aws

Guía para desarrolladores

OpenSearch Servicio Amazon

OpenSearch Servicio Amazon: Guía para desarrolladores

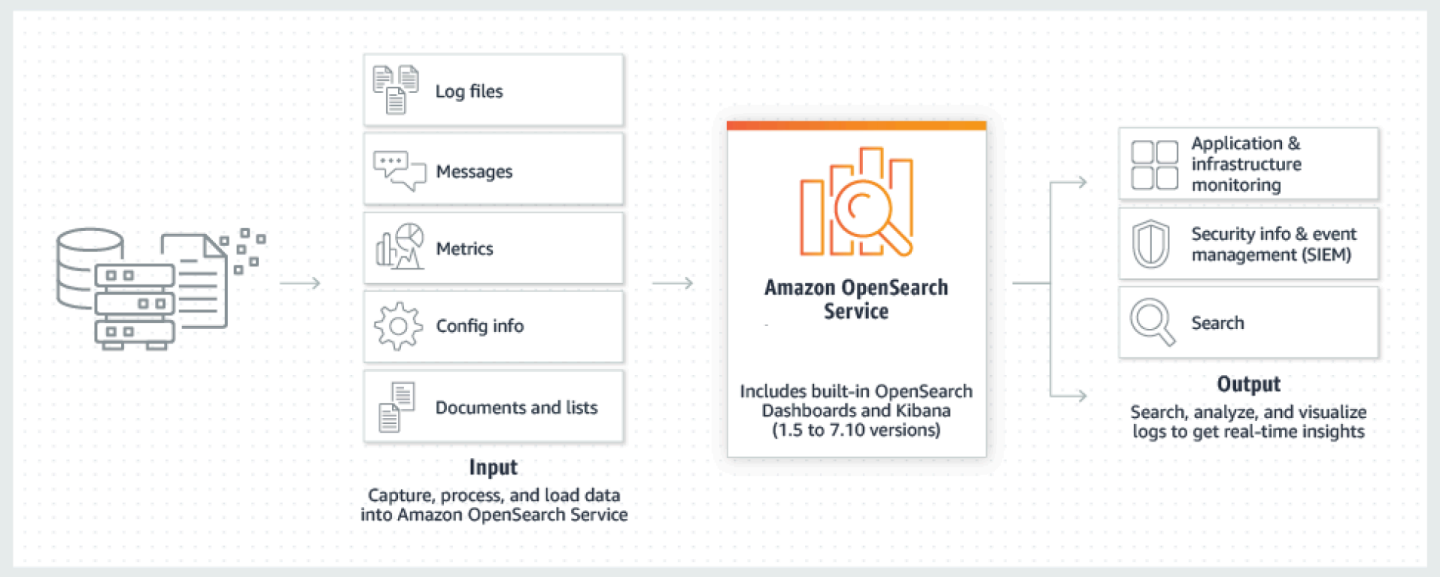
Table of Contents

¿Qué es Amazon OpenSearch Service?

Amazon OpenSearch Service es un servicio administrado que facilita la implementación, la operación y el escalado de clústeres de OpenSearch en la nube de AWS. Amazon OpenSearch Service es compatible con OpenSearch y con la version heredada de Elasticsearch OSS (con hasta 7.10, la versión final de código abierto del software). Al crear un clúster, tiene la opción de elegir qué motor de búsqueda utilizar.

OpenSearch es un motor de búsqueda y análisis totalmente de código abierto para casos de uso como análisis de registros, monitoreo de aplicaciones en tiempo real y análisis de secuencias de clics. Para más información, consulte la documentación de OpenSearch.

Amazon OpenSearch Service le proporciona todos los recursos para su clúster y lo inicia. También detecta y sustituye automáticamente los nodos de OpenSearch Service que tienen algún error. De este modo, reduce la sobrecarga asociada con las infraestructuras autoadministradas. Puede escalar el clúster con una única llamada al API o con algunos clics en la consola.



Para empezar a usar OpenSearch Service, debe crear un dominio de OpenSearch Service, que equivale a un clúster de OpenSearch Service. Cada instancia EC2 del clúster actúa como un nodo de OpenSearch Service.

Puede utilizar la consola de OpenSearch Service para instalar y configurar un dominio en unos minutos. Si prefiere el acceso mediante programación, puede utilizar el AWS CLI o los SDK de AWS.

Características de Amazon OpenSearch Service

OpenSearch Service incluye las siguientes características:

Escalado

- Varias configuraciones de CPU, memoria y capacidad de almacenamiento, que se denominan tipos de instancias, que incluyen instancias rentables de Graviton
- Hasta 3 PB de almacenamiento asociado
- Almacenamiento rentable UltraWarm y frío para datos de solo lectura

Seguridad

- Control de acceso de AWS Identity and Access Management (IAM)
- Integración sencilla con Amazon VPC y grupos de seguridad de VPC
- Cifrado de datos en reposo y cifrado de nodo a nodo.
- Autenticación de Amazon Cognito, HTTP Basic o SAML para paneles de OpenSearch
- Seguridad en el nivel de índice, de documento y de campo
- Registros de auditoría
- Tenencia múltiple de paneles

Estabilidad

- Numerosas ubicaciones geográficas para los recursos, denominadas regiones y zonas de disponibilidad
- Asignación de nodos en dos o tres zonas de disponibilidad de la misma región de AWS, lo que se conoce como Multi-AZ
- Nodos principales dedicados para aligerar las tareas de administración del clúster
- Instantáneas automatizadas para realizar backups y restaurar dominios de OpenSearch Service

Flexibilidad

- Compatibilidad con SQL para la integración con aplicaciones de inteligencia empresarial (BI)
- Paquetes personalizados para mejorar los resultados de búsqueda

Integración con servicios populares

- Visualización de datos mediante OpenSearch Dashboards
- Integración con Amazon CloudWatch para monitorerar las métricas de los dominios de OpenSearch Service y definir alarmas
- Integración con AWS CloudTrail para auditar las llamadas a la API de configuración en los dominios de OpenSearch Service
- Integración con Amazon S3, Amazon Kinesis y Amazon DynamoDB para cargar datos de streaming en OpenSearch Service
- Alertas de Amazon SNS cuando los datos superan determinados umbrales

Amazon OpenSearch sin servidor

Amazon OpenSearch sin servidor es una configuración bajo demanda, sin servidor y de escalado automático para Amazon OpenSearch Service. Elimina las complejidades operativas del aprovisionamiento, la configuración y el ajuste de los clústeres de OpenSearch. Para más información, consulte Amazon OpenSearch Serverless.

Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion es un recopilador de datos totalmente administrado, basado en Data Prepper, que proporciona datos de registro y rastreo en tiempo real a los dominios de Amazon OpenSearch Service y a las colecciones de OpenSearch sin servidor. Le permite filtrar, enriquecer, transformar, normalizar y agregar datos para su análisis y visualización posteriores. Para más información, consulte Amazon OpenSearch Ingestion.

Versiones compatibles de OpenSearch y Elasticsearch

OpenSearch Service admite actualmente las siguientes versiones de OpenSearch:

- 2.11, 2.9, 2.7, 2.5, 2.3, 1.3, 1.2, 1.1, 1.0

OpenSearch Service también admite las siguientes versiones heredadas de Elasticsearch OSS:

- 7.10, 7.9, 7.8, 7.7, 7.4, 7.1
- 6.8, 6.7, 6.5, 6.4, 6.3, 6.2, 6.0

- 5.6, 5.5, 5.3, 5.1
- 2.3
- 1.5

Para más información, consulte the section called “Operaciones admitidas”, the section called “Características por versión de motor” y the section called “Complementos por versión de motor”.

Si inicia un nuevo proyecto de OpenSearch Service, recomendamos que elija la última versión de OpenSearch compatible. Si tiene un dominio existente que utiliza una versión antigua de Elasticsearch, puede optar por mantener el dominio o migrar sus datos. Para más información, consulte the section called “Actualización de dominios”.

Precios de Amazon OpenSearch Service

Para OpenSearch Service, paga por cada hora de uso de una instancia EC2 y por el tamaño acumulado de cualquier volumen de almacenamiento de EBS adjunto a sus instancias. También se aplican cargos por transferencia de datos de AWS estándar.

Sin embargo, existen algunas excepciones notables en la transferencia de datos. Si un dominio utiliza varias zonas de disponibilidad, OpenSearch Service no facturará el tráfico entre estas zonas de disponibilidad. Se produce una transferencia de datos significativa dentro de un dominio durante la asignación de particiones y el reequilibrio. OpenSearch Service no mide ni factura este tráfico. Del mismo modo, OpenSearch Service no factura la transferencia de datos entre nodos UltraWarm/fríos y Amazon S3.

Para obtener información completa sobre precios, consulte los precios de Amazon OpenSearch Service. Para obtener información acerca de los gastos generados por los cambios de configuración, consulte the section called “Cargos por los cambios de configuración”.

Introducción a Amazon OpenSearch Service

Para empezar, debe registrarse para obtener una cuenta de Cuenta de AWS si no dispone de una. Después de configurar la cuenta, complete el tutorial Introducción de Amazon OpenSearch Service. Consulte los siguientes temas introductorios si desea obtener más información y conocer el servicio:

- Crear un dominio
- Ajustar el tamaño del dominio en función de la carga de trabajo

- Controlar el acceso a su dominio mediante una política de acceso al dominio o un control de acceso detallado
- Indexar datos manualmente o desde otros servicios de AWS
- Usar OpenSearch Dashboards para buscar sus datos y crear visualizaciones

Para obtener información sobre la migración a OpenSearch Service desde un clúster autoadministrado de OpenSearch, consulte the section called “Migrar a OpenSearch Service”.

Servicios de relacionados

OpenSearch Service se suele utilizar con los siguientes servicios:

Amazon CloudWatch

Los dominios de OpenSearch Service envían métricas automáticamente a CloudWatch para que pueda monitorear el estado y el rendimiento del dominio. Para más información, consulte Monitoreo de métricas del clúster de OpenSearch con Amazon CloudWatch.

CloudWatch Logs también puede funcionar en la dirección opuesta. Es posible configurar CloudWatch Logs para transmitir datos a OpenSearch Service para su análisis. Para más información, consulte the section called “Carga de datos de streaming desde Amazon CloudWatch”.

AWS CloudTrail

Puede utilizar AWS CloudTrail para obtener un historial de las llamadas a la API de configuración de OpenSearch Service y los eventos relacionados de su cuenta. Para más información, consulte Monitoreo de las llamadas a la API de Amazon OpenSearch Service con AWS CloudTrail.

Amazon Kinesis

Kinesis es un servicio administrado para el procesamiento de datos de streaming en tiempo real a una escala masiva. Para más información, consulte the section called “Cargar datos de streaming desde Amazon Kinesis Data Streams” y the section called “Carga de datos de streaming desde Amazon Data Firehose”.

Amazon S3

Amazon Simple Storage Service (Amazon S3) proporciona almacenamiento para Internet. Esta guía proporciona el código de muestra de Lambda para la integración con Amazon S3. Para más información, consulte the section called “Carga de datos de streaming desde Amazon S3”.

IAM de AWS

AWS Identity and Access Management (IAM) es un servicio web que puede utilizar para administrar el acceso a sus dominios de OpenSearch Service. Para más información, consulte the section called “Identity and Access Management”.

AWS Lambda

AWS Lambda es un servicio automático que permite ejecutar código sin aprovisionar ni administrar servidores. Esta guía proporciona código de muestra de Lambda para transmitir datos desde DynamoDB, Amazon S3 y Kinesis. Para más información, consulte the section called “Cargando datos de streaming en el OpenSearch servicio”.

