eventos de Amazon Redshift

Temas

- [Overview \(p. 471\)](#)
- [Visualización de eventos mediante la consola \(p. 471\)](#)
- [Visualización de eventos mediante el panelAWS SDK for Java \(p. 473\)](#)
- [Visualización de eventos mediante laAWS CLI/API de Amazon Redshift \(p. 474\)](#)
- [Notificaciones de eventos de Amazon Redshift \(p. 475\)](#)

Overview

Amazon Redshift realiza un seguimiento de eventos y retiene información relacionada con ellos durante varias semanas en suAWSaccount. Para cada evento, Amazon Redshift informa información como la fecha en la que se produjo cada evento, una descripción de él, su origen (por ejemplo, un clúster, un grupo de parámetros o una snapshot) y el ID de origen.

Amazon Redshift proporciona una notificación con antelación para algunos eventos. Estos eventos tienen una categoría de evento de `pending`. Por ejemplo, enviamos una notificación con antelación si se requiere una actualización de hardware para alguno de los nodos de su clúster. Puede suscribirse a los eventos pendientes de la misma forma que a otros eventos de Amazon Redshift. Para obtener más información, consulte [Suscripción a notificaciones de eventos de Amazon Redshift \(p. 475\)](#).

Puede utilizar Amazon Redshift Management Console, la API de Amazon Redshift o laAWSSDK para obtener información de eventos. Puede obtener una lista de todos los eventos o aplicar filtros, como duración del evento o fecha de comienzo y finalización, para obtener la información de eventos en un período específico.

También puede obtener eventos generados por un tipo de origen específico, como eventos de clúster o de grupo de parámetros. LaFuente muestra el nombre de recurso y el tipo de recurso que desencadena una acción determinada.

Puede crear suscripciones a notificaciones de eventos de Amazon Redshift de que especifican un conjunto de filtros de eventos. Cuando se produce un evento que coincide con los criterios de filtro, Amazon Redshift utiliza Amazon Simple Notification Service para informarle activamente de que se ha producido el evento.

Para ver una lista de los eventos de Amazon Redshift de por categoría y tipo de origen, consulte [the section called "Categorías y mensajes de eventos de Amazon Redshift" \(p. 477\)](#)

Visualización de eventos mediante la consola

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

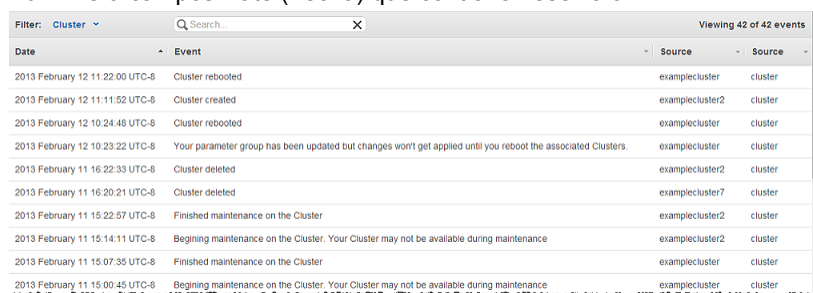
New console

Para ver eventos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, haga clic en EVENTS (EVENTOS).

Consola original

Para ver eventos en la consola de Amazon Redshift, seleccione **Eventos** en el panel de navegación. En la lista de eventos, puede filtrar los resultados mediante **Source Type** (Tipo de origen) o aplicar un valor de **Filter** (Filtro) personalizado que filtre el texto de todos los campos de la lista. Por ejemplo, si busca **12 Dec 2012** verá campos **Date** (Fecha) que contienen ese valor.



Date	Event	Source
2013 February 12 11:22:00 UTC-8	Cluster rebooted	examplecluster cluster
2013 February 12 11:11:52 UTC-8	Cluster created	examplecluster2 cluster
2013 February 12 10:24:48 UTC-8	Cluster rebooted	examplecluster cluster
2013 February 12 10:23:22 UTC-8	Your parameter group has been updated but changes won't get applied until you reboot the associated Clusters.	examplecluster cluster
2013 February 11 16:22:33 UTC-8	Cluster deleted	examplecluster2 cluster
2013 February 11 16:20:21 UTC-8	Cluster deleted	examplecluster7 cluster
2013 February 11 15:22:57 UTC-8	Finished maintenance on the Cluster	examplecluster2 cluster
2013 February 11 15:14:11 UTC-8	Beginning maintenance on the Cluster. Your Cluster may not be available during maintenance	examplecluster2 cluster
2013 February 11 15:07:35 UTC-8	Finished maintenance on the Cluster	examplecluster cluster
2013 February 11 15:00:45 UTC-8	Beginning maintenance on the Cluster. Your Cluster may not be available during maintenance	examplecluster cluster

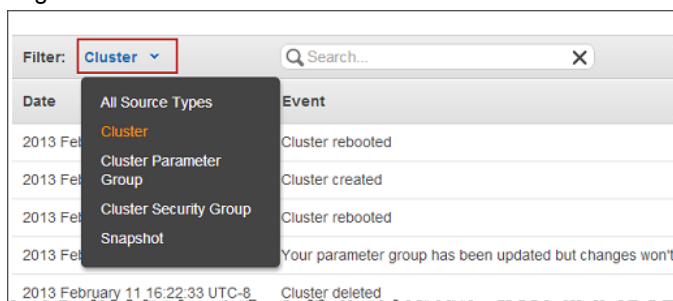
El tipo de origen de un evento indica de qué se trataba el evento. Se admiten los siguientes tipos de fuente: **Cluster** (Clúster), **Cluster Parameter Group** (Grupo de parámetros del clúster), **Grupo de seguridad de clúster**, y **Snapshot**.

Filtrado de eventos

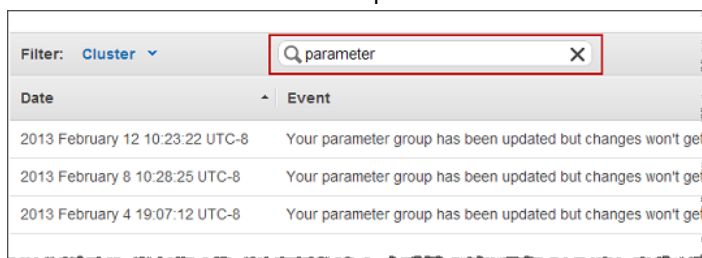
A menudo, desea encontrar una categoría específica de eventos o eventos para un clúster específico. En estos casos, puede filtrar los eventos visualizados.

Para filtrar eventos

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione **Events**.
3. Para filtrar eventos, realice una de las siguientes acciones:
 - a. Para filtrar por tipo de evento, haga clic en **Filter Cluster** (Filtrar clúster) y seleccione el tipo de origen.



- b. Para filtrar por texto en la descripción del evento, introduzca un valor en el cuadro de búsqueda. La lista decrece en función de lo que escribe.



Visualización de eventos mediante el panelAWS SDK for Java

En el siguiente ejemplo se enumeran los eventos de un clúster especificado y un tipo de origen de eventos especificado. En el ejemplo se muestra cómo utilizar la paginación.

Para obtener instrucciones paso a paso acerca de cómo ejecutar el siguiente ejemplo, consulte [Ejecución de ejemplos de Java para Amazon Redshift con Eclipse \(p. 411\)](#). Debe actualizar el código y especificar un identificador de clúster y un tipo de origen de eventos.

Example

```
/**
 * Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.
 *
 * This file is licensed under the Apache License, Version 2.0 (the "License").
 * You may not use this file except in compliance with the License. A copy of
 * the License is located at
 *
 * http://aws.amazon.com/apache2.0/
 *
 * This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
 * CONDITIONS OF ANY KIND, either express or implied. See the License for the
 * specific language governing permissions and limitations under the License.
 */

// snippet-sourcedescription:[ListEvents demonstrates how to list Amazon Redshift events.]
// snippet-service:[redshift]
// snippet-keyword:[Java]
// snippet-keyword:[Amazon Redshift]
// snippet-keyword:[Code Sample]
// snippet-keyword:[DescribeEvents]
// snippet-sourcetype:[full-example]
// snippet-sourcedate:[2019-01-31]
// snippet-sourceauthor:[AWS]
// snippet-start:[redshift.java.ListEvents.complete]

package com.amazonaws.services.redshift;

import java.util.Date;
import java.io.IOException;

import com.amazonaws.services.redshift.model.*;
```

```
public class ListEvents {

    public static AmazonRedshift client;
    public static String clusterIdentifier = "****provide cluster identifier****";
    public static String eventSourceType = "cluster"; // e.g. cluster-snapshot

    public static void main(String[] args) throws IOException {

        // Default client using the {@link
com.amazonaws.auth.DefaultAWSCredentialsProviderChain}

        client = AmazonRedshiftClientBuilder.defaultClient();

        try {
            listEvents();
        } catch (Exception e) {
            System.err.println("Operation failed: " + e.getMessage());
        }
    }

    private static void listEvents() {
        long oneWeeksAgoMilli = (new Date()).getTime() - (7L*24L*60L*60L*1000L);
        Date oneWeekAgo = new Date();
        oneWeekAgo.setTime(oneWeeksAgoMilli);
        String marker = null;

        do {
            DescribeEventsRequest request = new DescribeEventsRequest()
                .withSourceIdentifier(clusterIdentifier)
                .withSourceType(eventSourceType)
                .withStartTime(oneWeekAgo)
                .withMaxRecords(20);
            DescribeEventsResult result = client.describeEvents(request);
            marker = result.getMarker();
            for (Event event : result.getEvents()) {
                printEvent(event);
            }
        } while (marker != null);

    }

    static void printEvent(Event event)
    {
        if (event == null)
        {
            System.out.println("\nEvent object is null.");
            return;
        }

        System.out.println("\nEvent metadata:\n");
        System.out.format("SourceID: %s\n", event.getSourceIdentifier());
        System.out.format("Type: %s\n", event.getSourceType());
        System.out.format("Message: %s\n", event.getMessage());
        System.out.format("Date: %s\n", event.getDate());
    }
}

} // snippet-end:[redshift.java.ListEvents.complete]
```

Visualización de eventos mediante laAWS CLI/API de Amazon Redshift

Puede utilizar las siguientes operaciones de la ComAmazon Redshift (CLI, Interfaz de línea de comandos,

- [describe-events](#)

Amazon Redshift proporciona la siguiente API para visualizar eventos.

- [DescribeEvents](#)

Notificaciones de eventos de Amazon Redshift

Overview

Amazon Redshift Notification Service (Amazon SNS) para comunicar notificaciones sobre eventos de Amazon Redshift. Puede habilitar las notificaciones creando una suscripción a eventos de Amazon Redshift. En la suscripción de Amazon Redshift, debe especificar un conjunto de filtros para los eventos de Amazon Redshift y un tema de Amazon SNS. Siempre que se produce un evento que coincide con los criterios de filtro, Amazon Redshift publica un mensaje de notificación en el tema de Amazon SNS. A continuación, Amazon SNS transmite el mensaje a cualquier consumidor de Amazon SNS que tenga una suscripción a Amazon SNS al tema. Los mensajes enviados a los consumidores de Amazon SNS pueden ser admitidos en cualquier forma por Amazon SNS para unAWSPasos de, como un mensaje de correo electrónico, un mensaje de texto o una llamada a un punto de enlace HTTP. Por ejemplo, todas las regiones admiten notificaciones por correo electrónico, pero las notificaciones por SMS solo se pueden crear en la región EE. UU. Este (Norte de Virginia).

Al crear una suscripción a notificaciones de eventos de, debe especificar uno o varios filtros de eventos. Amazon Redshift envía notificaciones a través de la suscripción cada vez que se produce un evento que coincide con todos los criterios de filtro. Los criterios de filtro incluyen el tipo de origen (como un clúster o una snapshot), el ID de origen (como el nombre de un clúster o de una snapshot), la categoría del evento (como monitorización o seguridad) y la gravedad del evento (como INFO o ERROR).

Puede desactivar la notificación fácilmente sin eliminar una suscripción configurando laEnabled (Habilitado)botón de opción paraNoen laAWS Management Consoleo configurando la propiedadEnabledParafalsemediante la CLI o API de Amazon Redshift.

La facturación de las notificaciones de eventos de Amazon Redshift se efectúa a través de Amazon Simple Notification Service (Amazon SNS). Cuando se utiliza la notificación de eventos, se aplican las tarifas de Amazon SNS. Para obtener más información acerca de la facturación de Amazon, visite[Precios de Amazon Simple Notification Service](#).

También puede ver los eventos de Amazon Redshift que hayan ocurrido mediante la consola de administración. Para obtener más información, consulte [Eventos de Amazon Redshift \(p. 471\)](#).

Temas

- [Suscripción a notificaciones de eventos de Amazon Redshift \(p. 475\)](#)

Suscripción a notificaciones de eventos de Amazon Redshift

Puede crear una suscripción a notificaciones de eventos de Amazon Redshift para recibir notificaciones cada vez que se produzca un evento en un determinado clúster de, instantánea, grupo de seguridad o grupo de parámetros de. La forma más sencilla de crear una suscripción es con la consola de Amazon SNS. Para obtener información acerca de cómo crear un tema de Amazon SNS y suscribirse a él, consulte[Introducción a Amazon SNS](#).

Puede crear una suscripción a notificaciones de eventos de Amazon Redshift para recibir notificaciones cada vez que se produzca un evento en un determinado clúster de, instantánea, grupo de seguridad o grupo de parámetros de. La forma más sencilla de crear una suscripción es con la AWS Management

Console. Si decide crear las suscripciones de notificaciones de eventos mediante la CLI o la API de, debe crear un tema de Amazon Simple Notification Service y suscribirse a dicho tema con la consola de Amazon SNS o la API de Amazon SNS. También deberá conservar el Nombre de recurso de Amazon (ARN) del tema, ya que este se utiliza al enviar los comandos de la CLI o las acciones de la API. Para obtener información acerca de cómo crear un tema de Amazon SNS y suscribirse a él, consulte [Introducción a Amazon SNS](#).