Amazon DynamoDB

Amazon DynamoDB es un servicio de base de datos NoSQL completamente administrado que ofrece un rendimiento rápido y predecible con una escalabilidad óptima. Para obtener más información sobre la transmisión de datos a OpenSearch Service, consulte the section called “Carga de datos de streaming desde Amazon DynamoDB”.

Amazon QuickSight

Puede visualizar los datos de OpenSearch Service mediante los paneles de Amazon QuickSight. Para más información, consulte Uso de Amazon OpenSearch Service con Amazon QuickSight en la Guía del usuario de Amazon QuickSight.

> **Note**
>
> OpenSearch incluye código Elasticsearch con licencia de Apache de Elasticsearch B.V. y otro código fuente. Elasticsearch B.V. no es el origen de ese otro código fuente. ELASTICSEARCH es una marca comercial registrada de Elasticsearch B.V.

Configuración de Amazon OpenSearch Service

Temas

Registro para obtener una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Cómo registrarse en una Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario administrativo y utilice únicamente el usuario raíz para realizar tareas que requieran acceso de usuario raíz.

AWS le enviará un correo electrónico de confirmación luego de completar el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Crear un usuario administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de su Usuario raíz de la cuenta de AWS

1. Inicie sesión en la AWS Management Console como propietario de cuenta, elija Usuario raíz e ingrese el email de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitar un dispositivo MFA virtual para el usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario administrativo

1. Activar IAM Identity Center

   Para obtener instrucciones, consulte Enabling AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario administrativo.

   Para ver un tutorial sobre cómo utilizar Directorio de IAM Identity Center como origen de identidad, consulte Configure user access with the default Directorio de IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.

Cómo iniciar sesión como usuario administrativo

- Para iniciar sesión con el usuario del IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario del IAM Identity Center.

  Para obtener ayuda para iniciar sesión con un usuario del IAM Identity Center, consulte Iniciar sesión en el portal de acceso de AWS en la Guía del Usuario de AWS Sign-In.

Concesión de permisos

En entornos de producción, le recomendamos que utilice políticas más específicas. Para obtener más información sobre la administración de acceso, consulte Administración de acceso para recursos de AWS en la Guía del usuario de IAM.

Para dar acceso, añada permisos a los usuarios, grupos o roles:

- Usuarios y grupos en AWS IAM Identity Center:

  Cree un conjunto de permisos. Siga las instrucciones de Creación de un conjunto de permisos en la Guía del usuario de AWS IAM Identity Center.
- Usuarios administrados en IAM a través de un proveedor de identidades:

  Cree un rol para la federación de identidades. Siga las instrucciones de Creación de un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM.
- Usuarios de IAM:
  - Cree un rol que el usuario pueda aceptar. Siga las instrucciones descritas en Creación de un rol para un usuario de IAM en la Guía del usuario de IAM.
  - (No recomendado) Adjunte una política directamente a un usuario o añada un usuario a un grupo de usuarios. Siga las instrucciones descritas en Adición de permisos a un usuario (consola) de la Guía del usuario de IAM.

Conceder acceso programático

Los usuarios necesitan acceso programático si desean interactuar con AWS fuera de la AWS Management Console. La forma de conceder el acceso programático depende del tipo de usuario que acceda a AWS.

Para conceder acceso programático a los usuarios, seleccione una de las siguientes opciones.

¿Qué usuario necesita acceso programático?	Para	Mediante
Identidad del personal (Usuarios administrados en el Centro de identidades de IAM)	Utilice credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los SDK de AWS o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • En el caso de la AWS CLI, consulte Configuración de la AWS CLI para usar AWS IAM Identity Center en la Guía del usuario de AWS Command Line Interface.

¿Qué usuario necesita acceso programático?	Para	Mediante
		• En el caso de los SKD de AWS, las herramientas y las API de AWS, consulte Autenticación de IAM Identity Center en la Guía de referencia de SDK de AWS y herramientas.
IAM	Utilice credenciales temporales para firmar las solicitudes programáticas a la AWS CLI, los SDK de AWS o las API de AWS.	Siga las instrucciones de Uso de credenciales temporales con recursos de AWS de la Guía del Usuario de IAM.

¿Qué usuario necesita acceso programático?	Para	Mediante
IAM	(no recomendado) Utilice credenciales a largo plazo para firmar las solicitud es programáticas a la AWS CLI, los SDK de AWS o las API de AWS.	Siga las instrucciones de la interfaz que desea utilizar: • Para la AWS CLI, consulte Autenticación mediante credenciales de usuario de IAM en la Guía del usuario de AWS Command Line Interface. • Para los SDK de AWS y las herramientas, consulte Autenticación mediante credenciales a largo plazo en la Guía de referencia de SDK de AWS y herramien tas. • Para las API de AWS, consulte Administración de claves de acceso para usuarios de IAM en la Guía del usuario de IAM.

Instalación y configuración de la AWS CLI

Si desea utilizar las API de OpenSearch Service, debe instalar la última versión de AWS Command Line Interface (AWS CLI). No necesita la AWS CLI para utilizar OpenSearch Service desde la consola y puede empezar sin la CLI siguiendo los pasos que se indican en Introducción a Amazon OpenSearch Service.

Para configurar la AWS CLI

1. Para instalar la versión más reciente de la AWS CLI para macOS, Linux o Windows, consulte Instalación o actualización de la última versión de la AWS CLI.

2. Para configurar la AWS CLI y asegurar la configuración de su acceso a los Servicios de AWS, incluido OpenSearch Service, consulte Configuración rápida con `aws configure`.
3. Para verificar la configuración, ingrese el siguiente comando DataBrew en el símbolo del sistema.

```
aws opensearch help
```

Los comandos de la AWS CLI utilizan la Región de AWS predeterminada de su configuración, a menos que lo configure con un parámetro o un perfil. Para configurar su Región de AWS con un parámetro, puede añadir el parámetro `--region` a cada comando.

Para configurar su Región de AWS con un perfil, añada primero un perfil denominado en el archivo `~/.aws/config` o en el archivo `%UserProfile%/.aws/config` (para Microsoft Windows). Siga los pasos en Perfiles denominados para la AWS CLI. A continuación, defina la Región de AWS y otros ajustes con un comando similar al del ejemplo siguiente.

```
[profile opensearch]
aws_access_key_id = ACCESS-KEY-ID-OF-IAM-USER
aws_secret_access_key = SECRET-ACCESS-KEY-ID-OF-IAM-USER
region = us-east-1
output = text
```

Abra la consola

La mayoría de los temas orientados a las consolas de esta sección comienzan desde la consola de OpenSearch Service. Si aún no ha iniciado sesión en su Cuenta de AWS, inicie sesión, abra la consola de OpenSearch Service y continúe con la siguiente sección para empezar a utilizar OpenSearch Service.

Introducción a Amazon OpenSearch Service

En este tutorial se muestra cómo utilizar Amazon OpenSearch Service para crear y configurar un dominio de prueba. Un dominio de OpenSearch Service es sinónimo de clúster de OpenSearch. Los dominios son clústeres con la configuración, los tipos de instancia, los recuentos de instancias y los recursos de almacenamiento que especifique.

El tutorial muestra los pasos básicos para poner en marcha un dominio de OpenSearch Service rápidamente. Para obtener información detallada, consulte Creación y administración de dominios y los demás temas de esta guía. Para obtener información sobre la migración a OpenSearch Service desde un clúster autoadministrado de OpenSearch, consulte the section called “Migrar a OpenSearch Service”.

Puede completar los pasos en este tutorial usando la consola de OpenSearch Service, la AWS CLI o el SDK de AWS. Para obtener información sobre cómo instalar y configurar la AWS CLI, consulte la Guía del usuario de AWS Command Line Interface.

Paso 1: crear un dominio de Amazon OpenSearch Service

> **Important**
>
> Este es un tutorial conciso para configurar una prueba de dominio de Amazon OpenSearch Service. No utilice este proceso para crear dominios de producción. Para ver una versión completa del mismo proceso, consulte Creación y administración de dominios.

Un dominio de OpenSearch Service es sinónimo de clúster de OpenSearch. Los dominios son clústeres con la configuración, los tipos de instancia, los recuentos de instancias y los recursos de almacenamiento que especifique. Puede crear un dominio de OpenSearch Service con la consola, la AWS CLI o los SDK de AWS.

Para crear un dominio de OpenSearch Service con la consola

1. Visite https://aws.amazon.com y elija Iniciar sesión en la consola.
2. En Análisis, elija Amazon OpenSearch Service.
3. Elija Crear un dominio.

4. Proporcione un nombre para el dominio. Los ejemplos de este tutorial utilizan el nombre Películas.
5. Elija Creación estándar para el método de creación del dominio.

> **Note**
>
> Para configurar rápidamente un dominio de producción con las prácticas recomendadas, puede elegir Creación sencilla. Para el desarrollo y las pruebas de este tutorial, utilizaremos la Creación estándar.

6. Para las plantillas, elija Desarrollo/pruebas.
7. Para la opción de implementación, elija Dominio con modo de espera.
8. En Versión, elija la versión más reciente.
9. Por ahora, ignore las secciones de Nodos de datos, Almacenamiento de datos en caliente y en frío, Nodos maestros dedicados, Configuración de instantáneas y Puntos de conexión personalizados.
10. Para simplificar este tutorial, utilice un dominio de acceso público. En Red, elija Acceso público.
11. En la configuración de control de acceso detallado, mantenga seleccionada la casilla Habilitar el control de acceso detallado. Seleccione Crear usuario maestro e ingrese un nombre de usuario y una contraseña.
12. Por el momento, ignore las secciones Autenticación SAML y Autenticación de Amazon Cognito.
13. Para la Política de acceso, elija Utilizar únicamente control de acceso detallado. En este tutorial, el control de acceso detallado controla la autenticación, no la política de acceso al dominio.
14. Omita el resto de la configuración y elija Crear. Los dominios nuevos suelen tardar entre 15 y 30 minutos en inicializarse, pero pueden tardar más en función de la configuración. Una vez inicializado su dominio, selecciónelo para abrir su panel de configuración. Tome nota del punto de conexión del dominio en Información general (por ejemplo, `https://search-`*`my-domain`*`.us-east-1.es.amazonaws.com`), que deberá usar en el siguiente paso.

Siguiente: cargar datos en un dominio de OpenSearch Service para realizar la indexación

Paso 2: cargar los datos en Amazon OpenSearch Service para realizar la indexación

> **Important**
>
> Este es un tutorial conciso para cargar una pequeña cantidad de datos de prueba en Amazon OpenSearch Service. Para obtener más información sobre cómo cargar datos en un dominio de producción, consulte Indexación de datos.

Puede cargar datos en un dominio de OpenSearch Service mediante la línea de comandos o la mayoría de los lenguajes de programación.

El siguiente ejemplo requiere utilizar curl, (un cliente HTTP común), para que el proceso sea más cómodo y rápido. Los clientes como curl no pueden realizar la firma de solicitudes necesaria si sus políticas de acceso especifican roles o usuarios de IAM. Para realizar correctamente este proceso, debe utilizar un control de acceso detallado con un nombre de usuario primario y una contraseña, como los configuró en el Paso 1.

Puede instalar curl en Windows y utilizarlo desde el símbolo del sistema, pero recomendamos utilizar una herramienta como Cygwin o Windows Subsystem for Linux. La distribución de macOS y la mayoría de las distribuciones de Linux vienen con curl preinstalado.

Opción 1: cargar un solo documento

Ejecute el siguiente comando para agregar un único documento al dominio Películas:

```
curl -XPUT -u 'master-user:master-user-password' 'domain-endpoint/movies/_doc/1' -d
 '{"director": "Burton, Tim", "genre": ["Comedy","Sci-Fi"], "year": 1996, "actor":
 ["Jack Nicholson","Pierce Brosnan","Sarah Jessica Parker"], "title": "Mars Attacks!"}'
 -H 'Content-Type: application/json'
```

En el comando, proporcione el nombre de usuario y la contraseña que creó en el Paso 1.

Para obtener una explicación detallada de este comando y cómo realizar solicitudes firmadas a OpenSearch Service, consulte Indexación de datos.

Opción 2: cargar varios documentos

Para cargar un archivo JSON que contiene varios documentos en un dominio de OpenSearch Service

1. Cree un archivo local denominado `bulk_movies.json`. Pegue el siguiente contenido en el archivo y agregue una línea nueva al final:

```
{ "index" : { "_index": "movies", "_id" : "2" } }
{"director": "Frankenheimer, John", "genre": ["Drama", "Mystery", "Thriller",
 "Crime"], "year": 1962, "actor": ["Lansbury, Angela", "Sinatra, Frank", "Leigh,
 Janet", "Harvey, Laurence", "Silva, Henry", "Frees, Paul", "Gregory, James",
 "Bissell, Whit", "McGiver, John", "Parrish, Leslie", "Edwards, James", "Flowers,
 Bess", "Dhiegh, Khigh", "Payne, Julie", "Kleeb, Helen", "Gray, Joe", "Nalder,
 Reggie", "Stevens, Bert", "Masters, Michael", "Lowell, Tom"], "title": "The
 Manchurian Candidate"}
{ "index" : { "_index": "movies", "_id" : "3" } }
{"director": "Baird, Stuart", "genre": ["Action", "Crime", "Thriller"], "year":
 1998, "actor": ["Downey Jr., Robert", "Jones, Tommy Lee", "Snipes, Wesley",
 "Pantoliano, Joe", "Jacob, Ir\u00e8ne", "Nelligan, Kate", "Roebuck, Daniel",
 "Malahide, Patrick", "Richardson, LaTanya", "Wood, Tom", "Kosik, Thomas",
 "Stellate, Nick", "Minkoff, Robert", "Brown, Spitfire", "Foster, Reese",
 "Spielbauer, Bruce", "Mukherji, Kevin", "Cray, Ed", "Fordham, David", "Jett,
 Charlie"], "title": "U.S. Marshals"}
{ "index" : { "_index": "movies", "_id" : "4" } }
{"director": "Ray, Nicholas", "genre": ["Drama", "Romance"], "year": 1955, "actor":
 ["Hopper, Dennis", "Wood, Natalie", "Dean, James", "Mineo, Sal", "Backus, Jim",
 "Platt, Edward", "Ray, Nicholas", "Hopper, William", "Allen, Corey", "Birch,
 Paul", "Hudson, Rochelle", "Doran, Ann", "Hicks, Chuck", "Leigh, Nelson",
 "Williams, Robert", "Wessel, Dick", "Bryar, Paul", "Sessions, Almira", "McMahon,
 David", "Peters Jr., House"], "title": "Rebel Without a Cause"}
```

2. Ejecute el siguiente comando en el directorio local en el que está almacenado el archivo para cargarlo en el dominio Películas:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-
binary @bulk_movies.json -H 'Content-Type: application/json'
```

Para obtener más información acerca del formato de archivo masivo, consulte Indexación de datos.

Siguiente: buscar documentos

Paso 3: buscar documentos en Amazon OpenSearch Service

Para buscar documentos en un dominio de Amazon OpenSearch Service, utilice la API de búsqueda de OpenSearch. También puede utilizar OpenSearch Dashboards para buscar documentos en el dominio.

Para buscar documentos desde la línea de comandos

Ejecute el siguiente comando para buscar el dominio Películas para la palabra mars:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/movies/_search?
q=mars&pretty=true'
```

Si utilizó datos masivos en la página anterior, intente buscar rebel en su lugar.

Verá una respuesta parecida a la siguiente:

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 5,
    "successful" : 5,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 1,
      "relation" : "eq"
    },
    "max_score" : 0.2876821,
    "hits" : [
      {
        "_index" : "movies",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 0.2876821,
        "_source" : {
          "director" : "Burton, Tim",
          "genre" : [
            "Comedy",
```