Una suscripción a eventos de Amazon Redshift puede especificar los criterios de eventos a continuación:

- Para el tipo de origen, los valores son clúster, snapshot, grupos de parámetros y grupos de seguridad.
- El ID de origen de un recurso como `my-cluster-1` o `my-snapshot-20130823`. El ID debe ser para un recurso en la misma AWS Región como suscripción de eventos.
- Para la categoría del evento, los valores son configuración, administración, monitorización y seguridad.
- Para la gravedad del evento, los valores son INFO o ERROR.

Los criterios de evento pueden especificarse de manera independiente, con la excepción de que debe especificar un tipo de origen antes de poder especificar los ID de origen en la consola. Por ejemplo, puede especificar una categoría de evento sin tener que especificar un tipo de origen, un ID de origen o la gravedad. Si bien puede especificar el ID de origen para recursos que no son del tipo especificado en el tipo de origen, no se enviarán notificaciones para eventos desde esos recursos. Por ejemplo, si especifica un tipo de origen de un clúster y el ID de un grupo de seguridad, ninguno de los eventos suscitados por ese grupo de seguridad coincidirá con los criterios del filtro del tipo de origen, por lo que no se enviarán notificaciones para esos eventos.

Amazon Redshift envía una notificación para cualquier evento que coincide con todos los criterios especificados en una suscripción. Algunos ejemplos de los conjuntos de eventos que se devuelven son:

- La suscripción especifica un tipo de origen de un clúster, un ID de origen de `my-cluster-1`, una categoría de monitorización y una gravedad ERROR. La suscripción enviará notificaciones solo para los eventos de monitorización con una gravedad ERROR desde `my-cluster-1`.
- La suscripción especifica un tipo de origen de un clúster, una categoría de configuración y una gravedad INFO. La suscripción enviará notificaciones para los eventos de configuración con una gravedad INFO desde cualquier clúster de Amazon Redshift en la AWS Account.
- La suscripción especifica una categoría de configuración y una gravedad INFO. La suscripción enviará notificaciones para los eventos de configuración con una gravedad INFO desde cualquier recurso de Amazon Redshift en la AWS Account.
- La suscripción especifica una gravedad ERROR. La suscripción enviará notificaciones para todos los eventos con una gravedad ERROR desde cualquier recurso de Amazon Redshift en la AWS Account.

Si elimina o cambia el nombre de un objeto al que se hace referencia como ID de origen en una suscripción existente, la suscripción permanecerá activa, pero no habrá eventos para reenviar desde ese objeto. Si luego crea un objeto nuevo con el mismo nombre al que se hace referencia en la suscripción como ID de origen, la suscripción comenzará a enviar notificaciones de eventos desde ese nuevo objeto.

Amazon Redshift publica notificaciones de eventos en un tema de Amazon SNS, que se identifica por su nombre de recurso de Amazon (ARN). Cuando crea una suscripción a eventos mediante la consola de Amazon Redshift, puede especificar un tema de Amazon SNS o solicitar que la consola cree el tema cuando genere la suscripción. Todas las notificaciones de eventos de Amazon Redshift enviadas al tema de Amazon SNS se transmiten, a su vez, a todos los consumidores de Amazon que están suscritos a dicho tema. Utilice la consola de Amazon SNS para realizar cambios en el tema de Amazon SNS, como añadir suscripciones en el tema o quitarlas. Para obtener más información acerca de cómo crear temas de Amazon SNS y suscribirse a ellos, consulte [Introducción a Amazon Simple Notification Service](#).

En la siguiente sección, se enumeran todas las categorías y eventos de los que puede recibir notificaciones. Además, se proporciona información acerca de cómo suscribirse y trabajar con las suscripciones a eventos de Amazon Redshift.

Categorías y mensajes de eventos de Amazon Redshift

En esta sección, se muestran los ID de eventos y las categorías para cada tipo de origen de Amazon Redshift.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un clúster como tipo de origen.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1000	INFO	El grupo de parámetros [nombre del grupo de parámetros] se actualizó a las [hora]. Si solo cambió parámetros dinámicos, los clústeres asociados se modificarán ahora. Si cambió parámetros estáticos, todas las actualizaciones, incluidos los parámetros dinámicos, se aplicarán cuando reinicie los clústeres asociados.
Configuración	REDSHIFT-EVENT-1001	INFO	Se modificó su clúster de Amazon Redshift [nombre del clúster] para utilizar el grupo de parámetros [nombre del grupo de parámetros] a las [hora].
Configuración	REDSHIFT-EVENT-1500	ERROR	La Amazon VPC [nombre de la VPC] no existe. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1501	ERROR	Las subredes de cliente [nombre de la subred] que especificó para Amazon VPC [nombre de la VPC] no existen o no son válidos. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1502	ERROR	Subredes en un grupo de subredes de clúster [nombre de grupo de subredes] no tienen direcciones IP disponibles. No se pudo crear el clúster [nombre de clúster].
Configuración	REDSHIFT-EVENT-1503	ERROR	Amazon VPC [nombre de la VPC] no tiene una puerta de enlace a Internet asociada. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Configuración	REDSHIFT-EVENT-1504	ERROR	No se puede tener acceso al HSM para el clúster [nombre del clúster].
Configuración	REDSHIFT-EVENT-1505	ERROR	No se puede registrar el HSM para el clúster [nombre del clúster]. Pruebe con una configuración diferente.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1506	ERROR	Amazon Redshift superó el límite de interfaz de red elástica de su cuenta. Elimine hasta [cantidad máxima de interfaces de red elásticas] interfaces de red elásticas o solicite un aumento límite del número de interfaces de red porAWSRegión con EC2.
Configuración	REDSHIFT-EVENT-1509	ERROR	No se puede crear el clúster de Amazon Redshift [nombre del clúster] porque se ha alcanzado el límite de extremo de VPC de su cuenta. Elimine los endpoints de VPC no utilizados o solicite un aumento en el límite de los endpoints VPC. Para obtener más información, consulte Puntos de conexión de la VPC en la Guía del usuario de Amazon VPC.
Administración	REDSHIFT-EVENTO-2000	INFO	Se ha creado su clúster de Amazon Redshift [nombre del clúster] de y está listo para usarse.
Administración	REDSHIFT-EVENTO-2001	INFO	Se eliminó su clúster de Amazon Redshift [nombre del clúster] de a las [hora]. [Se guardó/no se guardó] una snapshot final.
Administración	REDSHIFT-EVENTO-2002	INFO	Su grupo de seguridad de VPC [nombre del grupo de seguridad] se actualizó a las [hora].
Administración	REDSHIFT-EVENTO-2003	INFO	Mantenimiento comenzado en el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Es posible que el clúster no esté disponible durante las tareas de mantenimiento.
Administración	REDSHIFT-EVENTO-2004	INFO	Mantenimiento completado en el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Administración	REDSHIFT-EVENTO-2006	INFO	Se inició un cambio de tamaño para su clúster de Amazon Redshift [nombre del clúster] a las [hora]. Su clúster estará en modo de solo lectura durante la operación de cambio de tamaño.
Administración	REDSHIFT-EVENTO-2007	INFO	Hay un cambio de tamaño en curso para su clúster de Amazon Redshift [nombre del clúster] de. Su clúster está en modo de solo lectura.
Administración	REDSHIFT-EVENTO-2008	INFO	Se inició una operación de restauración para crear una nueva snapshot [nombre de la snapshot] del clúster de Amazon Redshift [nombre del clúster] de a las [hora]. Para monitorizar el progreso de la restauración, revise la AWS Management Console.
Administración	REDSHIFT-EVENTO-2013	INFO	Se cambió el nombre de su clúster de Amazon Redshift [nombre del clúster] de a las [hora].

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENTO-2014	INFO	Se recibió una solicitud de restauración de tabla para el clúster de Amazon Redshift [nombre del clúster].
Administración	REDSHIFT-EVENTO-2015	INFO	Se canceló la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Administración	REDSHIFT-EVENTO-2016	INFO	Se inició un reemplazo de su clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Administración	REDSHIFT-EVENTO-2017	INFO	Mantenimiento iniciado por el cliente comenzado en el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Es posible que el clúster no esté disponible durante las tareas de mantenimiento.
Administración	REDSHIFT-EVENTO-2018	INFO	Mantenimiento iniciado por el cliente completado en el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Administración	REDSHIFT-EVENTO-2019	ERROR	Error del mantenimiento iniciado por el cliente en el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Devolviendo el clúster a su estado original.
Administración	REDSHIFT-EVENTO-2020	INFO	Se ha modificado la pista del clúster de Amazon Redshift [nombre del clúster] de [de pista] a [a pista].
Administración	REDSHIFT-EVENT-2021	ERROR	La [operación] del clúster [nombre del clúster] de Amazon Redshift no se realizó correctamente mientras adquiría capacidad de nuestro grupo de capacidad. Estamos trabajando para adquirir capacidad, pero por el momento hemos cancelado su solicitud. Elimine este clúster y vuelva a intentarlo más adelante.
Administración	REDSHIFT-EVENT-2022	ERROR	La [operación] del clúster [nombre del clúster] de Amazon Redshift no se realizó correctamente mientras adquiría capacidad de nuestro grupo de capacidad. Estamos trabajando para adquirir capacidad, pero por el momento hemos cancelado su solicitud. La capacidad está disponible en [zonas de disponibilidad alternativas]. Elimine este clúster y pruebe de nuevo en una zona de disponibilidad alternativa.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-2023	ERROR	Hemos detectado un error de hardware en el clúster de Amazon Redshift con un único nodo [nombre del clúster], que puede haber producido errores en las consultas o intermitencias en la disponibilidad del clúster. El clúster no se reemplazó correctamente mientras se adquiría capacidad de nuestro grupo de capacidad. Tiene que restaurar un nuevo clúster a partir de una instantánea. Elimine este clúster, seleccione la última instantánea disponible y restaure un nuevo clúster a partir de la instantánea. De este modo, dispondrá automáticamente de un hardware en buen estado.
Administración	REDSHIFT-EVENT-2024	ERROR	Hemos detectado un error de hardware en el clúster de Amazon Redshift con un único nodo [nombre del clúster], que puede haber producido errores en las consultas o intermitencias en la disponibilidad del clúster. El clúster no se reemplazó correctamente mientras se adquiría capacidad de nuestro grupo de capacidad. La capacidad está disponible en la zona de disponibilidad: [zonas de disponibilidad alternativas]. Elimine este clúster, seleccione la última instantánea disponible y restaure un nuevo clúster a partir de la instantánea. De este modo, dispondrá automáticamente de un hardware en buen estado.
Administración	REDSHIFT-EVENT-3011	INFO	El cambio de tamaño elástico para el clúster de Amazon Redshift '[nombre del clúster]' se inició a las [hora]. Durante el cambio de tamaño, se retendrán las conexiones de las bases de datos. Durante esta operación, es posible que algunas consultas y conexiones terminen o agoten el tiempo de espera.
Administración	REDSHIFT-EVENT-3012	INFO	Se recibió una solicitud de cambio de tamaño elástico para el clúster '[nombre del clúster]' iniciado a las [hora]. Le proporcionaremos una notificación de evento cuando comience el cambio de tamaño.
Pendiente	REDSHIFT-EVENT-2025	INFO	La base de datos para el clúster <nombre de clúster> se actualizará entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Pendiente	REDSHIFT-EVENT-2026	INFO	El clúster <nombre de clúster> se actualizará entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.
Monitorización	REDSHIFT-EVENT-2050	INFO	Se detectó un problema de hardware en el clúster [nombre del clúster] de Amazon Redshift. Se inició una solicitud de reemplazo a las [hora].
Monitorización	REDSHIFT-EVENT-3000	INFO	Se reinició su clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Monitorización	REDSHIFT-EVENT-3001	INFO	Se reemplazó automáticamente un nodo de su clúster de Amazon Redshift [nombre del clúster] de a las [hora] y el clúster está funcionando con normalidad.
Monitorización	REDSHIFT-EVENT-3002	INFO	Se completó el cambio de tamaño de su clúster de Amazon Redshift [nombre del clúster] de y su clúster está disponible para lecturas y escrituras. El cambio de tamaño se inició a las [hora] y tardó [horas] horas en completarse.
Monitorización	REDSHIFT-EVENT-3003	INFO	Se creó correctamente un clúster de Amazon Redshift [nombre del clúster] de a partir de la snapshot [nombre de la snapshot] y está disponible para usarse.
Monitorización	REDSHIFT-EVENT-3007	INFO	Se copió correctamente su snapshot [nombre de la snapshot] de Amazon Redshift [origen de laAWSRegión] a [destinoAWSRegión] en [hora].
Monitorización	REDSHIFT-EVENT-3008	INFO	Comenzó la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Monitorización	REDSHIFT-EVENT-3009	INFO	Se completó correctamente la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Monitorización	REDSHIFT-EVENT-3010	ERROR	Se produjo un error en la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Monitorización	REDSHIFT-EVENT-3013	ERROR	Se produjo un error en la operación de modificación de tamaño elástica solicitada para el clúster de Amazon Redshift [nombre del clúster] a las [hora] debido a [motivo].
Monitorización	REDSHIFT-EVENT-3014	INFO	Amazon Redshift reinició el clúster [nombre del clúster] a las [hora].

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Monitorización	REDSHIFT-EVENT-3500	ERROR	Se produjo un error en el cambio de tamaño en curso para su clúster [nombre del clúster] de Amazon Redshift. El cambio de tamaño se volverá a ejecutar automáticamente en unos minutos.
Monitorización	REDSHIFT-EVENT-3501	ERROR	Se produjo un error en la operación de restauración para crear un clúster de Amazon Redshift [nombre del clúster] de desde una snapshot [nombre de la snapshot] a las [hora]. Vuelva a realizar la operación.
Monitorización	REDSHIFT-EVENT-3504	ERROR	El bucket de Amazon S3 [nombre del bucket] de no es válido para el registro del clúster [nombre del clúster] de.
Monitorización	REDSHIFT-EVENT-3505	ERROR	El bucket de Amazon S3 [nombre del bucket] no tiene las políticas de IAM correctas para el clúster [nombre del clúster].
Monitorización	REDSHIFT-EVENT-3506	ERROR	El bucket de Amazon S3 [nombre del bucket] no existe. No se puede continuar con el registro del clúster [nombre del clúster].
Monitorización	REDSHIFT-EVENT-3507	ERROR	No se puede crear el clúster de Amazon Redshift [nombre del clúster] de utilizando la EIP [dirección IP]. Esta EIP ya está en uso.
Monitorización	REDSHIFT-EVENT-3508	ERROR	No se puede crear el clúster de Amazon Redshift [nombre del clúster] de utilizando la EIP [dirección IP]. No se ha encontrado la EIP.
Monitorización	REDSHIFT-EVENT-3509	ERROR	La copia de snapshot no está habilitada entre regiones para el clúster [nombre del clúster].
Monitorización	REDSHIFT-EVENT-3510	ERROR	Se produjo un error en el inicio de la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] a las [hora]. Motivo: [motivo].
Monitorización	REDSHIFT-EVENT-3511	ERROR	Se produjo un error en la restauración de tabla para el clúster de Amazon Redshift [nombre del clúster] a las [hora].
Monitorización	REDSHIFT-EVENT-3512	ERROR	Se produjo un error en el clúster de Amazon Redshift [nombre del clúster] de debido a un problema de hardware. El clúster se está restaurando automáticamente desde la última snapshot [nombre de la snapshot] creada a las [hora].

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Monitorización	REDSHIFT-EVENT-3513	ERROR	Se produjo un error en el clúster de Amazon Redshift [nombre del clúster] de debido a un problema de hardware. El clúster se está restaurando automáticamente desde la última snapshot [nombre de la snapshot] creada a las [hora]. Se deberá volver e enviar cualquier cambio en la base de datos que se haya realizado después de esta hora.
Monitorización	REDSHIFT-EVENT-3514	ERROR	Se produjo un error en el clúster de Amazon Redshift [nombre del clúster] de debido a un problema de hardware. El clúster se pondrá en estado de error de hardware. Elimine y restaure el clúster desde la última snapshot [nombre de la snapshot] creada a las [hora].
Monitorización	REDSHIFT-EVENT-3515	ERROR	Se produjo un error en el clúster de Amazon Redshift [nombre del clúster] de debido a un problema de hardware. El clúster se pondrá en estado de error de hardware. Elimine y restaure el clúster desde la última snapshot [nombre de la snapshot] creada a las [hora]. Se deberá volver e enviar cualquier cambio en la base de datos que se haya realizado después de esta hora.
Monitorización	REDSHIFT-EVENT-3516	ERROR	Se produjo un error en el clúster de Amazon Redshift [nombre del clúster] de debido a un problema de hardware y no hay copias de seguridad del clúster. El clúster se pondrá en estado de error de hardware y se puede eliminar.
Monitorización	REDSHIFT-EVENT-3519	INFO	El clúster comenzó a reiniciarse [nombre del clúster] a las [hora].
Monitorización	REDSHIFT-EVENT-3520	INFO	Se terminó de reiniciar el clúster [nombre del clúster] a las [hora].
Monitorización	REDSHIFT-EVENT-3521	INFO	Detectamos un problema de conectividad en el clúster '[nombre del clúster]'. Se inició un control diagnóstico automatizado a las [hora].
Monitorización	REDSHIFT-EVENT-3522	INFO	Se produjo un error en la acción de recuperación del clúster '[nombre del clúster]' a las [hora]. El equipo de Amazon Redshift está buscando una solución.
Monitorización	REDSHIFT-EVENT-3533	ERROR	Se canceló el cambio de tamaño del clúster '[nombre del clúster]' a las [hora]. La operación se canceló porque [motivo]. [acción necesaria].

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Monitorización	REDSHIFT-EVENT-3534	INFO	El cambio de tamaño elástico para el clúster de Amazon Redshift '[nombre del clúster]' se completó a las [hora]. El clúster está ahora disponible para operaciones de lectura y escritura mientras se realiza la transferencia de datos. Es posible que algunas consultas tarden más tiempo hasta que se complete la transferencia de datos.
Monitorización	REDSHIFT-EVENT-3537	INFO	Se completó la transferencia de datos de un clúster '[nombre del clúster]' de a las [hora en UTC].
Monitorización	REDSHIFT-EVENT-3600	INFO	La operación de cambio de tamaño solicitada para el clúster '[nombre del clúster]' de Amazon Redshift se canceló anteriormente. La reversión se completó a las [hora].
Pendiente	REDSHIFT-EVENT-3601	INFO	Un nodo del clúster <nombre de clúster> se sustituirá entre las <hora de inicio> y las <hora de finalización>. No puede posponer este mantenimiento. Planifíquelo en consecuencia.
Pendiente	REDSHIFT-EVENT-3602	INFO	La sustitución de un nodo del clúster <nombre de clúster> está programada entre las <hora de inicio> y las <hora de finalización>. No será posible obtener acceso al clúster. Planifíquelo en consecuencia.
Administración	REDSHIFT-EVENT-3603	INFO	La operación de restauración para crear el clúster [nombre del clúster] a partir de la instantánea [nombre de la instantánea] produjo un error interno. El clúster se pondrá en estado de restauración incompatible y se puede eliminar. Intente restaurar la instantánea en un clúster con otra configuración.
Administración	REDSHIFT-EVENT-3614	INFO	La acción programada [nombre de acción programada] se creó a las [hora en UTC]. La primera invocación está programada a las [hora en UTC].
Administración	REDSHIFT-EVENT-3615	INFO	La acción programada [nombre de acción programada] está programada a las [hora en UTC].
Monitorización	REDSHIFT-EVENT-3616	INFO	La acción programada [nombre de la acción programada] a las [hora en UTC] finalizó con el estado "SUCCEEDED".
Monitorización	REDSHIFT-EVENT-3617	ERROR	La acción programada [nombre de acción programada] se omitió a las [hora en UTC] debido a un retraso.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENT-3626	INFO	La acción programada [nombre de acción programada] se modificó a las [hora en UTC]. La primera invocación está programada a las [hora en UTC].
Administración	REDSHIFT-EVENT-3627	INFO	La acción programada [nombre de acción programada] se eliminó a las [hora en UTC].
Monitorización	REDSHIFT-EVENT-3628	ERROR	La acción programada [nombre de acción programada] a las [hora en UTC] finalizó con el estado "FAILED".
Administración	REDSHIFT-EVENT-3629	INFO	Se recibió su solicitud de reubicación de Amazon Redshift [nombre del clúster] de. Cuando se completa la reubicación de la zona de disponibilidad, Amazon Redshift envía una notificación de eventos.
Administración	REDSHIFT-EVENT-3630	INFO	Se trasladó correctamente un clúster de Amazon Redshift [nombre del clúster] de [zona de disponibilidad] a [zona de disponibilidad]. Puede usar el clúster ahora.
Administración	REDSHIFT-EVENT-3631	INFO	Amazon Redshift trasladó correctamente su clúster de Amazon Redshift [nombre del clúster] de [zona de disponibilidad] a [zona de disponibilidad] para recuperarse.
Administración	REDSHIFT-EVENT-3632	INFO	Amazon Redshift ha deshabilitado temporalmente la reubicación del clúster para su clúster de Amazon Redshift [nombre del clúster] de debido a cambios de configuración. Vuelva a intentarlo más tarde.
Seguridad	REDSHIFT-EVENT-4000	INFO	Se actualizaron sus credenciales maestras para su clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Seguridad	REDSHIFT-EVENT-4001	INFO	Se modificó el grupo de seguridad [nombre del grupo de seguridad] a las [hora]. Los cambios en todos los clústeres asociados se efectuarán de manera automática.
Seguridad	REDSHIFT-EVENT-4500	ERROR	El grupo de seguridad [nombre del grupo de seguridad] que proporcionó no es válido. No se aplicaron los cambios de configuración para el clúster [nombre del clúster]. Revise la AWS Management Console para corregir el problema.
Seguridad	REDSHIFT-EVENT-4501	ERROR	No se pudo encontrar el grupo de seguridad [nombre del grupo de seguridad] especificado en el grupo de seguridad de clúster [nombre del grupo de seguridad de clúster]. No se pudo completar la autorización.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4502	ERROR	Se produjo un error en la actualización de las credenciales maestras para el clúster de Amazon Redshift [nombre del clúster] de a las [hora] debido a la actividad simultánea. Permita que la carga de trabajo actual complete o reduzca la carga de trabajo activa y, a continuación, vuelva a intentar la operación.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un grupo de parámetros como tipo de origen.

Categorías y eventos de un grupo de parámetros como tipo de origen

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Configuración	REDSHIFT-EVENT-1002	INFO	El grupo de parámetros [nombre del grupo de parámetros] pasó del valor [valor] al [valor] a las [hora].
Configuración	REDSHIFT-EVENT-1003	INFO	Se creó el grupo [nombre del grupo] de parámetros del clúster.
Configuración	REDSHIFT-EVENT-1004	INFO	Se eliminó el grupo [nombre del grupo] de parámetros del clúster.
Configuración	REDSHIFT-EVENT-1005	INFO	Se actualizó el grupo [nombre] de parámetros del clúster a las [hora]. Si solo cambió parámetros dinámicos, los clústeres asociados se modificarán ahora. Si cambió parámetros estáticos, todas las actualizaciones, incluidos los parámetros dinámicos, se aplicarán cuando reinicie los clústeres asociados.

En la siguiente tabla, se muestra la categoría de eventos y una lista de eventos correspondiente a un grupo de seguridad como tipo de origen.

Categorías y eventos de un grupo de seguridad como tipo de origen

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4002	INFO	Se creó el grupo de seguridad [nombre del grupo] del clúster.
Seguridad	REDSHIFT-EVENT-4003	INFO	Se eliminó el grupo de seguridad [nombre del grupo] del clúster.

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Seguridad	REDSHIFT-EVENT-4004	INFO	Se cambió el grupo de seguridad [nombre del grupo] del clúster. Los cambios se aplicarán automáticamente a todos los clústeres asociados.

En la siguiente tabla, se muestra la categoría de eventos y una lista de los eventos correspondiente a una snapshot como tipo de origen.

Categorías y eventos de una instantánea como tipo de origen

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
Administración	REDSHIFT-EVENTO-2009	INFO	Se inició una snapshot de usuario [nombre de la snapshot] para el clúster de Amazon Redshift [nombre del clúster] de a las [hora]. Para monitorizar el progreso de la snapshot, revise la AWS Management Console.
Administración	REDSHIFT-EVENTO-2010	INFO	Se canceló la snapshot de usuario [nombre de la snapshot] para su clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Administración	REDSHIFT-EVENTO-2011	INFO	Se eliminó la snapshot de usuario [nombre de la snapshot] para el clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Administración	REDSHIFT-EVENTO-2012	INFO	Se inició la snapshot final [nombre de la snapshot] para el clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Monitorización	REDSHIFT-EVENT-3004	INFO	Se completó correctamente la snapshot de usuario [nombre de la snapshot] para su clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Monitorización	REDSHIFT-EVENT-3005	INFO	Se completó correctamente la snapshot final [nombre] para el clúster de Amazon Redshift [nombre] a las [hora].
Monitorización	REDSHIFT-EVENT-3006	INFO	Se canceló la snapshot final [nombre de la snapshot] para el clúster de Amazon Redshift [nombre del clúster] de a las [hora].
Monitorización	REDSHIFT-EVENT-3502	ERROR	Se produjo un error en la snapshot final [nombre de la snapshot] para el clúster de Amazon Redshift [nombre del clúster] de a las [hora]. El equipo está investigando el problema. Revise la AWS Management Console para volver a ejecutar la operación.
Monitorización	REDSHIFT-EVENT-3503	ERROR	Se produjo un error en la snapshot de usuario [nombre de la snapshot] para su clúster de

Categoría de Amazon Redshift	ID de evento	Gravedad del evento	Descripción
			Amazon Redshift [nombre del clúster] de a las [hora]. El equipo está investigando el problema. Revise la AWS Management Console para volver a ejecutar la operación.

Administración de notificaciones de eventos mediante la consola de Amazon Redshift

Temas

- [Creación de una suscripción a la notificación de eventos \(p. 488\)](#)

Puede crear una suscripción a notificaciones de eventos de Amazon Simple Notification Service (Amazon SNS) para enviar notificaciones cada vez que se produzca un evento en un determinado clúster de Amazon Redshift, una snapshot, un grupo de seguridad o un grupo de parámetros de. Estas notificaciones se envían a un tema de SNS, que a su vez, transmite mensajes a todos los consumidores de SNS que están suscritos al tema. Los mensajes de SNS que reciben los consumidores pueden estar en cualquier formato de notificación compatible con Amazon SNS para unaAWSPasos de, como un mensaje de correo electrónico, un mensaje de texto o una llamada a un punto de enlace HTTP. Por ejemplo, todas las regiones admiten notificaciones por correo electrónico, pero las notificaciones por SMS solo se pueden crear en la región EE. UU. Este (Norte de Virginia). Para obtener más información, consulte [Notificaciones de eventos de Amazon Redshift \(p. 475\)](#).

En esta sección, se describe cómo administrar las suscripciones de notificaciones de eventos de Amazon Redshift desde laAWS Management Console.

Creación de una suscripción a la notificación de eventos

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para crear una suscripción de evento

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el menú de navegación, haga clic en EVENTS (EVENTOS).
3. Elija la pestaña Event Subscriptions (Suscripciones de eventos) y, a continuación, elija Create event subscriptions (Crear suscripciones de eventos).
4. Introduzca las propiedades de su suscripción de evento, como nombre, tipo de fuente, categoría y gravedad. También puede habilitar temas de Amazon SNS para recibir notificaciones de eventos.
5. Haga clic en Create event subscriptions (Crear suscripciones de eventos) para crear su suscripción.

Consola original

Para crear una suscripción de notificación de eventos de Amazon Redshift.