```
            "Sci-Fi"
          ],
          "year" : 1996,
          "actor" : [
            "Jack Nicholson",
            "Pierce Brosnan",
            "Sarah Jessica Parker"
          ],
          "title" : "Mars Attacks!"
        }
      }
    ]
  }
}
```

Buscar documentos mediante OpenSearch Dashboards

OpenSearch Dashboards es una popular herramienta de visualización de código abierto diseñada para funcionar con OpenSearch. Proporciona una interfaz de usuario útil para que pueda buscar y monitorear índices.

Para buscar documentos de un dominio de OpenSearch Service mediante Dashboards

1. Desplácese hasta la URL de OpenSearch Dashboards para su dominio. Puede encontrar la URL en el panel del dominio en la consola de OpenSearch Service. La URL tiene este formato:

   ```
   domain-endpoint/_dashboards/
   ```

2. Inicie sesión con su nombre de usuario principal y contraseña.
3. Para utilizar Dashboards, debe crear al menos un patrón de índice. Dashboards utiliza estos patrones para identificar los índices que desea analizar. Abra el panel de navegación de la izquierda, elija Gestión de pilas, elija Patrones de índice y luego elija Crear patrón de índice. Para este tutorial, escriba Películas.
4. Elija Siguiente paso y, a continuación, elija Crear patrón de índice. Una vez creado el patrón, puede ver los diversos campos de documento, como`actor` y `director`.
5. Regrese a la pestaña Patrones de índice y asegúrese de que `movies` se establezca como valor predeterminado. Si no lo es, seleccione el patrón y elija el icono de estrella para convertirlo en el predeterminado.
6. Para comenzar a buscar los datos, abra el panel de navegación izquierdo y elija Descubrir.

7. En la barra de búsqueda, escriba mars, si cargó un solo documento, o rebel, si cargó varios documentos y, a continuación, presione Enter. Puede buscar otros términos, como nombres de actores o directores.

Siguiente: eliminar un dominio

Paso 4: eliminar un dominio de Amazon OpenSearch Service

Dado que el dominio Películas de este tutorial es para hacer pruebas, debe eliminarlo cuando termine de experimentar para evitar incurrir en gastos.

Para eliminar un dominio de OpenSearch Service de la consola

1. Inicie sesión en la consola de Amazon OpenSearch Service.
2. En Dominios, seleccione el dominio películas.
3. Elija Eliminar y confirme la eliminación.

Pasos siguientes

Ahora que sabe cómo crear un dominio e indexar datos, puede probar algunos de los siguientes ejercicios:

- Conozca más opciones avanzadas para crear un dominio. Para más información, consulte Creación y administración de dominios.
- Descubra cómo administrar los índices de un dominio. Para más información, consulte Administración de índices.
- Pruebe uno de los tutoriales para trabajar con Amazon OpenSearch Service. Para más información, consulte Tutoriales.

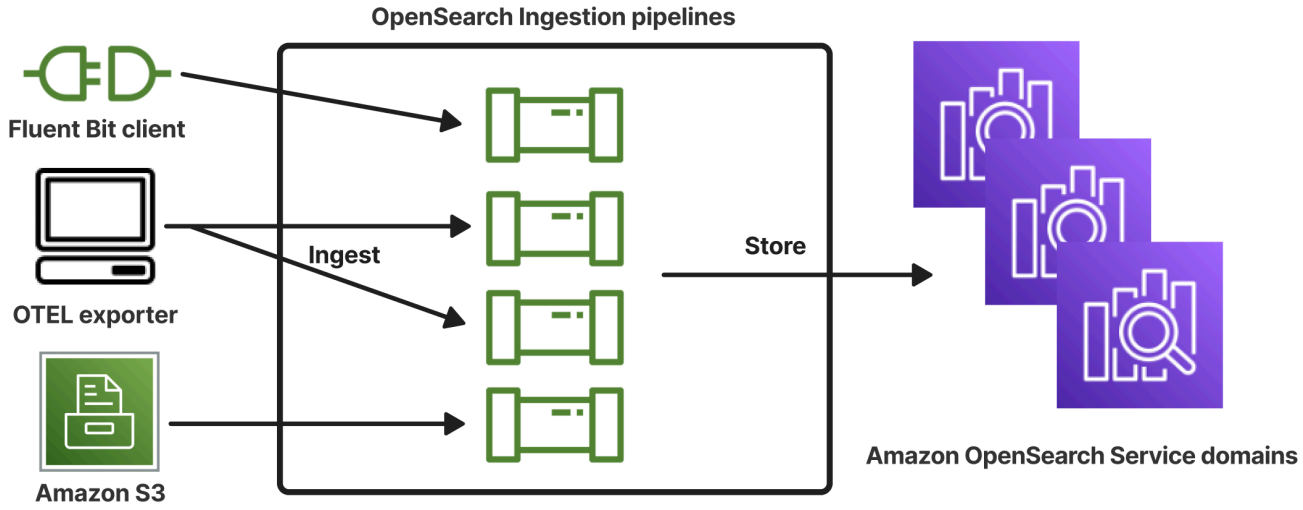
OpenSearch Ingestión de Amazon

Amazon OpenSearch Ingestion es un recopilador de datos sin servidor totalmente gestionado que proporciona datos de registro, métricas y rastreo en tiempo real a los dominios de Amazon OpenSearch Service y a las colecciones OpenSearch sin servidor.

Con OpenSearch Ingestion, ya no necesitará utilizar soluciones de terceros, como Logstash o Jaeger, para introducir datos en sus dominios de servicio y colecciones sin servidor. OpenSearch OpenSearch Puede configurar sus generadores de datos para que envíen datos a Ingestion. OpenSearch A continuación, entrega automáticamente los datos al dominio o la colección que especifique. También puede configurar OpenSearch Ingestion para transformar los datos antes de entregarlos.

Además, con OpenSearch Ingestion, no tiene que preocuparse por el aprovisionamiento de servidores, la administración y los parches del software ni por el escalado de su clúster de servidores. Usted aprovisiona los canales de ingestión directamente dentro del AWS Management Console, e OpenSearch Ingestion se encarga de gestionarlos y escalarlos.

OpenSearch La ingestión es un subconjunto de Amazon OpenSearch Service. Cuenta con tecnología de Data Prepper, que es un recopilador de datos de código abierto que puede filtrar, enriquecer, transformar, normalizar y agregar datos para su análisis y visualización posteriores.



Temas

- Conceptos clave
- Ventajas de la ingestión OpenSearch
- Limitaciones

- Versiones de Data Prepper admitidas
- Escala de canalizaciones
- OpenSearch Precios de ingestión
- Compatible Regiones de AWS
- OpenSearch Cuotas de ingestión
- Configuración de roles y usuarios en Amazon OpenSearch Ingestion
- Introducción a Amazon OpenSearch Ingestion
- Descripción general de las funciones de canalización en Amazon OpenSearch Ingestion
- Creación de canalizaciones OpenSearch de Amazon Ingestion
- Visualización de canalizaciones de Amazon OpenSearch Ingestion
- Actualización de las canalizaciones OpenSearch de Amazon Ingestion
- Detener e iniciar canalizaciones de Amazon OpenSearch Ingestion
- Eliminar canalizaciones de Amazon OpenSearch Ingestion
- Plugins y opciones compatibles para las canalizaciones de Amazon OpenSearch Ingestion
- Trabajar con las integraciones de Amazon OpenSearch Ingestion Pipeline
- Migración de datos entre dominios y colecciones mediante Amazon OpenSearch Ingestion
- Utilizar SDK de AWS para interactuar con Amazon OpenSearch Ingestion
- Casos de uso de Amazon OpenSearch Ingestion
- Seguridad en Amazon OpenSearch Ingestion
- Etiquetado de canalizaciones de Amazon OpenSearch Ingestion
- Registro y monitoreo de Amazon OpenSearch Ingestion con Amazon CloudWatch
- Prácticas recomendadas para Amazon OpenSearch Ingestion

Conceptos clave

Al comenzar con la OpenSearch ingestión, podrá beneficiarse de la comprensión de los siguientes conceptos:

Canalización

> Desde el punto de vista de OpenSearch la ingesta, una canalización se refiere a un único recopilador de datos aprovisionado que se crea dentro de Service. OpenSearch Puede

considerarlo como el archivo de configuración de YAML completo, que incluye una o más subcanalizaciones. Para ver los pasos para crear una canalización de ingesta, consulte the section called “Creación de canalizaciones”.

Subcanalización

Las subcanalizaciones se definen dentro de un archivo de configuración YAML. Cada subcanalización es una combinación de una sola fuente, un búfer, cero o más procesadores y uno o más receptores. Puede definir varias subcanalizaciones en un único archivo YAML, cada una con fuentes, procesadores y receptores únicos. Para facilitar la supervisión con CloudWatch y otros servicios, te recomendamos que especifiques un nombre de canalización que sea distinto de todas sus subcanalizaciones.

Puede encadenar varias subcanalizaciones en un único archivo YAML, de modo que la fuente de una subcanalización sea otra subcanalización y su receptor sea una tercera subcanalización. Para ver un ejemplo, consulte the section called “OpenTelemetry Colector”.

Origen

El componente de entrada de una subcanalización. Define el mecanismo mediante el cual una canalización consume los registros. La fuente puede consumir eventos ya sea recibiéndolos a través de HTTPS o leyendo desde puntos de conexión externos, como Amazon S3. Hay dos tipos de fuentes: basadas en push y basadas en pull. Las fuentes basadas en push, como los registros HTTP y OTel, transmiten los registros a los puntos de conexión de ingesta. Las fuentes basadas en pull, como el rastreo OTel y S3, extraen datos de la fuente.

Procesadores

Unidades de procesamiento intermedias que pueden filtrar, transformar y enriquecer los registros en el formato deseado antes de publicarlos en el receptor. El procesador es un componente opcional de una canalización. Si no define un procesador, los registros se publican en el formato definido en la fuente. Puede tener más de un procesador. Una canalización ejecuta los procesadores en el orden en el que los define.

Receptor

El componente de salida de una subcanalización. Define uno o más destinos en los que una subcanalización publica registros. OpenSearch La ingestión admite los dominios OpenSearch de servicio como receptores. También admite subcanalizaciones como receptores. Esto significa que puedes encadenar varias subcanalizaciones en una sola canalización de OpenSearch ingestión (archivo YAML). OpenSearch Los clústeres autogestionados no se admiten como receptores.

Búfer

La parte de un procesador que actúa como capa entre la fuente y el receptor. No puede configurar manualmente un búfer dentro de la canalización. OpenSearch La ingestión utiliza una configuración de búfer predeterminada.

Ruta

La parte de un procesador que permite a los autores de canalizaciones enviar únicamente los eventos que cumplan determinadas condiciones a distintos receptores.

Una definición de subcanalización válida debe contener una fuente y un receptor. Para obtener más información sobre cada uno de estos elementos de la canalización, consulte Referencia de configuración.

Ventajas de la ingestión OpenSearch

OpenSearch La ingestión tiene los siguientes beneficios principales:

- Elimina la necesidad de administrar manualmente una canalización autoaprovisionada.
- Escala automáticamente las canalizaciones en función de los límites de capacidad que defina.
- Mantiene la canalización actualizada con parches de seguridad y de errores.
- Ofrece la opción de conectar las canalizaciones a su nube privada virtual (VPC) para añadir un nivel de seguridad adicional.
- Le permite detener e iniciar canalizaciones para controlar los costos.
- Proporciona esquemas de configuración de canalizaciones para los casos de uso más habituales a fin de ayudarle a empezar a trabajar más rápido.
- Te permite interactuar mediante programación con tus canalizaciones a través de los distintos AWS SDK y la API de ingestión. OpenSearch
- Admite la supervisión del rendimiento en Amazon CloudWatch y el registro de errores en CloudWatch Logs.

Limitaciones

OpenSearch La ingestión tiene las siguientes limitaciones:

- Solo puede ingerir datos en dominios que ejecuten la OpenSearch versión 1.0 o una versión posterior, o Elasticsearch 6.8 o una versión posterior. Si utilizas la fuente de rastreo Otel, te recomendamos que utilices Elasticsearch 7.9 o una versión posterior para poder usar el complemento Dashboards. OpenSearch
- Si una canalización se escribe en un dominio de OpenSearch servicio que está dentro de una VPC, la canalización debe crearse en el Región de AWS mismo dominio.
- Solo puede configurar un único origen de datos dentro de una definición de canalización.
- No puedes especificar OpenSearch clústeres autogestionados como receptores.
- No puede especificar un punto de conexión personalizado como receptor. Aún puede escribir en un dominio que tenga habilitados los puntos de conexión personalizados, pero debes especificar su punto de conexión estándar.
- No puede especificar los recursos dentro de las regiones registradas como orígenes o receptores.
- Existen algunas limitaciones en los parámetros que se pueden incluir en una configuración de canalización. Para más información, consulte the section called “Requisitos y restricciones de configuración”.

Versiones de Data Prepper admitidas

OpenSearch Actualmente, Ingestion es compatible con las siguientes versiones principales de Data Prepper:

- 2.x

Al crear una canalización, utilice la opción de `version` necesaria para especificar la versión principal de Data Prepper que va a utilizar. Por ejemplo,. `version: "2"` OpenSearch Ingestion recupera la última versión secundaria compatible de esa versión principal y aprovisiona la canalización con esa versión. Para obtener más información, consulte the section called “Especificar la versión de la canalización”.

Actualmente, las canalizaciones OpenSearch de ingestión se aprovisionan con la versión 2.7 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.7. Para obtener información sobre las características y las correcciones de errores de cada versión de Data Prepper, consulte la página de Versiones. OpenSearch Ingestion no admite todas las versiones secundarias de una versión principal concreta.

Al actualizar el archivo de configuración YAML de una canalización, si hay soporte para una nueva versión secundaria de Data Prepper, OpenSearch Ingestion actualiza automáticamente la canalización a la última versión secundaria compatible de la versión principal especificada en la configuración de la canalización. Por ejemplo, es posible que tengas una `version: "2"` configuración de canalización e OpenSearch Ingestion inicialmente aprovisionó la canalización con la versión 2.6.0. Cuando se añade la compatibilidad con la versión 2.7.0 y realizas un cambio en la configuración de la canalización, OpenSearch Ingestion actualiza la canalización a la versión 2.7.0. Este proceso mantiene su canalización actualizada con las últimas correcciones de errores y mejoras de rendimiento. OpenSearch Ingestion no puede actualizar la versión principal de tu canalización a menos que cambies manualmente la `version` opción en la configuración de la canalización. Para obtener más información, consulte the section called “Actualización de las canalizaciones”.

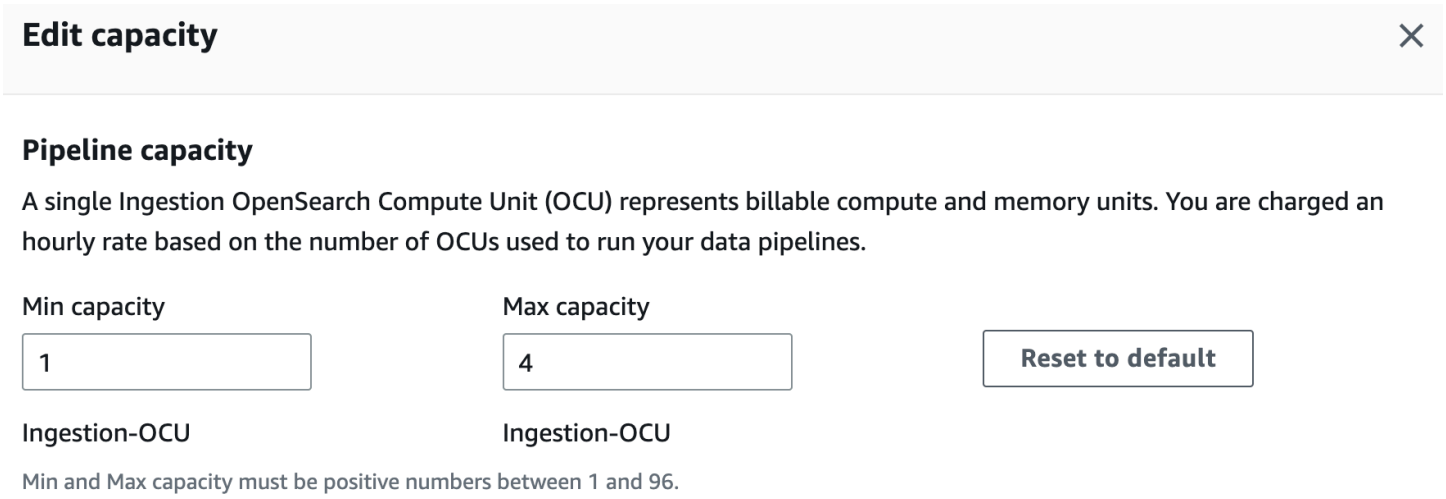
Escala de canalizaciones

No necesitas aprovisionar ni gestionar la capacidad de canalización tú mismo. OpenSearch Ingestion escala automáticamente la capacidad de sus canalizaciones en función de su carga de trabajo estimada, en función de las unidades de OpenSearch cómputo de ingestión (OCU de ingestión) mínimas y máximas que especifique.

Cada OCU de ingesta es una combinación de aproximadamente 8 GiB de memoria y 2 vCPU. Puede especificar los valores de OCU mínimos y máximos para una canalización, e OpenSearch Ingestion escalará automáticamente la capacidad de la canalización en función de estos límites.

Puede especificar los valores siguientes:

- Capacidad mínima: la canalización puede reducir la capacidad hasta este número de OCU de ingesta. La capacidad mínima especificada también es la capacidad inicial de una canalización.
- Capacidad máxima: la canalización puede aumentar la capacidad hasta este número de OCU de ingesta.



Asegúrese de que la capacidad máxima de la canalización sea lo suficientemente alta como para administrar los picos de carga de trabajo y que la capacidad mínima sea lo suficientemente baja como para minimizar los costos cuando la canalización no esté ocupada. En función de tu configuración, OpenSearch Ingestion escala automáticamente la cantidad de OCU de ingestión de tu canalización para procesar la carga de trabajo de ingesta. En cualquier momento dado, solo se le cobrarán las OCU de ingesta que se estén utilizando activamente en su canalización.

La capacidad asignada a tu canalización de OpenSearch ingestión se amplía y reduce en función de los requisitos de procesamiento de tu canalización y de la carga generada por la aplicación cliente. Cuando la capacidad es limitada, OpenSearch Ingestion se amplía mediante la asignación de más unidades de cómputo (GiB de memoria). Cuando la canalización procese cargas de trabajo más pequeñas o no procese datos en absoluto, puede reducir verticalmente hasta el mínimo de OCU de ingesta configuradas.

Puede especificar un mínimo de 1 OCU de ingesta, un máximo de 96 OCU de ingesta para las canalizaciones sin estado y un máximo de 48 OCU de ingesta para las canalizaciones con estado. Recomendamos un mínimo de 2 OCU de ingesta como mínimo para las fuentes push. Cuando el almacenamiento en búfer persistente esté activado, puede especificar un mínimo de 2 y un máximo de 384 OCU de ingesta.

Dada una canalización de registro estándar con una sola fuente, un patrón grok simple y un receptor, cada unidad de cómputo puede admitir hasta 2 MiB por segundo. En el caso de las canalizaciones de registro más complejas con varios procesadores, cada unidad de cómputo puede soportar una carga de ingesta menor. En función de la capacidad de la canalización y el uso de los recursos, se inicia el proceso de escalado OpenSearch de Ingestion.

Para garantizar una alta disponibilidad, las OCU de ingesta se distribuyen en las zonas de disponibilidad (AZ). La cantidad de AZ depende de la capacidad mínima que se especifique.

Por ejemplo, si especifica un mínimo de 2 unidades de cómputo, las OCU de ingesta que estén en uso en un momento dado se distribuyen uniformemente entre las 2 AZ. Si especifica un mínimo de 3 o más unidades de cómputo, las OCU de ingesta se distribuyen uniformemente en 3 AZ. Le recomendamos que aprovisione al menos dos OCU de ingesta para garantizar una disponibilidad del 99,9 % en sus canalizaciones de ingesta.

No se le facturan las OCU de ingesta cuando una canalización está en los estados `Create failed`, `Creating`, `Deleting` y `Stopped`.

Para ver instrucciones sobre cómo configurar y recuperar los ajustes de capacidad de una canalización, consulte the section called “Creación de canalizaciones”.

OpenSearch Precios de ingestión

En un momento específico, solo paga por la cantidad de OCU de ingesta que estén asignadas a una canalización, independientemente de si hay datos circulando por la canalización. OpenSearch La ingestión se adapta inmediatamente a sus cargas de trabajo al aumentar o reducir la capacidad de la canalización en función del uso.

Para obtener información completa sobre los precios, consulta los precios OpenSearch de Amazon Service.

Compatible Regiones de AWS

OpenSearch La ingestión está disponible en un subconjunto de Regiones de AWS ese OpenSearch servicio en el que está disponible. Para ver una lista de las regiones compatibles, consulta los puntos de conexión y las cuotas de Amazon OpenSearch Service en. Referencia general de AWS

OpenSearch Cuotas de ingestión

Para ver una lista de las cuotas predeterminadas para los recursos OpenSearch de ingestión, consulta las cuotas de Amazon OpenSearch Service.

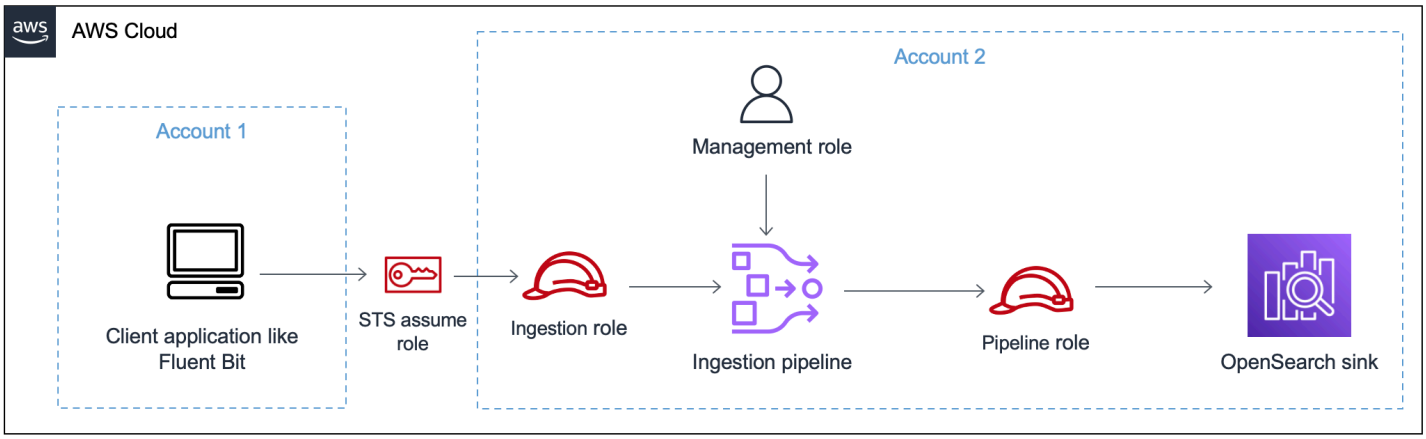
Configuración de roles y usuarios en Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion utiliza diversos modelos de permisos y roles de IAM para permitir que las aplicaciones de origen escriban en las canalizaciones y que las canalizaciones escriban en los receptores. Antes de empezar a incorporar datos, debe crear uno o más roles de IAM con permisos específicos en función de su caso de uso.

Como mínimo, se requieren los siguientes roles para configurar una canalización exitosa.

Nombre	Descripción
Rol de administración	Cualquier entidad principal que gestione canalizaciones (por lo general, un «administrador de canalizaciones») necesita un acceso de administración, que incluye permisos como `osis:CreatePipeline` y `osis:UpdatePipeline`. Estos permisos permiten al usuario administrar las canalizaciones, pero no necesariamente escribir datos en ellas.
Rol de canalización	El rol de canalización, que se especifica en la configuración de YAML de la canalización, proporciona los permisos necesarios para que una canalización escriba en el dominio o en el receptor de la colección y lea desde fuentes basadas en la extracción. Para obtener más información, consulte los temas siguientes: • the section called “Otorgar a Pipelines acceso a los dominios” • the section called “Otorgar a las canalizaciones acceso a las colecciones”
Rol de incorporación	El rol de ingestión contiene el permiso `osis:Ingest` para el recurso de canalización. Este permiso permite que los orígenes basados en push incorporen datos en una canalización.

La siguiente imagen muestra una configuración de canalización típica, en la que un origen de datos como Amazon S3 o Fluent Bit escribe en una canalización de una cuenta diferente. En este caso, el cliente debe asumir el rol de incorporación para poder acceder a la canalización. Para obtener más información, consulte the section called “Incorporación entre cuentas”.



Para obtener una guía de configuración sencilla, consulte the section called “Tutorial: incorporar datos a un dominio”.

Temas

- the section called “Rol de administración”
- the section called “Rol de incorporación”
- the section called “Rol de canalización”
- the section called “Incorporación entre cuentas”

Rol de administración

Además de los permisos `osis:*` básicos necesarios para crear y modificar una canalización, también necesita el permiso `iam:PassRole` para el recurso del rol de canalización. Cualquier Servicio de AWS que acepte un rol debe usar este permiso. OpenSearch Ingestion asume el rol cada vez que necesita escribir datos en un receptor. Esto ayuda a los administradores a garantizar que solo los usuarios autorizados puedan configurar OpenSearch Ingestion con un rol que concede permisos. Para obtener más información, consulte Concesión de permisos a un usuario para transferir un rol a un Servicio de AWS.

Si está usandoAWS Management Console (utiliza esquemas y, posteriormente, comprueba su canalización), necesita los siguientes permisos para crear y actualizar una canalización:

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