1. Inicie sesión en la AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Events (Eventos) y haga clic en la pestaña Subscriptions (Suscripciones).
3. En la página Subscriptions (Suscripciones) seleccione Create Event Subscription (Crear suscripción de eventos).
4. En el cuadro de diálogo Create Event Subscription (Crear suscripción de eventos), haga lo siguiente:
 - a. Utilice el panel Subscription Settings (Configuración de suscripción) para especificar los criterios de filtro de los eventos. A medida que elija los criterios, elEvents suscritosMuestra los eventos de Amazon Redshift que coincidan con los criterios. Haga lo siguiente:
 - i. En Categories (Categorías), seleccione una o varias categorías de eventos. Para especificar todas las categorías, seleccione Category (Categoría). Para seleccionar un subconjunto de categorías, haga clic en los botones de las categorías que desea incluir.
 - ii. En Severity (Gravedad), seleccione la gravedad del evento. Si selecciona Any (Cualquiera), se publicarán los eventos con la gravedad INFO o ERROR. Si selecciona Error, solo se publican los eventos con la gravedad ERROR.
 - iii. En Source Type elija un tipo de origen. La suscripción de eventos solamente publica los eventos generados por los recursos de ese tipo, como clústeres o grupos de parámetros de clústeres.
 - iv. En Resources (Recursos), especifique si deben publicarse los eventos de todos los recursos que tienen el tipo de origen especificado o solo un subconjunto de ellos. Seleccione Any (Cualquiera) para publicar eventos de todos los recursos del tipo especificado. Seleccione Choose Specific (Elegir específicos) si desea seleccionar recursos específicos.

Note

El nombre del cuadro Resource (Recurso) cambia para coincidir con el valor especificado en Source Type (Tipo de origen). Por ejemplo, si selecciona Cluster (Clúster) en Source Type (Tipo de origen), el nombre del cuadro Resources (Recursos) cambiará a Clusters (Clústeres).

Si selecciona Choose Specific (Elegir específicos), puede especificar los ID de los recursos específicos cuyos eventos se publicarán en la suscripción de eventos. Debe especificar los recursos de a uno por vez y añadirlos a la suscripción de eventos. Solo puede especificar recursos que estén en la misma AWS Región como suscripción de eventos. Los eventos que especifique aparecen bajo el cuadro Specify IDs (Especificar identificadores).

- A. Para especificar un recurso existente, busque el recurso en el cuadro Specify IDs (Especificar identificadores) y haga clic en el botón + de la columna Add (Agregar).
 - B. Para especificar el ID de un recurso antes de crearlo, escriba el ID en el cuadro situado bajo Specify IDs (Especificar identificadores) y haga clic en el botón Add (Agregar). Puede hacer esto para añadir recursos que prevé crear más adelante.
 - C. Para quitar un recurso de una suscripción de eventos, haga clic en el cuadro X que se encuentra a la derecha del recurso.
- b. En la parte inferior del panel, en el cuadro de texto Name (Nombre), escriba un nombre para la suscripción de notificaciones de eventos.
 - c. Elija Yes (Sí) para activar la suscripción. Si desea crear la suscripción, pero que todavía no envíen notificaciones, seleccione No. Se enviará un mensaje de confirmación cuando se haya creado la suscripción, independientemente de esta configuración.
 - d. Seleccionar Siguiente Para seguir especificando el tema de Amazon SNS.

Create Event Subscription

Subscription Settings
Choose your settings for this event subscription below.

Categories:

Category
☐ management
☒ monitoring
☐ security
☐ configuration

Severity: **Error**

Source Type: **Cluster**

Clusters: **Choose Specific**

Specify IDs:

ID	Add
albttestcluster1	+
examplecluster	+
	Add

Subscribed Events
The subscription settings you have selected will cause you to receive notifications for the following events:

Event	Level	Categories
Cluster: <cluster name> resize failed at <time in UTC>. Operation will retry automatically within a few minutes.	ERROR	monitoring
Restore Cluster: <cluster name> from snapshot: <snapshot name> failed at <time in UTC>. Please retry from the console.	ERROR	monitoring

Name: Name of the Subscription.

- e. Utilice una de las tres pestañas para especificar el tema de Amazon SNS que la suscripción va a utilizar para publicar eventos.
 - i. Para seleccionar un tema de Amazon SNS existente en una lista, seleccione la **Use Existing Topic** (Usar tema existente) y seleccione el tema de la lista.
 - ii. Para especificar un tema de Amazon SNS existente por su nombre de recurso de Amazon (ARN), seleccione la **Proporcione ARN del tema** y especifique el ARN en el cuadro **ARN:**. Puede encontrar el ARN de un tema de Amazon SNS en la consola de Amazon SNS:
 - A. Inicie sesión en la **AWS Management Console** y abra la consola de Amazon SNS en <https://console.aws.amazon.com/sns/v3/home>.
 - B. En el panel de navegación expanda **Topics** (Temas).
 - C. Seleccione el tema que desea incluir en la suscripción de eventos de Amazon Redshift.
 - D. En el panel **Topic Details** (Detalles del tema), copie el valor del campo **Topic ARN:** (ARN del tema).
 - iii. Para que la operación de creación de una suscripción cree también un nuevo tema de Amazon SNS, seleccione la **Crear nuevo tema** y realice una de las siguientes opciones:
 - A. En **Name** (Nombre), escriba el nombre del tema.
 - B. En cada destinatario de las notificaciones, seleccione el método de notificación en **Send** (Enviar), indique una dirección válida en **to** (para) y haga clic en **Add Recipient** (Añadir destinatario). Solo puede crear **SMSEntradas** en la región **EE.UU.** Este (Norte de Virginia).
 - C. Para quitar un destinatario, haga clic en la **X** roja de la columna **Remove** (Eliminar).

Create Event Subscription

Name:* Provide a name for the SNS topic that will be created.

Specify Recipients:* Send to e.g. user@domain.com

Type	Recipient	Remove
email	myemail@mycompany.com	<input checked="" type="button" value="X"/>
sms	phonenumber	<input checked="" type="button" value="X"/>

*Required

5. Para crear la suscripción, haga clic en Create (Crear). Para eliminar la definición sin crear una suscripción, haga clic en Cancel (Cancelar). Para regresar a la configuración de la suscripción, haga clic en Previous (Anterior).

(Consola original) Gestión de suscripciones a eventos

Publicación de suscripciones de notificación de eventos de Amazon Redshift.

Puede hacer un listado de sus suscripciones actuales de notificación de eventos de Amazon Redshift.

Para hacer un listado de sus suscripciones actuales de notificación de eventos de Amazon Redshift.

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Events. En la pestaña Subscriptions (Suscripciones), se muestran todas las suscripciones de notificación de eventos.

Modificar una suscripción de notificación de eventos de Amazon Redshift.

Después de crear una suscripción, puede cambiar el nombre de la suscripción, el identificador del origen, las categorías o el ARN del tema.

Para modificar una suscripción de notificación de eventos de Amazon Redshift.

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Events (Eventos) y haga clic en la pestaña Subscriptions (Suscripciones).
3. En el panel Subscriptions (Suscripciones), elija la suscripción que desea modificar y haga clic en Modify (Modificar).
4. En el cuadro de diálogo Modify Event Subscription (Modificar suscripción de eventos), haga lo siguiente:
 - a. Utilice el panel Subscription Settings (Configuración de suscripción) para cambiar los criterios de filtro de eventos. A medida que elija los criterios, elEvents suscritosSe muestran los eventos de Amazon Redshift que coinciden con los criterios de. Haga lo siguiente:

- i. En Categories (Categorías), seleccione una o varias categorías de eventos. Para especificar todas las categorías, seleccione Category (Categoría). Para seleccionar un subconjunto de categorías, haga clic en los botones de las categorías que desea incluir.
 - ii. En Severity (Gravedad), seleccione la gravedad del evento.
 - iii. En Source Type elija un tipo de origen.
 - iv. En Resources (Recursos), seleccione los identificadores de los recursos del tipo de origen especificado. La suscripción solo publicará los eventos generados por los recursos especificados.
- b. Para habilitar la suscripción, en Enabled (Habilitado) seleccione Yes (Sí). Seleccione No para deshabilitar la suscripción.
- c. Seleccione **Siguiente** para seguir modificando el tema de Amazon SNS.
- d. Utilice una de las tres pestañas para cambiar el tema de Amazon SNS de que utilizará la suscripción para publicar eventos.
 - i. Para seleccionar un tema de Amazon SNS existente en una lista, seleccione la opción **Use Existing Topic** (Usar tema existente) y seleccione el tema de la lista.
 - ii. Para especificar un tema de Amazon SNS existente por su nombre de recurso de Amazon (ARN), seleccione la **Proporcionar ARN** y especifique el ARN en el cuadro **ARN**.
 - iii. Para que la operación de modificación de una suscripción cree también un nuevo tema de Amazon SNS, seleccione la **Crear nuevo tema** y realice una de las siguientes opciones:
 - A. En Name (Nombre), escriba un nombre para el tema.
 - B. En cada destinatario de las notificaciones, seleccione el método de notificación en **Send** (Enviar), indique una dirección válida en **to** (para) y haga clic en **Add Recipient** (Añadir destinatario). Solo puede crear **SMS Entradas** en la región EE.UU. Este (Norte de Virginia).
 - C. Para quitar un destinatario, haga clic en la X roja de la columna **Remove** (Eliminar).
5. Seleccione **Modify** (Modificar) para guardar los cambios. Para eliminar los cambios sin modificar la suscripción, haga clic en **Cancel** (Cancelar). Para regresar a la configuración de la suscripción, haga clic en **Previous** (Anterior).

Pasos para añadir un identificador de origen a una suscripción a notificaciones de eventos de Amazon Redshift.

Puede añadir un identificador de origen (el origen de Amazon Redshift que genera el evento) a una suscripción existente.

Pasos para añadir un identificador de origen a una suscripción a notificaciones de eventos de Amazon Redshift.

1. Puede añadir o quitar fácilmente identificadores de origen mediante la consola de Amazon Redshift si los selecciona o anula la selección cuando modifica una suscripción. Para obtener más información, consulte [Modificar una suscripción de notificación de eventos de Amazon Redshift](#). (p. 491).
2. Seleccione **Modify** (Modificar) para guardar los cambios. Para eliminar los cambios sin modificar la suscripción, haga clic en **Cancel** (Cancelar). Para regresar a la configuración de la suscripción, haga clic en **Previous** (Anterior).

Pasos para quitar un identificador de origen de una suscripción a notificaciones de eventos de Amazon Redshift.

Puede quitar un identificador de origen (el origen de Amazon Redshift que genera el evento) de una suscripción si ya no desea recibir notificaciones de los eventos de ese origen.

Pasos para quitar un identificador de origen de una suscripción a notificaciones de eventos de Amazon Redshift.

- Puede añadir o quitar fácilmente identificadores de origen mediante la consola de Amazon Redshift si los selecciona o anula la selección cuando modifica una suscripción. Para obtener más información, consulte [Modificar una suscripción de notificación de eventos de Amazon Redshift](#). (p. 491).

[Elimina una suscripción de notificación de eventos de Amazon Redshift.](#)

Puede eliminar una suscripción cuando ya no la necesite. Los suscriptores del tema dejarán de recibir notificaciones de los eventos especificados en la suscripción.

Para eliminar una suscripción de notificación de eventos de Amazon Redshift.

1. Inicie sesión en laAWS Management Consoley abra la consola de Amazon Redshift en<https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione Events (Eventos) y haga clic en la pestaña Subscriptions (Suscripciones).
3. En el panel Subscriptions (Suscripciones), seleccione la suscripción que desee eliminar.
4. Elija Eliminar.

Administración de notificaciones de eventos mediante laAWS CLly la API de Amazon Redshift

Puede utilizar las siguientes operaciones de la CLI de Amazon Redshift para administrar las notificaciones de eventos.

- [create-event-subscription](#)
- [delete-event-subscription](#)
- [describe-event-categories](#)
- [describe-event-subscriptions](#)
- [describe-events](#)
- [modify-event-subscription](#)

Puede utilizar las siguientes acciones de la API de Amazon Redshift para administrar las notificaciones de eventos.

- [CreateEventSubscription](#)
- [DeleteEventSubscription](#)
- [DescribeEventCategories](#)
- [DescribeEventSubscriptions](#)
- [DescribeEvents](#)
- [ModifyEventSubscription](#)

Para obtener más información acerca de las notificaciones de eventos de Amazon Redshift, consulte[Notificaciones de eventos de Amazon Redshift](#) (p. 475).

Cuotas y límites de Amazon Redshift

Cuotas de Amazon Redshift

Amazon Redshift tiene cuotas que limitan el uso de varios recursos en su AWS Region. Existe un valor predeterminado para cada cuota, y algunas cuotas se pueden ajustar. Para cuotas ajustables, puede solicitar un aumento de AWS en una cuenta AWS Region enviando un [Formulario de aumento de límite de Amazon Redshift](#).

Nombre de la cuota	AWS valor predeterminado	Ajustable	Descripción
AWS Cuentas que puede autorizar para restaurar una instantánea por instantánea	20	No	Número máximo de AWS Cuentas que puede autorizar para restaurar una instantánea por instantánea.
AWS Cuentas que puede autorizar para restaurar una instantánea por instantánea AWS KMS clave	100	No	Número máximo de AWS Cuentas que puede autorizar para restaurar una instantánea, por AWS KMS La clave de. Es decir, si tiene 10 instantáneas que están cifradas con una sola clave de KMS, puede autorizar a 10 AWS Cuentas de restauración instantánea u otras combinaciones que sumen hasta 100 cuentas y no excedan las 20 cuentas por cada instantánea.
Roles de IAM de clúster que permiten a Amazon Redshift acceder a otros AWS services	10	No	Número máximo de roles de IAM que puede asociar a un clúster para permitir que Amazon Redshift pueda acceder a otros AWS para el usuario que posee los roles de clúster e IAM.
Nivel de simultaneidad (slots de consulta) de todas las colas de WLM manuales definidas por el usuario	50	No	Máximo número de slots de consulta en todas las colas definidas por el usuario a través de la administración manual de cargas de trabajo.

Nombre de la cuota	AWSvalor predeterminado	Ajustable	Descripción
Clústeres de escalado de simultaneidad	10	Sí	Número máximo de clústeres de escalado de simultaneidad.
Nodos DC2 de un clúster	128	Sí	Número máximo de nodos DC2 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clusters y nodos en Amazon Redshift (p. 5).
Nodos DS2 de un clúster	128	Sí	Número máximo de nodos DS2 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clusters y nodos en Amazon Redshift (p. 5).
Suscripciones de eventos	20	Sí	Número máximo de suscripciones de eventos de esta cuenta en laAWSRegión .
Nodos	200	Sí	Número máximo de nodos en todas las instancias de la base de datos de esta cuenta en laAWSRegión .
Grupos de parámetros	20	No	Número máximo de grupos de parámetros de esta cuenta en laAWSRegión .
Nodos RA3 de un clúster	128	Sí	Número máximo de nodos RA3 que se pueden asignar a un clúster. Para obtener más información sobre los límites de cada tipo de nodo, consulte Clusters y nodos en Amazon Redshift (p. 5).
Endpoints VPC administrados por RedShift conectados a un clúster	30	Sí	Número máximo de puntos de enlace de la VPC administrados por Redshift que se pueden conectar a un clúster. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Trabajar con terminales de VPC gestionados por Redshift en Amazon Redshift (p. 41).
Los beneficiarios al clúster acceden a través de un endpoint VPC administrado por RedShift	5	Sí	Número máximo de beneficiarios que un propietario de clúster puede autorizar para crear un extremo VPC administrado por RedShift para un clúster. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Trabajar con terminales de VPC gestionados por Redshift en Amazon Redshift (p. 41).
Endpoints VPC administrados por RedShift por autorización	5	Sí	Número máximo de puntos de enlace de la VPC administrados por Redshift que se pueden crear por autorización. Para obtener más información acerca de los puntos de enlace de la VPC administrados por Redshift, consulte Trabajar con terminales de VPC gestionados por Redshift en Amazon Redshift (p. 41).
Nodos reservados	200	Sí	Número máximo de nodos reservados de esta cuenta en laAWSRegión .

Nombre de la cuota	AWSvalor predeterminado	Ajustable	Descripción
Esquemas de cada base de datos por clúster	9900	No	Número máximo de esquemas que se pueden crear en cada base de datos y cada clúster. No obstante, los esquemas <code>pg_temp_*</code> no se tienen cuentan para calcular esta cuota.
Grupos de seguridad	20	Sí	Número máximo de grupos de seguridad de esta cuenta en laAWSRegión .
Tamaño de fila única cuando carga se realiza mediante COPY	4	No	Tamaño máximo (en MB) de una sola fila cuando la carga se realiza mediante el comando COPY.
Instantáneas	20	Sí	Número máximo de instantáneas de usuario de esta cuenta en laAWSRegión .
Grupos de subredes	20	Sí	Número máximo de grupos de subredes de esta cuenta en laAWSRegión .
Subredes de un grupo de subredes	20	Sí	Número máximo de subredes de un grupo de subredes.
Tablas de nodos de clúster de tipo large	9900	No	Número máximo de tablas en los nodos de clúster de tipo large. Este límite incluye las tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de consultas o el mantenimiento del sistema. Las vistas no se incluyen en este límite.
Tablas de nodos de clúster de tipo xlarge	9900	No	Número máximo de tablas en los nodos de clúster de tipo xlarge. Este límite incluye las tablas temporales. Las tablas temporales incluyen las tablas temporales definidas por el usuario y las tablas temporales creadas por Amazon Redshift durante el procesamiento de consultas o el mantenimiento del sistema. Las vistas no se incluyen en este límite.
Tablas de nodos de clúster de tipo x1plus	20 000	No	Número máximo de tablas en los nodos de clúster de tipo x1plus.
Tablas de nodos de clúster de tipo 4xlarge	100 000	No	Número máximo de tablas en los nodos de clúster de tipo 4xlarge.

Nombre de la cuota	AWSvalor predeterminado	Ajustable	Descripción
Tablas de nodos de clúster de tipo 8xlarge	100 000	No	Número máximo de tablas en los nodos de clúster de tipo 8xlarge. Este límite incluye las tablas temporales. Amazon Redshift puede definir o crear las tablas temporales durante el procesamiento de consultas o el mantenimiento del sistema. Las vistas no se incluyen en este límite.
Tablas de nodos de clúster de tipo 16xlarge	100 000	No	Número máximo de tablas en los nodos de clúster de tipo 16xlarge. Este límite incluye las tablas temporales. Amazon Redshift puede definir o crear las tablas temporales durante el procesamiento de consultas o el mantenimiento del sistema. Las vistas no se incluyen en este límite.
Bases de datos de un clúster definidas por el usuario	60	No	Número máximo de bases de datos definidas por el usuario que se pueden crear en cada clúster.
Tiempo de espera para sesiones inactivas o inactivas	4 horas	No	Esta configuración se aplica al clúster. Para obtener información acerca de cómo establecer el valor de tiempo de espera de sesión inactiva para un usuario, consulte ALTER USER en la Guía para desarrolladores de bases de datos. La configuración del usuario tiene prioridad sobre la configuración del clúster.

Cuotas y límites de Amazon Redshift Spectrum

Amazon Redshift Spectrum tiene las siguientes cuotas y límites:

- Número máximo de bases de datos AWS cuando se utiliza una cuenta AWS Glue Data Catalog. Para ver este valor, consulte [AWS Glue Cuotas de servicio de](#) en la Referencia general de Amazon Web Services.
- Número máximo de tablas por cada base de datos cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte [AWS Glue Cuotas de servicio de](#) en la Referencia general de Amazon Web Services.
- Número máximo de particiones por cada tabla cuando se utiliza AWS Glue Data Catalog. Para ver este valor, consulte [AWS Glue Cuotas de servicio de](#) en la Referencia general de Amazon Web Services.
- Número máximo de particiones AWS cuando se utiliza una cuenta AWS Glue Data Catalog. Para ver este valor, consulte [AWS Glue Cuotas de servicio de](#) en la Referencia general de Amazon Web Services.
- El número máximo de columnas de tablas externas cuando se utiliza AWS Glue Data Catalog es de 1598 cuando las pseudocolumnas están habilitadas y de 1600 cuando no lo están.
- El tamaño máximo de un valor de cadena de un archivo ION o JSON cuando se utiliza AWS Glue Data Catalog es 16 KB.
- Puede añadir un máximo de 100 particiones en una única instrucción ALTER TABLE.
- Todos los datos de S3 deben estar en la misma AWS Región como clúster de Amazon Redshift.
- Las marcas temporales de ION y JSON deben usar el formato [ISO8601](#).
- No se admite la compresión externa de archivos ORC.
- Los SERDE de Text, OpenCSV y Regex no admiten delimitadores octales mayores que ``\177``

- Debe especificar un predicado en la columna de partición para evitar que se lean datos de todas las particiones.

Por ejemplo, el predicado siguiente filtrará la columna `ship_dtm`, pero no aplicará el filtro en la columna de partición `ship_yyyymm`:

```
WHERE ship_dtm > '2018-04-01'.
```

Para omitir las particiones innecesarias, tiene que añadir un predicado `WHERE ship_yyyymm = '201804'`. Este predicado limitará las operaciones de lectura a la partición `\ship_yyyymm=201804\`.

Estos límites no se aplican a un metaalmacén Apache Hive.

Restricciones en la nomenclatura:

En la siguiente tabla se describen las restricciones de la nomenclatura de Amazon Redshift.

Identificador de clúster	• Un identificador de clúster debe contener caracteres en minúscula únicamente. • Debe incluir entre 1 y 63 caracteres alfanuméricos o guiones. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos. • Debe ser único para todos los clústeres de una cuenta de AWS.
Nombre de base de datos	• El nombre de una base de datos debe contener de 1 a 64 caracteres alfanuméricos. • Debe contener letras en minúscula únicamente. • No puede ser una palabra reservada. Para ver una lista de palabras reservadas, consulte Palabras reservadas en la Guía para desarrolladores de bases de datos.
Nombre de endpoint de un endpoint VPC administrado por RedShift	• Un nombre de extremo debe contener entre 1 y 30 caracteres. • Los caracteres válidos son A-Z, 0-9 y guion (-). • El primer carácter debe ser una letra. • El nombre no puede contener dos guiones consecutivos ni terminar con guion.
Nombre de usuario maestro	• Un nombre de usuario maestro debe contener caracteres en minúscula únicamente. • Debe contener de 1 a 128 caracteres alfanuméricos. • El primer carácter debe ser una letra. • No puede ser una palabra reservada. Para ver una lista de palabras reservadas, consulte Palabras reservadas en la Guía para desarrolladores de bases de datos.
Contraseña maestra	• Una contraseña maestra debe contener entre 8 y 64 caracteres. • Debe contener una letra mayúscula como mínimo.

	• Debe contener una letra minúscula como mínimo. • Debe contener un número. • Puede usar cualquier carácter ASCII con códigos ASCII 33 —126, excepto '(comillas sencillas), "(comillas dobles), \, / o @.
Nombre del grupo de parámetros	• El nombre de un grupo de parámetros debe contener de 1 a 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • El primer carácter debe ser una letra. • No puede terminar con un guion ni contener dos guiones consecutivos.
Nombre del grupo de seguridad de clúster	• El nombre de un grupo de seguridad de clúster no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser Default. • Debe ser único para todos los grupos de seguridad creados por la cuenta de AWS.
Nombre del grupo de subred	• El nombre de un grupo de subred no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser Default. • Debe ser único para todos los grupos de seguridad creados por la cuenta de AWS.
Identificador de instantánea de clúster	• Un identificador de instantánea de clúster no debe contener más de 255 caracteres alfanuméricos o guiones. • Debe contener caracteres en minúscula únicamente. • No debe ser Default. • Debe ser único para todos los grupos de seguridad creados por la cuenta de AWS.

Etiquetado de recursos en Amazon Redshift

Temas

- [Información general del proceso de etiquetado \(p. 500\)](#)
- [Administración de etiquetas de recursos mediante la consola \(p. 501\)](#)
- [Administración de etiquetas mediante la API de Amazon Redshift \(p. 505\)](#)

Información general del proceso de etiquetado

En AWS, las etiquetas las define el usuario y se componen de pares clave-valor. Amazon Redshift permite usar etiquetas para proporcionar metadatos sobre los recursos y categorizar los informes de facturación en función de la asignación de costos. Para utilizar etiquetas para la asignación de costos, primero debe activar esas etiquetas en el servicio AWS Billing and Cost Management. Si desea obtener más información acerca de la configuración y el uso de etiquetas para la facturación, consulte [Uso de etiquetas de asignación de costos](#) y [Configuración de un informe mensual de asignación de costos](#).

Las etiquetas no son obligatorias para los recursos de Amazon Redshift, pero ayudan a proporcionar contexto. Es posible que desee etiquetar recursos con metadatos en relación con los centros de costos, nombres de proyectos y otra información relevante relacionada con el recurso. Por ejemplo, suponga que desea hacer un seguimiento de qué recursos pertenecen a un entorno de prueba y a un entorno de producción. Puede crear una clave denominada `environment` y proporcionar el valor de `test` o de `production` para identificar los recursos que se utilizan en cada entorno. Si usa el etiquetado en otros AWS, para mantener la coherencia, le recomendamos que cree los mismos pares clave-valor para los recursos de Amazon Redshift.

Después de que cambia el tamaño de un clúster y después de que restaura una snapshot de un clúster dentro de la misma región, se conservan las etiquetas para los recursos. Sin embargo, no se conservan las etiquetas si copia una snapshot a otra región, por lo que deberá volver a crear las etiquetas en la nueva región. Si elimina un recurso, se eliminarán todas las etiquetas asociadas.

Cada recurso tiene un conjunto de etiquetas, que es una colección de una o varias etiquetas asignadas al recurso. Cada recurso puede tener hasta 50 etiquetas por cada conjunto de etiquetas. Puede añadir etiquetas al crear un recurso y después de que se haya creado. Puede añadir etiquetas a los siguientes tipos de recursos en Amazon Redshift:

- CIDR/IP
- Clúster
- Grupo de seguridad de clúster
- Regla de entrada del grupo de seguridad de clúster
- Grupo de seguridad de Amazon EC2
- Conexión de un módulo de seguridad de hardware (HSM)
- Certificado de cliente del HSM
- Grupo de parámetros
- Instantánea
- Subnet group

Para utilizar el etiquetado desde la consola de Amazon Redshift, el usuario de IAM puede adjuntar la política administrada por `AWSAmazonRedshiftFullAccess`. Para obtener un ejemplo de política de IAM con permisos de etiquetado limitados que puede adjuntar a un usuario de la consola de Amazon Redshift, consulte [Ejemplo 7: Permitir a un usuario etiquetar recursos con la consola de Amazon Redshift \(p. 320\)](#). Para obtener más información acerca del etiquetado, consulte [¿Qué es ?AWSResource Groups?](#).

Requisitos de etiquetado

Las etiquetas tienen los siguientes requisitos:

- Las claves no pueden tener el prefijo `aws :`.
- Las claves deben ser únicas dentro de un conjunto de etiquetas.
- Una clave debe tener entre 1 y 128 caracteres permitidos.
- Un valor debe tener entre 0 y 256 caracteres permitidos.
- No es necesario que los valores sean únicos dentro de un conjunto de etiquetas.
- Los caracteres permitidos para las claves y los valores son letras y dígitos Unicode, espacios en blanco y cualquiera de estos símbolos: `_ . : / = + - @`.
- Las claves y los valores distinguen entre mayúsculas y minúsculas.

Administración de etiquetas de recursos mediante la consola

Note

Hay una nueva consola disponible para Amazon Redshift. Elija entre las instrucciones de New console (Nueva consola) o Original console (Consola original) en función de la consola que utilice. Las instrucciones de New console (Nueva consola) están abiertas de forma predeterminada.

New console

Para administrar etiquetas en recursos de Amazon Redshift

1. Inicie sesión en AWS Management Console y abra la consola de Amazon Redshift en <https://console.aws.amazon.com/redshift/>.
2. En el panel de navegación, seleccione CONFIGy, a continuación, seleccione Manage tags (Administrar etiquetas).
3. Introduzca sus elecciones para los recursos y seleccione qué etiquetas añadir, modificar o eliminar. A continuación seleccione Manage tags of the resources that you choose (Administrar las etiquetas de los recursos que elija).

Los recursos que puede etiquetar incluyen clústeres, grupos de parámetros, grupos de subredes, certificados de clientes HSM, conexiones HSM e instantáneas.

4. En la página Administrar etiquetas Seleccione la página de navegación, Revisar y aplicar cambios en las etiquetas Seleccione y, después, Aplicar Para guardar los cambios.