```
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:GetPipelineBlueprint",
            "osis:ListPipelineBlueprints",
            "osis:GetPipeline",
            "osis:ListPipelines",
            "osis:GetPipelineChangeProgress",
            "osis:ValidatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Si utiliza el AWS CLI (sin validar previamente su canalización ni utiliza esquemas), necesita los siguientes permisos para crear y actualizar una canalización:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:UpdatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/pipeline-role"
         ],
```

```
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Rol de canalización

Una canalización necesita ciertos permisos para escribir en su receptor. Estos permisos dependen de si el receptor es un dominio de OpenSearch Service o una colección de OpenSearch sin servidor.

Además, es posible que una canalización necesite permisos para extraer información de la aplicación de origen (si el origen es un complemento basado en la extracción) y permisos para escribir en una cola de mensajes fallidos de S3, si está configurada.

Temas

- Escribir en un receptor de dominio
- Escribir en un receptor de colecciones
- Escribir en una cola de mensajes fallidos

Escribir en un receptor de dominio

Una canalización de OpenSearch Ingestion necesita permiso para escribir en un dominio de OpenSearch Service que esté configurado como su receptor. Estos permisos incluyen la capacidad de describir el dominio y enviarle solicitudes HTTP.

Para ofrecer a su canalización los permisos necesarios para escribir en un receptor, primero cree un rol AWS Identity and Access Management (de IAM) con los permisos necesarios. Estos permisos son los mismos para las canalizaciones públicas y de VPC. A continuación, especifique el rol de canalización en la política de acceso al dominio para que el dominio pueda aceptar las solicitudes de escritura de la canalización.

Por último, especifique el ARN del rol como el valor de la opción sts_role_arn en la configuración de la canalización:

```
version: "2"
source:
```

```
  http:
    ...
processor:
  ...
sink:
  - opensearch:
      ...
      aws:
        sts_role_arn: arn:aws:iam::{your-account-id}:role/pipeline-role
```

Para obtener instrucciones para completar cada uno de estos pasos, consulte Permitir que las canalizaciones accedan a dominios.

Escribir en un receptor de colecciones

Una canalización de OpenSearch Ingestion necesita permiso para escribir en una colección de OpenSearch sin servidor que esté configurada como su receptor. Estos permisos incluyen la capacidad de describir el dominio y enviarle solicitudes HTTP.

En primer lugar, cree un rol de IAM que tenga el permiso `aoss:BatchGetCollection` para todos los recursos (*). A continuación, incluya este rol en una política de acceso a los datos y asígnele permisos para crear índices, actualizar índices, describir índices y escribir documentos dentro de la colección. Por último, especifique el ARN del rol como el valor de la opción sts_role_arn en la configuración de la canalización.

Para obtener instrucciones para completar cada uno de estos pasos, consulte Permitir que las canalizaciones accedan a las colecciones.

Escribir en una cola de mensajes fallidos

Si configura la canalización para escribir en una cola de mensajes fallidos (DLQ), debe incluir la opción en la configuración de la DLQ. `sts_role_arn` Los permisos incluidos en este rol permiten que la canalización acceda al bucket de S3 que especifique como destino para los eventos de la DLQ.

Debe usar el mismo `sts_role_arn` en todos los componentes de la canalización. Por lo tanto, debe adjuntar una política de permisos independiente a su rol de canalización que otorgue acceso a la DLQ. Como mínimo, el rol debe permitir la acción `S3:PutObject` en el recurso del bucket:

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

```
  "Statement": [
    {
      "Sid": "WriteToS3DLQ",
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::my-dlq-bucket/*"
    }
  ]
}
```

A continuación, puede especificar el rol en la configuración de la DLQ de la canalización:

```
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/pipeline-role"
```

Rol de incorporación

Todos los complementos de origen que OpenSearch Ingestion admite actualmente, con la excepción de S3, utilizan una arquitectura basada en push. Esto significa que la aplicación de origen envía los datos a la canalización, en lugar de que la canalización extraiga los datos del origen.

Por lo tanto, debe conceder a las aplicaciones de origen los permisos necesarios para incorporar datos a una canalización de OpenSearch Ingestion. Como mínimo, el rol que firma la solicitud debe tener permiso para realizar la acción `osis:Ingest`, lo que le permitirá enviar datos a una canalización. Se requieren los mismos permisos para los puntos de conexión de canalizaciones públicas y de VPC.

El siguiente ejemplo de política permite a la entidad principal asociada incorporar datos en una canalización única llamada `my-pipeline`:

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

```
      "Sid": "PermitsWriteAccessToPipeline",
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-west-2:{your-account-id}:pipeline/my-pipeline"
    }
  ]
}
```

Para obtener más información, consulte the section called “Trabajo con integraciones en canalización”.

Incorporación entre cuentas

Es posible que tenga que incorporar datos a una canalización desde una Cuenta de AWS diferente, como una cuenta de aplicación. Para configurar la incorporación entre cuentas, defina un rol de incorporaco+pm dentro de la misma cuenta que la canalización y establezca una relación de confianza entre el rol de ingesta y la cuenta de la aplicación:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

A continuación, configure la aplicación para que asuma el rol de incorporación. La cuenta de la aplicación debe conceder al rol de aplicación permisos AssumeRole para el rol de incorporación en la cuenta de canalización.