Consola original

A continuación se muestra un ejemplo de Administrar etiquetas Para un recurso de Amazon Redshift, como un clúster o un grupo de parámetros.

Manage Tags

Apply tags to your resources to help organize and identify them.
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn More](#) about tagging your resources.

Applied Tags

Key	Value	Delete
environment	test	☐
owner	admin	☐

Add Tags

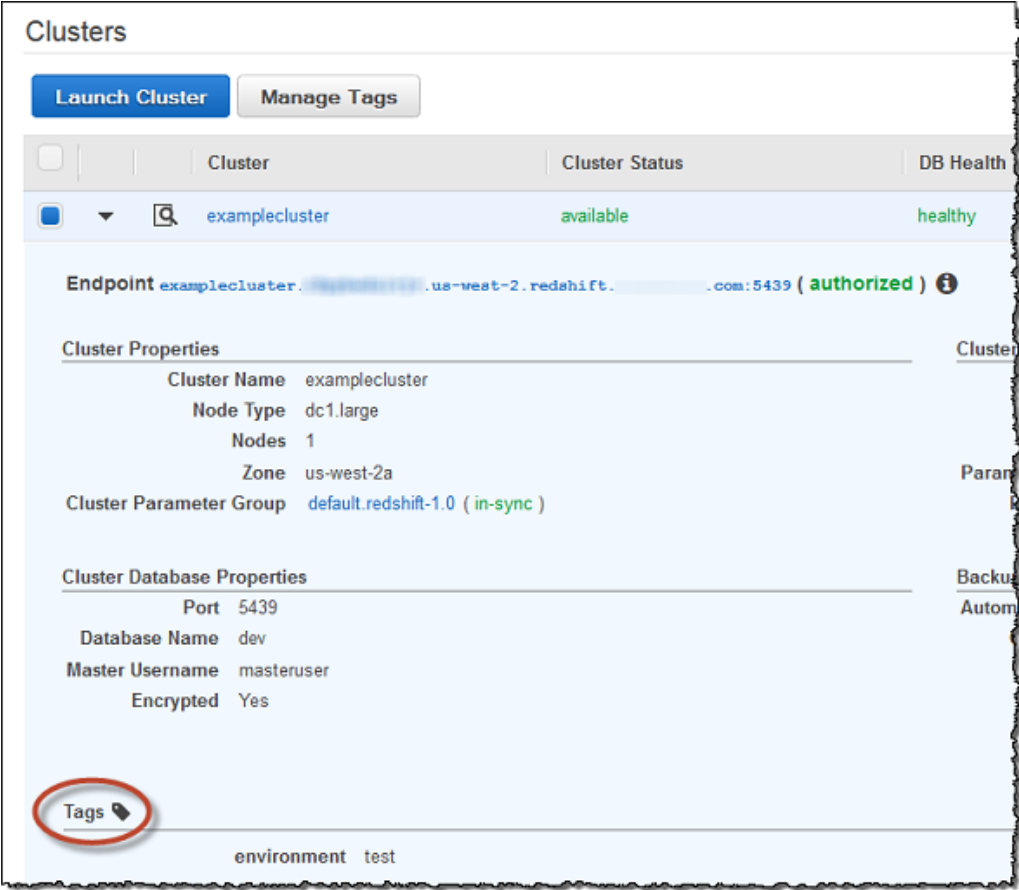
Key	Value	
version	beta	☐
Add key	Empty value	

Puede utilizar el **Añadir etiquetas** Para añadir pares de claves a un recurso de Amazon Redshift. Cuando comience a especificar un par de claves en la sección **Add Tags** (Añadir etiquetas), aparecerá una fila nueva en la que podrá añadir otro par de claves, y así sucesivamente. Para obtener más información acerca de los caracteres permitidos para las claves y los valores, consulte [Requisitos de etiquetado](#) (p. 501).

Si decide no añadir una determinada etiqueta al recurso, puede quitarla de la sección **Add Tags** (Añadir etiquetas) seleccionando la X de la fila. Una vez que haya especificado los pares de claves que desea añadir, aplique los cambios para que queden asociados con el recurso.

Una vez que se han añadido pares de claves a un recurso, estas se muestran en la sección **Applied Tags** (Etiquetas aplicadas), que corresponde al conjunto de etiquetas del recurso. Puede modificar el valor de una etiqueta, pero no puede modificar el nombre de la clave. No obstante, puede eliminar una clave si ya no la necesita para ese recurso.

Para ver las etiquetas de un recurso, consulte la sección **Applied Tags** (Etiquetas aplicadas) de la ventana **Manage Tags** (Administrar etiquetas). También puede ver rápidamente las etiquetas si navega a un tipo de recurso del panel de navegación y expande después el recurso en la lista para ver la sección **Tags** (Etiquetas). A continuación, se muestra un ejemplo de un clúster desplegado para ver diferentes propiedades, incluidas las etiquetas asociadas con el clúster.



Cómo abrir la ventana Manage Tags

En la tabla siguiente se describe cómo abrir el Administrar etiquetas. En cada uno de los recursos de Amazon Redshift que admiten etiquetas.

Recurso	Descripción
Clúster	En el panel de navegación, elija Clusters (Clústeres) y seleccione un clúster de la lista. A continuación seleccione Manage tags (Administrar etiquetas).
Instantánea	En el panel de navegación, elija Snapshots (Instantáneas) y seleccione una instantánea de la lista. A continuación, elija Manage tags (Administrar etiquetas) en Actions (Acciones).
Grupo de seguridad de clúster	En el panel de navegación, elija Security (Seguridad). En la pestaña Security Groups (Grupos de seguridad), seleccione un grupo de seguridad de la lista. A continuación seleccione Manage tags (Administrar etiquetas).
Regla de entrada del grupo de seguridad de clúster	En el panel de navegación, elija Security (Seguridad). En la pestaña Security Groups (Grupos de seguridad), seleccione un grupo de seguridad de la lista. En la página Security Group Connections (Conexiones del grupo de seguridad), elija una regla de entrada y seleccione Manage Tags (Administrar etiquetas).

Recurso	Descripción
Subnet group	En el panel de navegación, elija Security (Seguridad). En la pestaña Subnet Groups (Grupos de subredes), elija un grupo de subredes de la lista. A continuación seleccione Manage tags (Administrar etiquetas).
conexión de HSM	En el panel de navegación, elija Security (Seguridad). En la pestaña HSM Connections (Conexiones de HSM), elija una conexión de la lista. A continuación seleccione Manage tags (Administrar etiquetas).
Certificado del HSM	En el panel de navegación, elija Security (Seguridad). En la pestaña HSM Certificates (Certificados de HSM), elija un certificado de la lista. A continuación seleccione Manage tags (Administrar etiquetas).
Grupo de parámetros	En el panel de navegación, haga clic en Parameter Groups (Grupos de parámetros) y elija un grupo de parámetros de la lista. A continuación seleccione Manage tags (Administrar etiquetas).

Cómo administrar etiquetas en la consola de Amazon Redshift

Mediante la tabla de la anterior sección, navegue hasta el recurso con el que quiera trabajar. A continuación, utilice los procedimientos en esta sección para añadir, modificar, eliminar y ver las etiquetas del recurso.

Cómo añadir etiquetas a un recurso

1. Navegue al recurso en el que desea añadir etiquetas y abra la ventana Manage Tags (Administrar etiquetas).
2. En Add Tags (Añadir etiquetas), escriba un nombre de clave en el cuadro Key (Clave) y un valor de clave en el cuadro Value (Valor). Por ejemplo, escriba `environment` en el cuadro Key (Clave) y `production` en el cuadro Value (Valor). Repita este pasos para añadir cualquier etiqueta adicional.
3. Elija Apply Changes (Aplicar cambios).

Pasos para modificar las etiquetas asociadas a un recurso

1. Navegue al recurso en el que desea modificar etiquetas y abra la ventana Manage Tags (Administrar etiquetas).
2. En Applied Tags (Etiquetas aplicadas), busque la clave que desea modificar. En el cuadro Value (Valor), escriba un nuevo valor para la clave. Repita la operación en cualquier otra etiqueta que desee modificar.
3. Elija Apply Changes (Aplicar cambios).

Pasos para eliminar las etiquetas asociadas a un recurso

1. Navegue al recurso del que desea eliminar etiquetas y abra la ventana Manage Tags (Administrar etiquetas).
2. En Applied Tags (Etiquetas aplicadas), busque la clave que desea eliminar. Active la casilla Delete (Eliminar). Repita la operación en cualquier otra etiqueta que desee eliminar.
3. Elija Apply Changes (Aplicar cambios).

Administración de etiquetas mediante la API de Amazon Redshift

Puede utilizar la siguiente AWS CLI para operaciones de administración de etiquetas en Amazon Redshift.

- [create-tags](#)
- [delete-tags](#)
- [describe-tags](#)

Puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar etiquetas:

- [CreateTags](#)
- [DeleteTags](#)
- [DescribeTags](#)
- [Tag](#)
- [TaggedResource](#)

Además, puede utilizar las siguientes operaciones de la API de Amazon Redshift para administrar y ver las etiquetas de un recurso determinado:

- [CreateCluster](#)
- [CreateClusterParameterGroup](#)
- [CreateClusterSecurityGroup](#)
- [CreateClusterSnapshot](#)
- [CreateClusterSubnetGroup](#)
- [CreateHsmClientCertificate](#)
- [CreateHsmConfiguration](#)
- [DescribeClusters](#)
- [DescribeClusterParameterGroups](#)
- [DescribeClusterSecurityGroups](#)
- [DescribeClusterSnapshots](#)
- [DescribeClusterSubnetGroups](#)
- [DescribeHsmClientCertificates](#)
- [DescribeHsmConfigurations](#)

Historial de revisión

En la tabla siguiente se describen los cambios importantes de cada versión de la Guía de administración de clústeres Después de junio de 2018. Para obtener notificaciones sobre las actualizaciones de esta documentación, puede suscribirse a una fuente RSS.

Versión de API: 01/12/2012

Última actualización de la documentación: 11 de diciembre de 2020

Para ver una lista con los cambios realizados en la Guía para desarrolladores de bases de datos de Amazon Red, consulte [Historial de revisión de la base de datos de Amazon Redshift](#).

Para obtener más información acerca de las nuevas características, incluida una lista de correcciones y los números de versión del clúster asociado, consulte el [historial de versiones del clúster](#).

update-history-change	update-history-description	update-history-date
Support con la integración de la consola con socios	Puede integrarse con socios mediante la consola de Amazon Redshift.	9 de diciembre de 2020
Support bilidad con la capacidad de mover clústeres entre zonas de disponibilidad	Ahora puede mover clústeres RA3 entre zonas de disponibilidad.	9 de diciembre de 2020
Support de tipos de nodos ra3.xlplus	Ahora puede crear tipos de nodos ra3.xlplus.	9 de diciembre de 2020
Support de controlador JDBC versión 2.0	Ahora puede configurar el controlador JDBC versión 2.0.	5 de noviembre de 2020
Support para UDF de Lambda y tokenización	Ahora puede escribir UDF de Lambda para habilitar la tokenización externa de datos.	26 de octubre de 2020
Support para programar la ejecución de una sentencia SQL	Ahora puede programar una consulta en la consola de Amazon Redshift.	22 de octubre de 2020
Support con la API de datos para Amazon Redshift	Ahora puede acceder a Amazon Redshift con la API de datos integrada. Las actualizaciones de la documentación incluyen una Referencia de la API de datos de Amazon Redshift.	10 de septiembre de 2020
Support para la supervisión de consultas de la consola de Amazon Redshift	Se ha actualizado la guía para describir los nuevos gráficos de supervisión de consultas de.	7 de mayo de 2020
Compatibilidad con los límites de uso	Se ha actualizado la guía con una descripción de los límites de uso.	23 de abril de 2020
Autenticación multifactor	Se ha actualizado la guía para describir la compatibilidad de la autenticación multifactor.	20 de abril de 2020

La función de cambio de tamaño elástico ahora permite modificar el tipo de nodo	Se ha actualizado la descripción del cambio de tamaño elástico.	6 de abril de 2020
Compatibilidad de tipos de nodos ra3.4xlarge con almacenamiento administrado	Se ha actualizado la guía para incluir los tipos de nodos ra3.4xlarge.	2 de abril de 2020
Soporte para pausa y reanudación	Se ha actualizado la guía para describir las operaciones de pausa y reanudación del clúster.	11 de marzo de 2020
Compatibilidad con Microsoft Azure AD como proveedor de identidades	Se actualizó la guía para describir los pasos para usar Microsoft Azure AD como proveedor de identidades.	10 de febrero de 2020
Compatibilidad con el tipo de nodo RA3	Se ha actualizado la guía para describir el nuevo tipo de nodo RA3.	3 de diciembre de 2019
Soporte para la nueva consola	Se ha actualizado la guía para describir la nueva consola de Amazon Redshift.	11 de noviembre de 2019
Actualizaciones de la información de seguridad	Actualizaciones a la documentación de información de seguridad.	24 de junio de 2019
Mejoras de las instantáneas	Ahora Amazon Redshift admite varias mejoras para administrar y programar instantáneas.	4 de abril de 2019
Escalado de simultaneidad	Puede configurar la administración de cargas de trabajo (WLM) para habilitar el modo de escalado de simultaneidad. Para obtener más información, consulte Configuración de la carga de trabajo .	21 de marzo de 2019
Controladores JDBC y ODBC actualizados	Ahora Amazon Redshift admite nuevas versiones de los controladores JDBC y ODBC. Para obtener más información, consulte Configuración de una conexión JDBC y Configuración de una conexión ODBC .	4 de febrero de 2019

Mantenimiento pospuesto	Si necesita volver a programar el período de mantenimiento de su clúster, tiene la opción de posponer el mantenimiento hasta 14 días. Si necesitamos actualizar el hardware o realizar alguna otra actualización obligatoria durante el período de postergación, le notificaremos y realizaremos los cambios necesarios. Su clúster no está disponible durante estas actualizaciones. Para obtener más información, consulte Mantenimiento diferido.	20 de noviembre de 2018
Notificación avanzada	Amazon Redshift proporciona una notificación con antelación para algunos eventos. Estos eventos tienen una categoría de evento de <code>pending</code>. Por ejemplo, enviamos una notificación con antelación si se requiere una actualización de hardware para alguno de los nodos de su clúster. Puede suscribirse a los eventos pendientes de la misma forma que a otros eventos de Amazon Redshift. Para obtener más información, consulte Suscripción a notificaciones de eventos de Amazon Redshift.	20 de noviembre de 2018
Elastic resize (Cambio de tamaño elástico)	El cambio de tamaño elástico es el método más rápido de cambiar el tamaño de un clúster. El cambio de tamaño elástico agrega o quita nodos de un clúster existente y, a continuación, redistribuye automáticamente los datos a los nuevos nodos. Como no crea un nuevo clúster, la operación de cambio de tamaño elástico se completa rápidamente, normalmente en unos pocos minutos. Para obtener más información, consulte Cambio de tamaño de clústeres.	15 de noviembre de 2018

Nuevos controladores ODBC	Los controladores ODBC de Amazon Redshift de se han actualizado a la versión 1.4.3.1000. Para obtener más información, consulte Configuración de una conexión ODBC .	8 de noviembre de 2018
Cancelación de la operación de cambio de tamaño	Ahora puede cancelar una operación de cambio de tamaño mientras aún está en curso. Para obtener más información, consulte Información general de la operación de cambio de tamaño .	2 de noviembre de 2018
Modificación del clúster para cambiar el cifrado	Puede modificar un clúster sin cifrar para utilizar AWS Key Management Service (AWS KMS), utilizando un AWS o administrada por el cliente (CMK) o administrada por el cliente. Cuando modifica su clúster para habilitar el cifrado de KMS, Amazon Redshift migra automáticamente sus datos a un nuevo clúster cifrado. También puede migrar un clúster no cifrado a un clúster cifrado modificando el clúster.	16 de octubre de 2018
El espectro de Amazon Redshift admite Enhanced VPC Routing	Ahora puede utilizar Redshift Spectrum con Enhanced VPC Routing habilitado para su clúster. Es posible que deba realizar algún paso de configuración adicional. Para obtener más información, consulte Uso de Amazon Redshift Spectrum con Enhanced VPC Routing .	10 de octubre de 2018
Editor de consultas	Ahora puede ejecutar consultas SQL desde la consola de administración de Amazon Redshift.	4 de octubre de 2018
Gráfico de desglose de ejecuciones de cargas de trabajo	Ahora es posible obtener una vista detallada del rendimiento de las cargas de trabajo consultando el gráfico de desglose de ejecuciones de cargas de trabajo en la consola. Para obtener más información, consulte Análisis del rendimiento de las cargas de trabajo .	30 de julio de 2018

Pistas de mantenimiento	Ahora puede determinar si el clúster se actualizará siempre a la última versión de Amazon Redshift o a una versión anterior seleccionando una pista de mantenimiento. Para obtener más información, consulte Elección de pistas de mantenimiento del clúster .	26 de julio de 2018
Controladores JDBC y ODBC actualizados	Ahora Amazon Redshift admite nuevas versiones de los controladores JDBC y ODBC. Para obtener más información, consulte Configuración de una conexión JDBC y Configuración de una conexión ODBC .	13 de julio de 2018
Versiones de lanzamiento de clúster bajo demanda	Ahora puede actualizar su clúster a la última versión de lanzamiento en cuanto esté disponible. Para obtener más información, consulte Administración de versiones del clúster .	29 de junio de 2018

En la siguiente tabla se describen los cambios importantes en la Guía de administración de clústeres antes de julio de 2018.

Cambio	Descripción	Fecha de la versión
Nuevas métricas de CloudWatch	Se han agregado nuevas métricas de CloudWatch para monitorear el rendimiento de las consultas. Para obtener más información, consulte Supervisión de Amazon Redshift mediante las métricas de CloudWatch (p. 422) .	17 de mayo de 2018
Nuevos controladores JDBC y ODBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.2.12.1017. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129) . Los controladores ODBC de Amazon Redshift de se han actualizado a la versión 1.1001. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138) .	7 de marzo de 2018
Cifrado de HSM	solo admite Amazon Redshift.AWS CloudHSMPara la administración de claves de módulo de seguridad de hardware (HSM). Para obtener más información, consulte Cifrado de base de datos de Amazon (p. 286) .	6 de marzo de 2018
Encadenamiento de roles de IAM	Si un rol de IAM que está asociado al clúster no tiene acceso a los recursos necesarios, puede encadenar otro rol, que posiblemente pertenezca a otra cuenta. El clúster asumirá de forma temporal el rol encadenado para obtener acceso a los datos. También puede conceder acceso entre cuentas mediante el encadenamiento de roles. Cada uno	23 de febrero de 2018

Cambio	Descripción	Fecha de la versión
	de los roles de la cadena asume el rol siguiente, hasta que el clúster asume el rol situado al final de la cadena. Puede encadenar un máximo de 10 roles. Para obtener más información, consulte Encadenamiento de roles de IAM en Amazon Redshift (p. 366).	
Nuevos tipos de nodos DC2	La nueva generación de tipos de nodos de Dense Compute (DC, computación de alta densidad) ofrece un rendimiento mucho mejor al mismo precio que DC1. Para aprovechar las mejoras del rendimiento, puede migrar su clúster DC1 a los más recientes tipos de nodos DC2. Para obtener más información, consulte Clusters y nodos en Amazon Redshift (p. 5).	17 de octubre de 2017
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift se han actualizado a la versión 1.2.10.1009. Asimismo, ahora se admiten controladores JDBC con la versión 4.2. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129).	16 de octubre de 2017
Certificados de ACM	Amazon Redshift está sustituyendo los certificados SSL de sus clústeres por AWS Certificate Manager (ACM) expidió certificados. ACM es una entidad de certificación (CA) pública de confianza en la que confían la mayoría de los sistemas actuales. Es posible que tenga que actualizar sus certificados de CA raíz de confianza actuales para seguir conectándose a los clústeres que usan SSL. Para obtener más información, consulte Migración a certificados de ACM para las conexiones SSL (p. 155).	18 de septiembre de 2017
Roles vinculados a servicios	Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Amazon Redshift. Los roles vinculados a servicios están predefinidos por Amazon Redshift e incluyen todos los permisos que el servicio requiere para llamar a AWS en nombre de su clúster de Amazon Redshift. Para obtener más información, consulte Uso de roles vinculados a servicios para Amazon Redshift (p. 322).	18 de septiembre de 2017
Autenticación de usuarios de base de datos de IAM	Puede configurar el sistema para permitir que los usuarios creen credenciales de usuario e inicien sesión en la base de datos en función de sus credenciales de IAM. También puede configurar el sistema para permitir que los usuarios inicien sesión mediante el inicio de sesión único (SSO) federado a través de un proveedor de identidad compatible con SAML 2.0. Para obtener más información, consulte Uso de la autenticación de IAM para generar credenciales de usuario de base de datos (p. 324).	11 de agosto de 2017

Cambio	Descripción	Fecha de la versión
Nuevos controladores JDBC y ODBC	Los nuevos controladores JDBC y ODBC admiten la autenticación de usuarios de bases de datos de IAM. Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.2.7.1003. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129). Los controladores ODBC de Amazon Redshift de se han actualizado a la versión 1.3.6.1000. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138).	11 de agosto de 2017
La restauración de nivel de tabla admite Enhanced VPC Routing (enrutamiento VPC mejorado)	La restauración de nivel de tabla ahora se admite en clústeres que utilizan Enhanced VPC Routing (p. 202) . Para obtener más información, consulte Restauración de una tabla a partir de una instantánea (p. 245) .	19 de julio de 2017
Reglas de monitorización de consultas	A través de las reglas de monitorización de consultas de WLM, puede definir los límites de rendimiento basados en métricas para las colas de WLM y especificar la acción que se debe realizar cuando una consulta supera esos límites: log, hop o abort. Puede definir las reglas de monitorización de consultas como parte de la configuración de la administración de cargas de trabajo (WLM). Para obtener más información, consulte Configuración de la administración de cargas de trabajo (p. 213) .	21 de abril de 2017
Nuevos controladores JDBC y ODBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.2.1.1001. Asimismo, ahora se admiten controladores JDBC con la versión 4.2. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129). Los controladores ODBC de Amazon Redshift de se han actualizado a la versión 1.1000. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138).	18 de noviembre de 2016
Enhanced VPC Routing	Cuando utiliza el enrutamiento de VPC mejorado de Amazon Redshift, Amazon Redshift obliga a todos los COPY y DESCARGARE El tráfico entre el clúster y los repositorios de datos a través de Amazon VPC. Para obtener más información, consulte Enhanced VPC Routing (p. 202) .	15 de septiembre de 2016
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.17.1017. Asimismo, ahora se admiten controladores JDBC con la versión 4.2. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129) .	5 de julio de 2016

Cambio	Descripción	Fecha de la versión
Nuevos campos de registro de conexión	El registro de auditoría Registro de conexión (p. 374) tiene dos campos nuevos para realizar un seguimiento de las conexiones SSL. Si habitualmente carga registros de auditoría a una tabla de Amazon Redshift, necesitará añadir las siguientes columnas nuevas a la tabla de destino: sslcompression y sslexpansion.	5 de mayo de 2016
Nuevos controladores ODBC	Los controladores ODBC de Amazon Redshift de se han actualizado a la versión 1.2.7.1007. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138) .	30 de marzo de 2016
Roles de IAM para COPY y UNLOAD	Ahora puede especificar uno o másAWS Identity and Access Management(IAM) que el clúster puede utilizar para la autenticación para obtener acceso a otrosAWSServicios de . Los roles de IAM ofrecen una alternativa más segura para proporcionar la autenticación con los comandos COPY, UNLOAD o CREATE LIBRARY. Para obtener más información, consulte Autorizar a Amazon Redshift a obtener acceso a otrosAWSServicios de en su nombre (p. 363) y Autorización de uso de las operaciones COPY, UNLOAD, CREATE EXTERNAL SCHEMA mediante roles de IAM (p. 368) .	29 de marzo de 2016
Restaurar desde la tabla	Puede restaurar una tabla desde una instantánea de clúster a una tabla nueva en un clúster activo. Para obtener más información, consulte Restauración de una tabla a partir de una instantánea (p. 245) .	10 de marzo de 2016
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.10.1013. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129) . Ahora puede definir la propiedad SSLMode para especificar si el controlador debe verificar los nombres del host cuando valida los certificados TLS/SSL. Para obtener más información, consulte Configurar las opciones del controlador JDBC (p. 134) .	18 de febrero de 2016
Uso de la condición IAM en las políticas	Puede restringir aún más el acceso a recursos mediante el elemento Condición en las políticas de IAM. Para obtener más información, consulte Uso de condiciones de políticas de IAM para control de acceso preciso (p. 309) .	10 de diciembre de 2015
Modificación a acceso público	Puede modificar un clúster existente en una VPC para cambiar si es de acceso público o no. Para obtener más información, consulte Modificación de un clúster (p. 59) .	20 de noviembre de 2015

Cambio	Descripción	Fecha de la versión
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.10.1010. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129). Los controladores Amazon RedShiftOBC de se han actualizado a la versión 1.2.6.1006. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138).	19 de noviembre de 2015
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	28 de agosto de 2015
Actualización de la documentación	Se actualizó la guía para la solución de problemas sobre la configuración de opciones de red para asegurar que los hosts con diferentes tamaños de maximum transmission unit (MTU, unidad de transmisión máxima) puedan determinar el tamaño de un paquete para una conexión. Para obtener más información, consulte Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster (p. 173).	25 de agosto de 2015
Actualización de la documentación	Se revisó toda la sección sobre los grupos de parámetros para una mejor organización y claridad. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift (p. 210).	17 de agosto de 2015
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift de se han actualizado a la versión 1.1.7. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129).	14 de agosto de 2015
Propiedades dinámicas de WLM	El parámetro de configuración de WLM ahora admite la aplicación de algunas propiedades de manera dinámica. Otras propiedades son cambios estáticos y requieren que los clústeres asociados se reinicien para que se apliquen los cambios de la configuración. Para obtener más información, consulte Propiedades dinámicas y estáticas de WLM (p. 213) y Grupos de parámetros de Amazon Redshift (p. 210).	3 de agosto de 2015
Copia de clústeres cifrados con KMS a otroAWSRegión	Se ha añadido contenido sobre la configuración de la copia de instantánea para conceder la habilitación para copiarAWS KMSClústeres cifrados con otraAWSRegión . Para obtener más información, consulte CopiarAWS KMS —instantáneas cifradas en otroAWSRegión (p. 287).	28 de julio de 2015
Actualización de la documentación	Se ha actualizado la sección de cifrado de la base de datos para explicar mejor cómo utiliza Amazon RedshiftAWS KMSo HSM para administrar las claves y cómo funciona el proceso de cifrado con cada una de estas opciones. Para obtener más información, consulte Cifrado de base de datos de Amazon (p. 286).	28 de julio de 2015

Cambio	Descripción	Fecha de la versión
Nuevos controladores JDBC	Los controladores JDBC de Amazon Redshift se han actualizado a la versión 1.1.7. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129) .	2 de julio de 2015
Nuevo tipo de nodo	Amazon Redshift ahora ofrece un nuevo tipo de nodo, el DS2. Se actualizaron las referencias a los tipos de nodos existentes en la documentación para utilizar los nuevos nombres introducidos en esta publicación. También se revisó la sección para una mejor explicación sobre las combinaciones de tipos de nodos y aclaración de los límites de cuota predeterminados. Para obtener más información, consulte Clusters y nodos en Amazon Redshift (p. 5) .	9 de junio de 2015
Ofertas de nodos reservados	Se añadió contenido sobre las nuevas ofertas de nodos reservados. También se revisó la sección para brindar una mejor explicación y comparación de las ofertas disponibles y proporcionar ejemplos para demostrar cómo los precios de los nodos reservados y bajo demanda afectan la facturación. Para obtener más información, consulte Overview (p. 271) .	9 de junio de 2015
Nuevos controladores ODBC	Se ha actualizado el controlador ODBC de Amazon Redshift. Se añadió una sección sobre las versiones anteriores de estos controladores y un enlace a las notas de la versión de los controladores. Para obtener más información, consulte Configuración de una conexión ODBC (p. 138) .	5 de junio de 2015
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	30 de abril de 2015
Actualización de la documentación	Se han actualizado los enlaces de descarga de a nuevas versiones de los controladores JDBC de Amazon Redshift y se ha añadido una sección sobre las versiones anteriores de estos controladores. También se añadió un enlace a las notas de la versión de los controladores. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129) .	1 de abril de 2015