Para ver ejemplos de pasos detallados y ejemplos de políticas de IAM, consulte the section called “Provisión de acceso de ingesta entre cuentas”.

Otorgar a Amazon OpenSearch Ingestion pipelines acceso a los dominios

Una canalización OpenSearch de Amazon Ingestion necesita permiso para escribir en el dominio de OpenSearch servicio que está configurado como receptor. Para proporcionar acceso, debe configurar un rol AWS Identity and Access Management (IAM) con una política de permisos

restrictiva que limite el acceso al dominio al que una canalización envía datos. Por ejemplo, es posible que desee limitar una canalización de incorporación únicamente al dominio y los índices necesarios para respaldar su caso de uso.

Antes de especificar el rol en la configuración de la canalización, debe configurarlo con una relación de confianza adecuada y, a continuación, concederle acceso al dominio dentro de la política de acceso al dominio.

Temas

Paso 1: crear un rol de canalización

El rol que especifique en el parámetro sts_role_arn de una configuración de canalización debe tener una política de permisos adjunta que le permita enviar datos al receptor del dominio. También debe tener una relación de confianza que permita a OpenSearch Ingestion asumir el rol. Para ver instrucciones sobre cómo adjuntar una política a un rol, consulte Adición de permisos de identidad de IAM en la Guía del usuario de IAM.

En el siguiente ejemplo de política se muestra el privilegio mínimo que se puede proporcionar en el rol sts_role_arn de configuración de una canalización para escribir en un solo dominio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/*"
        },
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:*:{your-account-id}:domain/{domain-namedomain}/*"
        }
```

```
    ]
}
```

Si piensa reutilizar el rol para escribir en varios dominios, puede ampliar la política sustituyendo el nombre de dominio por un carácter comodín (*).

El rol debe tener la siguiente relación de confianza, que permita a OpenSearch Ingestion asumir el rol de canalización:

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

Además, le recomendamos que agregue las claves de condición `aws:SourceAccount` y `aws:SourceArn` a la política para protegerse contra el problema del suplente confuso. La cuenta de origen es la propietaria de la canalización.

Por ejemplo, podría agregar el siguiente bloque de condición a la política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "{your-account-id}"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:{region}:{your-account-id}:pipeline/*"
    }
}
```

Paso 2: incluir la función de canalización en la política de acceso al dominio

Para que una canalización escriba datos en un dominio, el dominio debe tener una política de acceso a nivel de dominio que permita al rol de canalización sts_role_arn acceder a ellos.

El siguiente ejemplo de política de acceso al dominio permite que el rol de canalización denominado `pipeline-role`, que creó en el paso anterior, escriba datos en el dominio denominado `ingestion-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
      },
      "Action": ["es:DescribeDomain", "es:ESHttp*"],
      "Resource": "arn:aws:es:{region}:{your-account-id}:domain/{domain-name}/*"
    }
  ]
}
```

Paso 3: asignar el rol de canalización (solo para dominios que utilicen un control de acceso detallado)

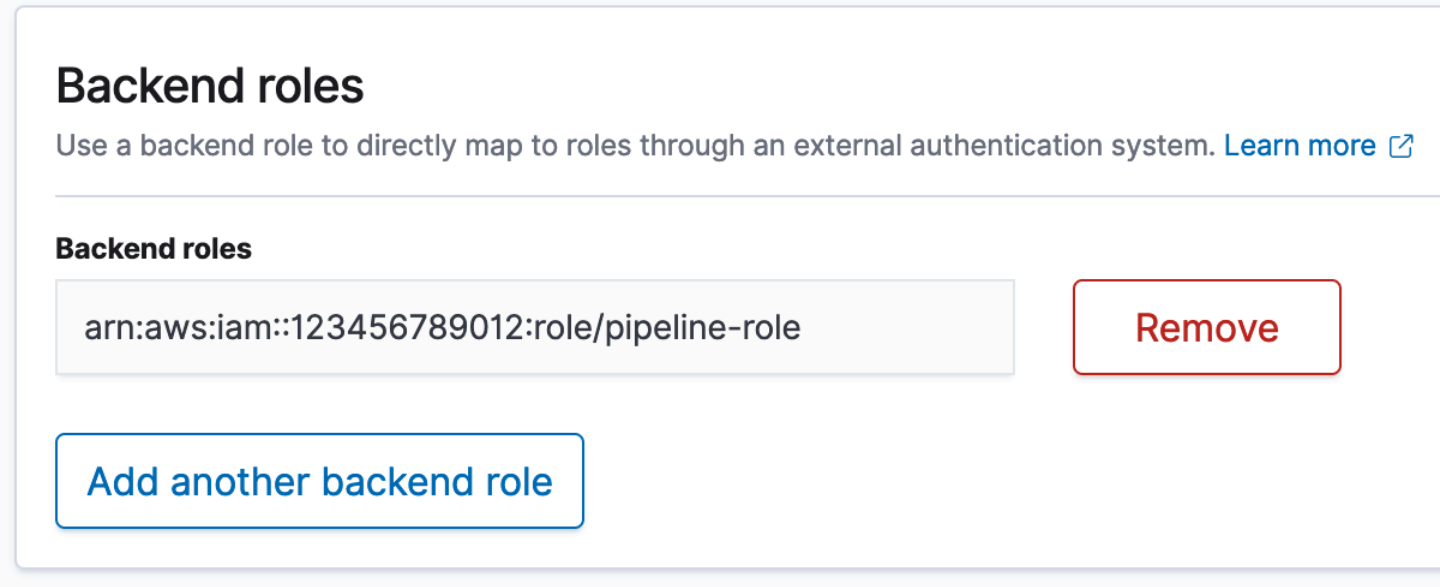
Si su dominio utiliza un control de acceso detallado para la autenticación, debe seguir algunos pasos adicionales para proporcionar a su canalización acceso a un dominio. Los pasos varían en función de la configuración del dominio:

Escenario 1: función de maestro y función de canalización diferentes: si utiliza un nombre de recurso de Amazon (ARN) de IAM como usuario maestro y es diferente de la función de canalización `sts_role_arn` (), debe asignar la función de canalización a la función de backend OpenSearch`all_access`. Básicamente, esto añade el rol de canalización como usuario maestro adicional. Para obtener más información, consulte Usuarios maestros adicionales.

Escenario 2: Usuario maestro en la base de datos de usuarios interna: si tu dominio usa un usuario maestro en la base de datos de usuarios interna y la autenticación básica HTTP para los OpenSearch paneles, no puedes pasar el nombre de usuario y la contraseña maestros directamente a la configuración de la canalización. En su lugar, debes asignar la función de canalización (`sts_role_arn`) a la función de OpenSearch `all_access` backend. Básicamente, esto añade el rol de canalización como usuario maestro adicional. Para obtener más información, consulte Usuarios maestros adicionales.

Escenario 3: el mismo rol de maestro y rol de canalización (poco común): si utiliza un ARN de IAM como usuario maestro y es el mismo ARN que utiliza como rol de canalización (`sts_role_arn`), no necesita realizar ninguna otra acción. La canalización tiene los permisos necesarios para escribir en el dominio. Este escenario es poco común porque la mayoría de los entornos utilizan un rol de administrador o algún otro rol como rol de maestro.

La siguiente imagen muestra cómo asignar el rol de canalización a un rol de backend:



Paso 4: especificar el rol en la configuración de la canalización

Para crear una canalización correctamente, debe especificar el rol de canalización que creó en el paso 1 como parámetro sts_role_arn en la configuración de la canalización. La canalización asume esta función para firmar las solicitudes al receptor del dominio OpenSearch de servicio.

En el campo `sts_role_arn`, especifique el ARN del rol de canalización de IAM:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG}" ]
  sink:
    - opensearch:
```

```
        hosts: [ "https://search-{domain-name}.us-east-1.es.amazonaws.com" ]
        index: "my-index"
        aws:
          region: "[region}"
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
```

Para ver una referencia completa de los parámetros obligatorios y no admitidos, consulte the section called “Complementos y opciones compatibles”.

Otorgar a Amazon OpenSearch Ingestion pipelines acceso a las colecciones

Una canalización OpenSearch de Amazon Ingestion necesita permiso para escribir en la colección OpenSearch Serverless que está configurada como sumidero. Para proporcionar acceso, debe configurar un rol AWS Identity and Access Management (IAM) con una política de permisos restrictiva que limite el acceso a la colección a la que una canalización envía datos. OpenSearch La ingestión puede incorporar datos tanto a una colección pública como a una colección de VPC.

Antes de especificar el rol en la configuración de la canalización, debe configurarlo con una relación de confianza adecuada y, a continuación, concederle permisos de acceso a los datos de los índices de colección.

Temas

Limitaciones

Las siguientes limitaciones se aplican a las canalizaciones que escriben en colecciones sin servidor: OpenSearch

- El procesador de grupos de trazas Otel no funciona actualmente con los sumideros de recopilación OpenSearch Serverless.
- Actualmente, OpenSearch Ingestion solo admite la operación antigua, mientras que OpenSearch Serverless admite la `_template` operación componible. `_index_template` Por lo tanto,

si la configuración de canalización incluye la opción `index_type`, debe configurarla en `management_disabled`.

Paso 1: crear un rol de canalización

El rol que especifique en el parámetro sts_role_arn de una configuración de canalización debe tener una política de permisos adjunta que le permita enviar datos al receptor de recopilación. También debe tener una relación de confianza que permita a OpenSearch Ingestion asumir el rol. Para ver instrucciones sobre cómo adjuntar una política a un rol, consulte Adición de permisos de identidad de IAM en la Guía del usuario de IAM.

En el siguiente ejemplo de política se muestra el privilegio mínimo que se puede proporcionar en el rol sts_role_arn de configuración de una canalización para escribir en las colecciones:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:aoss:{region}:{your-account-
id}:collection/{collection-id}"
        },
        {
            "Action": [
                "aoss:CreateSecurityPolicy",
                "aoss:GetSecurityPolicy",
                "aoss:UpdateSecurityPolicy",
                "aoss:APIAccessAll"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "{collection-name}"
                }
            }
        }
    ]
}
```

El rol debe tener la siguiente relación de confianza, que permita a OpenSearch Ingestion asumirlo:

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

Además, le recomendamos que agregue las claves de condición `aws:SourceAccount` y `aws:SourceArn` a la política para protegerse contra el problema del suplente confuso. La cuenta de origen es la propietaria de la canalización.

Por ejemplo, podría agregar el siguiente bloque de condición a la política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "{your-account-id}"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:osis:{region}:{your-account-id}:pipeline/*"
    }
}
```

Paso 2: crear una colección

Cree una colección OpenSearch sin servidor con la siguiente configuración:

- La siguiente política de acceso a los datos, que concede los permisos necesarios para el rol de canalización:

```
[
  {
    "Rules": [
```

```
      {
        "Resource": [
          "index/{collection-name}/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:WriteDocument",
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::{account-id}:role/{pipeline-role}"
    ],
    "Description": "Pipeline role access"
  }
]
```

> **Note**
>
> En el elemento `Principal`, especifique el nombre de recurso de Amazon (ARN) del rol de canalización que creó en el paso anterior.

- Una política de acceso a la red. Puede ingerir datos en una colección pública o en una colección de VPC. Si usa una colección de VPC, la política de red debe permitir que uno o más puntos de enlace de VPC accedan a la colección. Por ejemplo, puedes añadir la siguiente política de red, que permite que un punto final de VPC acceda a la colección:

```
[
   {
      "Description":"VPC access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/{collection-name}"
            ]
         }
      ],
      "AllowFromPublic": false,
```

```
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   }
]
```

> **Note**
>
> Además, debes especificar el nombre de la política de red en la `network_policy_name` opción de la configuración de la canalización. Consulte el paso 3 para ver un ejemplo de configuración de canalización.

Para obtener instrucciones sobre cómo crear una colección, consultethe section called “Creación de colecciones”.

Paso 3: crear una canalización

Por último, cree una canalización en la que especifique la función de la canalización y los detalles de la colección. La canalización asume esta función para firmar las solicitudes que se envían al receptor de recopilación OpenSearch Serverless.

Asegúrese de hacer lo siguiente:

- Para la opción de `hosts`, especifique el punto de conexión de la colección que creó en el paso 2.
- Para la opción de `sts_role_arn`, especifique el nombre de recurso de Amazon (ARN) del rol de canalización que creó en el paso 1.
- Establezca la opción de `serverless` en `true`.
- Defina la `network_policy_name` opción con el nombre de la política de red adjunta a la colección.

```
version: "2"
log-pipeline:
  source:
    http:
        path: "/log/ingest"
  processor:
    - date:
        from_time_received: true
```

```
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://{collection-id}.{region}.aoss.amazonaws.com" ]
        index: "my-index"
        aws:
          serverless: true
          serverless_options:
            network_policy_name: "{network-policy-name}" # If the policy doesn't exist,
a new policy is created.
          region: "us-east-1"
          sts_role_arn: "arn:aws:iam::{account-id}:role/{pipeline-role}"
```

Para ver una referencia completa de los parámetros obligatorios y no admitidos, consulte the section called “Complementos y opciones compatibles”.

Introducción a Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion admite la ingesta de datos en dominios gestionados de OpenSearch Service y en colecciones OpenSearch sin servidor. Los tutoriales siguientes muestran los pasos básicos para poner en marcha una canalización para cada uno de estos casos de uso.

> **Note**
>
> La creación de canalizaciones fallará si no configura los permisos correctos. Consulte the section called “Configuración de roles y usuarios” para comprender mejor las funciones necesarias antes de crear una canalización.

Temas

Tutorial: incorporar datos a un dominio mediante Amazon OpenSearch Ingestion

En este tutorial se muestra cómo utilizar Amazon OpenSearch Ingestion para configurar una canalización sencilla e incorporar datos en un dominio de Amazon OpenSearch Service. Una

canalización es un recurso que OpenSearch Ingestion aprovisiona y administra. Puede usar una canalización para filtrar, enriquecer, transformar, normalizar y agregar datos para el análisis y la visualización posteriores en OpenSearch Service.

Este tutorial recorre los pasos básicos para poner en marcha una canalización de forma rápida. Para obtener información más detallada, consulte the section called “Creación de canalizaciones”.

En este tutorial, deberá completar los siguientes pasos:

1. Crear el rol de canalización.
2. Crear un dominio.
3. Crear una canalización.
4. Incorporar algunos datos de muestra.

Dentro de este tutorial, creará los recursos siguientes:

- Una canalización llamada `ingestion-pipeline`
- Un nombre de dominio denominado `ingestion-domain` en el que escribirá la canalización
- Un rol de IAM llamado `PipelineRole` que asumirá la canalización para escribir en el dominio

Permisos necesarios

Para completar este tutorial, debe tener los permisos de IAM correctos. Su usuario o rol debe tener adjunta una política basada en la identidad con los siguientes permisos mínimos. Estos permisos le permiten crear un rol de canalización (`iam:Create`), crear o modificar un dominio (`es:*`) y trabajar con canalizaciones (`osis:*`).

Además, el permiso `iam:PassRole` es obligatorio para el recurso del rol de canalización. Este permiso le permite transferir la función de canalización a OpenSearch Ingestion para que pueda escribir datos en el dominio.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
```

```
            "osis:*",
            "iam:Create*",
            "es:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Paso 1: crear el rol de canalización

En primer lugar, cree un rol que asuma la canalización para acceder al receptor de dominio de OpenSearch Service. Incluirá esta función en la configuración de la canalización más adelante en este tutorial.

Para crear el rol de canalización

1. Abra la consola de AWS Identity and Access Management en https://console.aws.amazon.com/iamv2/.
2. Elija Políticas y después, Crear política.
3. En este tutorial, incorporará datos a un dominio llamado `ingestion-domain`, que creará en el siguiente paso. Seleccione JSON y pegue la siguiente política en el editor. Sustituya `{your-account-id}` por su Identificador de cuenta y modifique la región si es necesario.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "es:DescribeDomain",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "es:ESHttp*",
            "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-
domain/*"
        }
    ]
}
```

Si desea escribir datos en un dominio existente, sustituya `ingestion-domain` por el nombre de su dominio.

> **Note**
>
> Para simplificar este tutorial, utilizaremos una política de acceso amplia. No obstante, en entornos de producción, se recomienda que se aplique una política de acceso más restrictiva a su rol de canalización. Para ver un ejemplo de política que proporciona los permisos mínimos necesarios, consulte the section called “Otorgar a Pipelines acceso a los dominios”.

4. Elija Siguiente, elija Siguiente y asigne a su política el nombre pipeline-policy.
5. Elija Crear política.
6. A continuación, cree un rol y añádale la política. Elija Roles y después Crear rol.
7. En Política de confianza personalizada y pegue la siguiente política en el editor:

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

8. Elija Siguiente. Luego busque y seleccione pipeline-policy (que acaba de crear).
9. Seleccione Siguiente y asigne al rol el nombre PipelineRole.

10. Elija Crear rol.

Recuerde el nombre de recurso de Amazon (ARN) del rol (por ejemplo, `arn:aws:iam::{your-account-id}:role/PipelineRole`). Lo necesitará cuando cree la canalización.

Paso 2: crear un dominio

A continuación, cree un dominio denominado `ingestion-domain` al que desee incorporar datos.

Vaya a la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home y cree un dominio que cumpla los siguientes requisitos:

- Funciona en OpenSearch 1.0 o superior, o Elasticsearch 7.4 o superior
- Utiliza el acceso público
- No utiliza el control de acceso detallado

> **Note**
>
> Estos requisitos están pensados para garantizar la simplicidad de este tutorial. En los entornos de producción, puede configurar un dominio con acceso a VPC o utilizar un control de acceso detallado. Para obtener instrucciones, consulte el resto de temas de este capítulo.

El dominio debe tener una política de acceso que otorgue permiso a `PipelineRole`, el cual creó en el paso anterior. La canalización asumirá este rol (denominada sts_role_arn en la configuración de la canalización) para enviar datos al receptor de dominios de OpenSearch Service.

Asegúrese de que el dominio tenga la siguiente política de acceso a nivel de dominio, que permite el acceso al dominio `PipelineRole`. Sustituya la Región y el ID de cuenta por los suyos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::{your-account-id}:role/PipelineRole"
      },
      "Action": "es:*",
```

```
      "Resource": "arn:aws:es:us-east-1:{your-account-id}:domain/ingestion-domain/*"
    }
  ]
}
```

Para obtener más información sobre la creación de políticas de acceso a nivel de dominio, consulte Políticas de acceso basadas en recursos.

Si ya ha creado un dominio, modifique su política de acceso actual para proporcionar los permisos anteriores a `PipelineRole`.

> **Note**
>
> Recuerde el punto de conexión del dominio (por ejemplo, `https://search-ingestion-domain.us-east-1.es.amazonaws.com`). Lo utilizará en el siguiente paso para configurar la canalización.

Paso 3: crear una canalización

Ahora que tiene un dominio y un rol con los derechos de acceso adecuados, puede crear una canalización.

Para crear una canalización

1. En la consola de Amazon OpenSearch Service, elija Canalizaciones en el panel de navegación izquierdo.
2. Elija Create pipeline.
3. Asigne el nombre ingestion-pipeline a la canalización y mantenga la configuración de capacidad como predeterminada.
4. En este tutorial, crearemos una subcanalización sencilla llamada `log-pipeline` que utilice el complemento fuente Http. Este complemento acepta datos de registro en un formato de matriz JSON. Especificará un único dominio de OpenSearch sin servidor como el receptor e incorporará todos los datos al índice `application_logs`.

   En Configuración de canalización, pegue la siguiente configuración de YAML en el editor:

   ```
   version: "2"
   log-pipeline:
   ```

```
source:
  http:
    path: "/${pipelineName}/test_ingestion_path"
processor:
  - date:
      from_time_received: true
      destination: "@timestamp"
sink:
  - opensearch:
      hosts: [ "https://search-ingestion-domain.us-east-1.es.amazonaws.com" ]
      index: "application_logs"
      aws:
        sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
        region: "us-east-1"
```

> **Note**
>
> La opción `path` especifica la ruta del URI para la incorporación. Esta opción es necesaria para las fuentes basadas en la extracción. Para obtener más información, consulte the section called “Especificación de la ruta de ingesta”.

5. Reemplace la URL `hosts` por el punto de conexión del dominio que creó (o modificó) en la sección anterior. Sustituya el parámetro `sts_role_arn` por el ARN de `PipelineRole`.
6. Elija Validar canalización y asegúrese de que la validación se realice correctamente.
7. Para simplificar este tutorial, configure el acceso público para la canalización. En Red, elija Acceso público.

   Para obtener información acerca de la configuración del acceso a VPC, consulte the section called “Protección de canalizaciones dentro de una VPC”.
8. Mantenga habilitada la publicación de registros en caso de que surja algún problema al completar este tutorial. Para obtener más información, consulte the section called “Monitorear registros de canalización”.

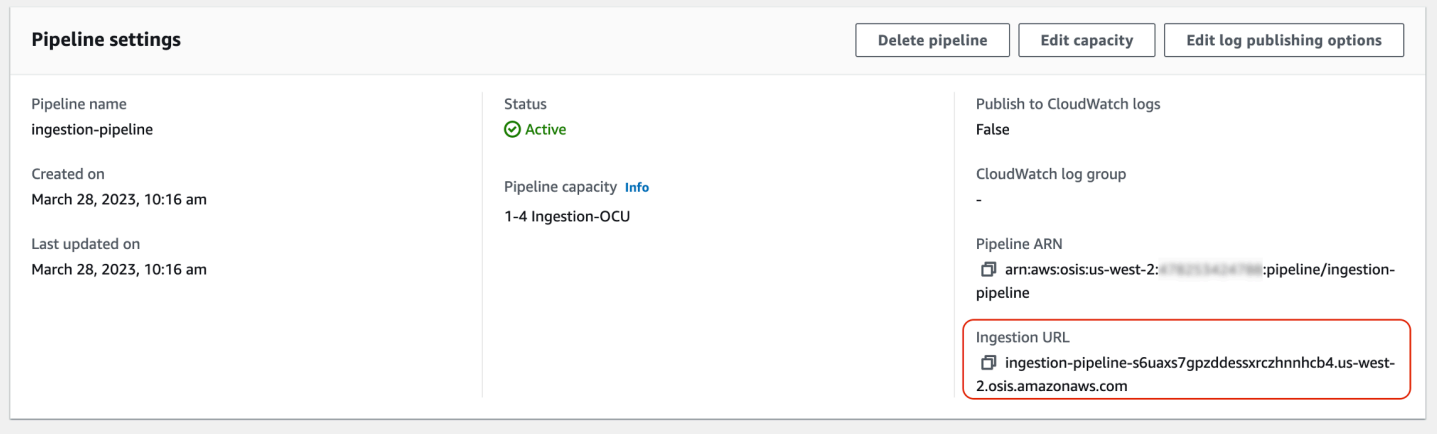
   Especifique el siguiente nombre de grupo de registros: `/aws/vendedlogs/OpenSearchIngestion/ingestion-pipeline/audit-logs`
9. Elija Siguiente. Revise la configuración de la canalización y elija Crear canalización. La canalización tarda entre 5 y 10 minutos en activarse.