Cambio	Descripción	Fecha de la versión
Actualización de la documentación	Se añadieron descargas de nuevas versiones de los controladores JDBC de Amazon Redshift. También se ha actualizado el formato de la dirección URL de Amazon Redshift JDBC. Para obtener más información, consulte Configuración de una conexión de controlador JDBC versión 1.0 (p. 129). Se añadieron reglas de entrada del grupo de seguridad del clúster como recurso que se puede etiquetar. Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift (p. 500). Se actualizaron las instrucciones para añadir una regla de entrada del grupo de seguridad del clúster y se añadieron instrucciones para etiquetar una regla de entrada del grupo de seguridad del clúster. Para obtener más información, consulte Administración de grupos de seguridad de clúster mediante la consola (p. 391).	16 de marzo de 2015
Nueva característica	Esta publicación de Amazon Redshift presenta nuevos controladores JDBC y ODBC optimizados para utilizarse con Amazon Redshift. Para obtener más información, consulte Conexión a un clúster de Amazon Redshift mediante herramientas de cliente SQL (p. 98).	26 de febrero de 2015
Nueva característica	Esta publicación de Amazon Redshift presenta las métricas de rendimiento del clúster que le permiten ver y analizar los detalles de ejecución de una consulta. Para obtener más información, consulte Visualización de consultas y cargas (p. 448).	26 de febrero de 2015
Actualización de la documentación	Se ha añadido una nueva política de ejemplo en la que se muestra la concesión de permisos a AWS acciones de servicio y recursos en los que se basa Amazon Redshift. Para obtener más información, consulte Ejemplos de políticas administradas por el cliente (p. 316).	16 de enero de 2015
Actualización de la documentación	Se actualizó la guía sobre la configuración de la maximum transmission unit (MTU, unidad de transmisión máxima) para deshabilitar tramas gigantes TCP/IP. Para obtener más información, consulte Usar EC2-VPC al crear el clúster (p. 9) y Falta de respuesta de las consultas y pérdidas de consultas antes de llegar al clúster (p. 173).	16 de enero de 2015
Actualización de la documentación	Se ha revisado el contenido sobre el parámetro <code>wlm_json_configuration</code> y se ha proporcionado una sintaxis de ejemplo para configurar este parámetro utilizando la AWS CLI en los sistemas operativos Microsoft Windows, Mac OS X y Linux. Para obtener más información, consulte Configuración de la administración de cargas de trabajo (p. 213).	13 de enero de 2015
Actualización de la documentación	Se añadieron notificaciones y descripciones faltantes de eventos. Para obtener más información, consulte Categorías y mensajes de eventos de Amazon Redshift (p. 477).	8 de enero de 2015

Cambio	Descripción	Fecha de la versión
Actualización de la documentación	Se han actualizado las directrices sobre las políticas de IAM para las acciones y recursos de Amazon Redshift. Se revisó la sección para mejorar la organización y la claridad. Para obtener más información, consulte Seguridad en Amazon Redshift (p. 283) .	21 de noviembre de 2014
Nueva característica	Esta versión de Amazon Redshift introduce la capacidad de cifrar clústeres mediante claves de cifrado de AWS Key Management Service (AWS KMS). AWS KMS combina hardware y software seguros de alta disponibilidad para ofrecer un sistema de administración de claves adaptado a la nube. Para obtener más información acerca de AWS KMS y las opciones de cifrado de Amazon Redshift, consulte Cifrado de base de datos de Amazon (p. 286) y Administración de clústeres a través de la consola (p. 44) .	12 de noviembre de 2014
Nueva característica	Esta publicación de Amazon Redshift presenta la función para etiquetar los recursos, como clústeres y instantáneas. Las etiquetas le permiten proporcionar metadatos definidos por el usuario para categorizar los informes de facturación basados en la asignación de costos y ayudar a identificar mejor los recursos de inmediato. Para obtener más información, consulte Etiquetado de recursos en Amazon Redshift (p. 500) .	4 de noviembre de 2014
Nueva característica	Se aumentó el límite de nodos máximo a 128 para los tamaños de nodo dw1.8xlarge y dw2.8xlarge. Para obtener más información, consulte Clusters y nodos en Amazon Redshift (p. 5) .	30 de octubre de 2014
Actualización de la documentación	Se añadieron enlaces a los paquetes redistribuibles de Microsoft Visual C++ 2010 que se requieren para que Amazon Redshift utilice los controladores PostgreSQL ODBC. Para obtener más información, consulte Instalación y configuración del controlador ODBC de Amazon Redshift en Microsoft Windows (p. 139) .	30 de octubre de 2014
Nueva característica	Se ha añadido la función para terminar consultas y cargas desde la consola de Amazon Redshift. Para obtener más información, consulte Visualización de consultas y cargas (p. 448) y Visualización de métricas de clúster durante las operaciones de carga (p. 460) .	28 de octubre de 2014
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	17 de octubre de 2014
Nuevo contenido	Se añadió contenido sobre el cierre y la eliminación de clústeres. Para obtener más información, consulte Cierre y eliminación de clústeres (p. 33) y Eliminación de un clúster (p. 61) .	14 de agosto de 2014

Cambio	Descripción	Fecha de la versión
Actualización de la documentación	Se ha clarificado el comportamiento de la opción Allow Version Upgrade (Permitir actualización de versiones) en los clústeres. Para obtener más información, consulte Descripción general de los clústeres de Amazon Redshift (p. 5) .	14 de agosto de 2014
Actualización de la documentación	Se revisaron los procedimientos, las capturas de pantalla y la organización de tema sobre el trabajo con clústeres de en la consola de Amazon Redshift. Para obtener más información, consulte Administración de clústeres a través de la consola (p. 44) .	11 de julio de 2014
Nuevo contenido	Se añadió un nuevo tutorial sobre el cambio de tamaño de los clústeres de Amazon Redshift, que incluye cómo cambiar el tamaño de un clúster mientras reduce la cantidad de tiempo que el clúster está en modo de solo lectura. Para obtener más información, consulte Cambio de tamaño de los clústeres de Amazon Redshift (p. 23) .	27 de junio de 2014
Nueva característica	Se añadió la función para cambiar el nombre de los clústeres. Para obtener más información, consulte Cambio de nombre de los clústeres (p. 32) y Modificación de un clúster (p. 59) .	2 de junio de 2014
Actualización de la documentación	Se actualizó el ejemplo de código .NET para utilizar el proveedor de datos ODBC cuando se conecta a un clúster mediante programación utilizando .NET. Para obtener más información, consulte Conexión a un clúster mediante .NET (p. 168) .	15 de mayo de 2014
Nueva característica	Se añadieron las opciones para seleccionar un grupo de parámetros y un grupo de seguridad diferentes cuando restaura un clúster a partir de una instantánea. Para obtener más información, consulte Restauración de un clúster desde una instantánea (p. 258) .	12 de mayo de 2014
Nueva característica	Se ha añadido una nueva sección para describir cómo se configura una alarma predeterminada de Amazon CloudWatch para supervisar el porcentaje de espacio en disco utilizado en un clúster de Amazon Redshift. Esta alarma es una nueva opción en el proceso de creación de clúster. Para obtener más información, consulte Alarma predeterminada de espacio en disco (p. 21) .	28 de abril de 2014
Actualización de la documentación	Se ha clarificado la información acerca de la compatibilidad de Elliptic curve Diffie—Hellman Exchange (ECDHE) en Amazon Redshift. Para obtener más información, consulte Conexión mediante una SSL (p. 152) .	22 de abril de 2014
Nueva característica	Se ha añadido una instrucción sobre la compatibilidad de Amazon Redshift con el protocolo de acuerdo de claves Elíptico curve Diffie—Hellman (ECDH). Para obtener más información, consulte Conexión mediante una SSL (p. 152) .	18 de abril de 2014

Cambio	Descripción	Fecha de la versión
Actualización de la documentación	Se revisaron y reorganizaron los temas en la sección Conexión a un clúster de Amazon Redshift mediante herramientas de cliente SQL (p. 98) . Se añadió más información acerca de las conexiones ODBC y JDBC y se agregó una nueva sección para solucionar problemas de conexión.	15 de abril de 2014
Actualización de la documentación	Se añadió una versión en los ejemplos de la política de IAM a lo largo de la guía.	3 de abril de 2014
Actualización de la documentación	Se añadió información acerca del funcionamiento de los precios cuando cambia el tamaño de un clúster. Para obtener más información, consulte Compra de nodos reservados de Amazon Redshift (p. 271) .	2 de abril de 2014
Nueva característica	Se añadió una sección sobre un nuevo parámetro, <code>max_cursor_result_set_size</code> , que establece el tamaño máximo de conjuntos de resultados, en megabytes, que pueden almacenarse por cursor individual. El valor del parámetro también afecta el número de cursores activos simultáneamente para el clúster. Para obtener más información, consulte Grupos de parámetros de Amazon Redshift (p. 210) .	28 de marzo de 2014
Nueva característica	Se ha añadido una explicación sobre el campo Cluster Version (Versión del clúster), que ahora incluye la versión del motor del clúster y el número de revisión de la base de datos. Para obtener más información, consulte Clúster de Amazon Redshift (p. 5) .	21 de marzo de 2014
Nueva característica	Se ha actualizado el procedimiento de cambio de tamaño para mostrar información nueva sobre el progreso del cambio de tamaño en la pestaña Status (Estado) del clúster. Para obtener más información, consulte Redimensionamiento de un clúster (p. 64) .	21 de marzo de 2014
Actualización de la documentación	Se reorganizó y actualizó ¿Qué es Amazon Redshift (p. 1) y se revisó Información general sobre la administración de Amazon Redshift (p. 1) . Se publicaron varias correcciones de la documentación.	21 de febrero de 2014
Nueva característica	Se añadieron nuevos tipos y tamaños de nodos para los clústeres de Amazon Redshift y se reescribió el tema relacionado información general del clúster para obtener una mejor organización y claridad basada en los comentarios. Para obtener más información, consulte Clúster de Amazon Redshift (p. 5) .	23 de enero de 2014
Nueva característica	Se ha añadido información sobre el uso de direcciones IP elásticas (EIP) para los clústeres de Amazon Redshift de acceso público de en las nubes virtuales privadas. Para obtener más información sobre EIP en Amazon Redshift, consulte Administración de clústeres en una VPC (p. 75) y Creación de un clúster en una VPC (p. 77) .	20 de diciembre de 2013

Cambio	Descripción	Fecha de la versión
Nueva característica	Adición de información sobre laAWS CloudTrailPara Amazon Redshift. Para obtener más información acerca de la compatibilidad de Amazon Redshift para CloudTrail, consulte Registro de llamadas de la API de Amazon Redshift conAWS CloudTrail (p. 380).	13 de diciembre de 2013
Nueva característica	Se ha añadido información sobre el nuevo registro de actividad del usuario y laenable_user_activity_loggingPara la función de registro de auditoría de bases de datos de en Amazon Redshift. Para obtener más información acerca del registro de auditoría de la base de datos, consulte Registro de auditoría de bases de datos (p. 373). Para obtener más información acerca de los parámetros de la base de datos, consulte Grupos de parámetros de Amazon Redshift (p. 210).	6 de diciembre de 2013
Nueva característica	Se ha actualizado para describir la configuración de Amazon Redshift para copiar automáticamente las instantáneas manuales y automáticas a unAWSRegión . Para obtener más información acerca de la configuración para copiar instantáneas entre regiones, consulte Copia de instantáneas en otroAWSRegión (p. 242).	14 de noviembre de 2013
Nueva característica	Se ha añadido una sección para describir el registro de auditoría de Amazon Redshift para la actividad de conexión y la actividad del usuario, así como el almacenamiento de estos registros en Amazon S3. Para obtener más información acerca del registro de auditoría de la base de datos, consulte Registro de auditoría de bases de datos (p. 373).	11 de noviembre de 2013
Nueva característica	Se ha añadido una sección para describir el cifrado de Amazon Redshift con nuevas características para administrar las claves de cifrado de en un módulo de seguridad de hardware (HSM) y rotar claves de cifrado. Para obtener más información acerca del cifrado, el HSM; y la rotación de claves, consulte Cifrado de base de datos de Amazon (p. 286), Cifrado para Amazon Redshift mediante módulos de seguridad de hardware (p. 288) y Rotación de claves de cifrado en Amazon Redshift (p. 289).	11 de noviembre de 2013
Nueva característica	Se ha actualizado para describir la publicación de notificaciones de eventos de Amazon Redshift mediante Amazon SNS. Para obtener más información sobre las notificaciones de eventos de Amazon Redshift, consulte Notificaciones de eventos de Amazon Redshift (p. 475).	11 de noviembre de 2013
Nueva característica	Se ha actualizado para describir los permisos de nivel de recursos de IAM. Para obtener más información acerca de los permisos de Amazon Redshift IAM, consulte Seguridad en Amazon Redshift (p. 283).	9 de agosto de 2013

Cambio	Descripción	Fecha de la versión
Nueva característica	Se realizó una actualización para describir la restauración de las métricas de progreso. Para obtener más información, consulte Restauración de un clúster desde una instantánea (p. 243) .	9 de agosto de 2013
Nueva característica	Se realizó una actualización para describir el uso compartido de instantáneas de clústeres y la creación de métricas de progreso de instantáneas. Para obtener más información, consulte Uso compartido de instantáneas (p. 248) .	17 de julio de 2013
Correcciones de la documentación	Se publicaron varias correcciones de la documentación.	8 de julio de 2013
Nuevas pantallas de consolas	Se ha actualizado la Guía de administración de clústeres para hacer coincidir los cambios realizados en la consola de Amazon Redshift.	22 de abril de 2013
Nueva guía	Esta es la primera versión de la Guía de administración de Amazon Redshift.	14 de febrero de 2013

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.