Paso 4: incorporar algunos datos de muestra

Cuando el estado de la canalización sea `Active`, puede empezar a incorporarle datos. Debe firmar todas las solicitudes HTTP que se envíen a la canalización mediante la versión 4 de Signature. Use una herramienta HTTP como Postman o awscurl para enviar algunos datos a la canalización. Al igual que ocurre con la indexación de datos directamente en un dominio, la incorporación de datos a una canalización siempre requiere un rol de IAM o una clave de acceso y una clave secreta de IAM.

> **Note**
>
> La entidad principal que firma la solicitud debe tener el permiso de IAM `osis:Ingest`.

Primero, obtenga la URL de incorporación en la página de Configuración de canalización:



Luego, incorpore algunos datos de muestra. La siguiente solicitud de ejemplo usa awscurl para enviar un único archivo de registro al índice `application_logs`:

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Debería ver una respuesta `200 OK`. Si recibe un error de autenticación, es posible que se deba a que está incorporando datos de una cuenta distinta a la de la canalización. Consulte the section called “Solucionar problemas de permisos”.

Ahora, consulte el índice `application_logs` para asegurarse de que la entrada de registro se haya incorporado correctamente:

```
awscurl --service es --region us-east-1 \
     -X GET \
     https://search-{ingestion-domain}.us-east-1.es.amazonaws.com/application_logs/
_search | json_pp
```

Respuesta de ejemplo:

```
{
   "took":984,
   "timed_out":false,
   "_shards":{
      "total":1,
      "successful":5,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"application_logs",
            "_type":"_doc",
            "_id":"z6VY_IMBRpceX-DU6V4O",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2022-10-21T21:00:25.502Z"
            }
```

```
            }
        ]
    }
}
```

Solucionar problemas de permisos

Si ha seguido los pasos del tutorial y sigue viendo errores de autenticación cuando intenta incorporar datos, puede que se deba a que la función que escribe en una canalización Cuenta de AWS no es la canalización misma. En este caso, debe crear y asumir un rol que le permita específicamente incorporar datos. Para obtener instrucciones, consulte the section called “Provisión de acceso de ingesta entre cuentas”.

Recursos relacionados

Este tutorial presenta un caso práctico sencillo de incorporación de un único documento a través de HTTP. En escenarios de producción, configurará las aplicaciones de cliente (como Fluent Bit, Kubernetes u OpenTelemetry Collector) para enviar datos a una o más canalizaciones. Es probable que sus canalizaciones sean más complejas que en el ejemplo sencillo de este tutorial.

Para empezar a configurar sus clientes e incorporar datos, consulte los siguientes recursos:

- Creación y administración de canalizaciones
- Configuración de clientes para enviar datos a OpenSearch Ingestion
- Documentación de Data Prepper

Tutorial: Ingerir datos en una colección mediante Amazon OpenSearch Ingestion

En este tutorial, se muestra cómo utilizar Amazon OpenSearch Ingestion para configurar una canalización sencilla e ingerir datos en una colección de Amazon OpenSearch Serverless. Una canalización es un recurso que OpenSearch Ingestion aprovisiona y administra. Puede usar una canalización para filtrar, enriquecer, transformar, normalizar y agregar datos para el análisis y la visualización posteriores en OpenSearch Service.

Para ver un tutorial que muestra cómo incorporar datos en un dominio de OpenSearch servicio aprovisionado, consulte. the section called “Tutorial: incorporar datos a un dominio”

En este tutorial, deberá completar los siguientes pasos:

1. Crear la canalización.
2. Crear una colección.
3. Crear una canalización.
4. Incorporar algunos datos de muestra.

Dentro de este tutorial, creará los recursos siguientes:

- Una canalización llamada `ingestion-pipeline-serverless`
- Una colección llamada `ingestion-collection` donde escribirá la canalización
- Un rol de IAM llamado `PipelineRole` que asumirá la canalización para escribir en la colección

Permisos necesarios

Para completar este tutorial, debe tener los permisos de IAM correctos. Su usuario o rol debe tener adjunta una política basada en la identidad con los siguientes permisos mínimos. Estos permisos le permiten crear un rol de canalización (`iam:Create*`), crear o modificar una colección (`aoss:*`) y trabajar con canalizaciones (`osis:*`).

Además, el permiso `iam:PassRole` es obligatorio para el recurso del rol de canalización. Este permiso le permite transferir la función de canalización a OpenSearch Ingestion para que pueda escribir datos en la colección.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:*",
            "iam:Create*",
            "aoss:*"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/PipelineRole"
         ],
```

```
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

Paso 1: crear el rol de canalización

En primer lugar, cree una función que asuma la canalización para acceder al receptor de recopilación OpenSearch Serverless. Incluirá esta función en la configuración de la canalización más adelante en este tutorial.

Para crear el rol de canalización

1. Abre la AWS Identity and Access Management consola en https://console.aws.amazon.com/iamv2/.
2. Elija Políticas y después, Crear política.
3. Seleccione JSON y pegue la siguiente política en el editor.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:BatchGetCollection",
        "aoss:APIAccessAll"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:aoss:{region}:{your-account-id}:collection/{collection-
id}"
    },
    {
      "Action": [
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy"
      ],
      "Effect": "Allow",
      "Resource": "*",
      "Condition": {
```

```
        "StringEquals": {
          "aoss:collection": "{collection-name}"
        }
      }
    }
  ]
}
```

4. Seleccione Siguiente, elija Siguiente y asigne un nombre a su póliza collection-pipeline-policy.
5. Elija Crear política.
6. A continuación, cree un rol y añádale la política. Elija Roles y después Crear rol.
7. En Política de confianza personalizada y pegue la siguiente política en el editor:

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

8. Elija Siguiente. Luego busca y selecciona collection-pipeline-policy(la que acabas de crear).
9. Seleccione Siguiente y asigne un nombre al rol PipelineRole.
10. Elija Crear rol.

Recuerde el nombre de recurso de Amazon (ARN) del rol (por ejemplo, `arn:aws:iam::{your-account-id}:role/PipelineRole`). Lo necesitará para crear la canalización.

Paso 2: crear una colección

A continuación, cree una colección para incorporar datos. El nombre que le pondremos a la colección será `ingestion-collection`.

1. Dirígete a la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.

2. Seleccione Colecciones del panel de navegación de la izquierda y elija Crear colección.
3. Nombra la colección ingestion-collection.
4. En Configuración de acceso a la red, cambie el tipo de acceso a Público.
5. Mantenga todas las demás configuraciones en sus valores predeterminados y elija Siguiente.
6. Seleccione JSON para el Método de definición y pegue la siguiente política en el editor. Esta política realiza dos tareas:

   - Permite que el rol de canalización escriba en la colección.
   - Le permite leer de la colección. Más adelante, después de incorporar algunos datos de muestra a la canalización, consultará la colección para garantizar que los datos se hayan incorporado y escrito correctamente en el índice.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/ingestion-collection/*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:UpdateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument",
          "aoss:WriteDocument"
        ],
        "ResourceType": "index"
      }
    ],
    "Principal": [
      "arn:aws:iam::{your-account-id}:role/PipelineRole",
      "arn:aws:iam::{your-account-id}:role/Admin"
    ],
    "Description": "Rule 1"
  }
]
```

7. Sustituya los elementos `Principal`. La primera entidad principal debe especificar el rol de canalización que ha creado. El segundo debe especificar un usuario o rol que pueda usar para consultar la colección más adelante.

8. Elija Siguiente. Asigne un nombre a la política de acceso pipeline-domain-accessy vuelva a seleccionar Siguiente.
9. Revise la configuración de la colección y seleccione Enviar.

Cuando la colección esté activa, anote el OpenSearch punto final en Punto final (por ejemplo,`https://{collection-id}.us-east-1.aoss.amazonaws.com`). Lo necesitará cuando cree la canalización.

Paso 3: crear una canalización

Ahora que tiene una colección y un rol con los derechos de acceso adecuados, puede crear una canalización.

Para crear una canalización

1. En la consola de Amazon OpenSearch Service, selecciona Pipelines en el panel de navegación izquierdo.
2. Elija Crear canalización.
3. Asigne el nombre serverless-ingestion a la canalización y mantenga la configuración de capacidad como predeterminada.
4. En este tutorial, crearemos una subcanalización sencilla llamada `log-pipeline` que utilice el complemento fuente HTTP. El complemento acepta datos de registro en un formato de matriz JSON. Especificaremos una única colección OpenSearch sin servidor como sumidero e incorporaremos todos los datos al índice. `my_logs`

   En Configuración de canalización, pegue la siguiente configuración de YAML en el editor:

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/test_ingestion_path"
  processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://{collection-id}.us-east-1.aoss.amazonaws.com" ]
```

```
        index: "my_logs"
        aws:
          sts_role_arn: "arn:aws:iam::{your-account-id}:role/PipelineRole"
          region: "us-east-1"
          serverless: true
```

5. Reemplace la URL `hosts` por el punto de conexión de la colección que creó en la sección anterior. Sustituya el parámetro `sts_role_arn` por el ARN de `PipelineRole`. Si lo desea, modifique el `region`.
6. Elija Validar canalización y asegúrese de que la validación se realice correctamente.
7. Para simplificar este tutorial, configuraremos el acceso público para la canalización. En Red, elija Acceso público.

   Para obtener información acerca de la configuración del acceso a VPC, consulte the section called “Protección de canalizaciones dentro de una VPC”.
8. Mantenga habilitada la publicación de registros en caso de que surja algún problema al completar este tutorial. Para obtener más información, consulte the section called “Monitorear registros de canalización”.

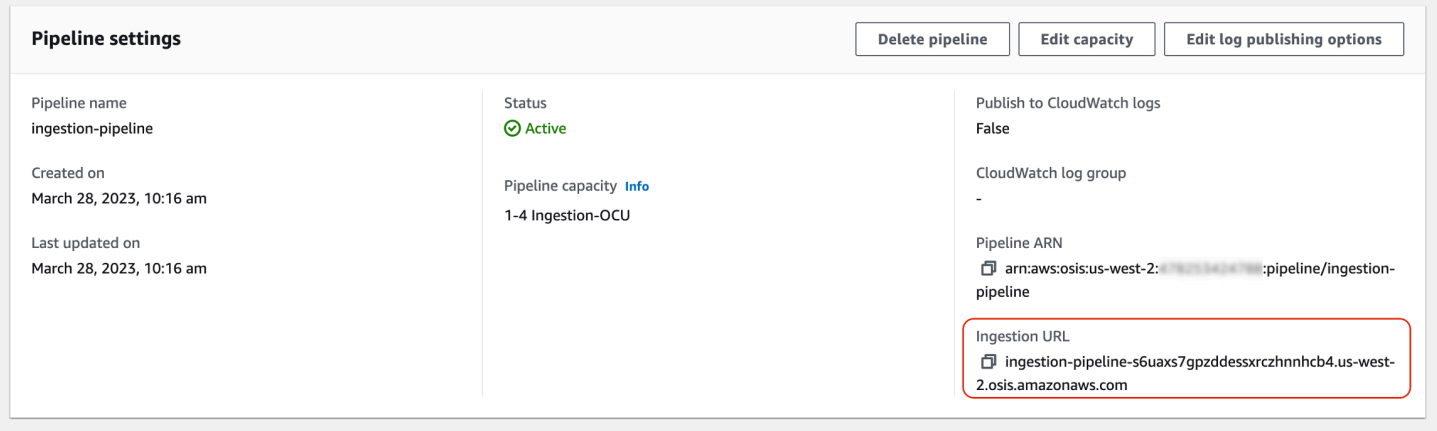
   Especifique el siguiente nombre de grupo de registros: `/aws/vendedlogs/OpenSearchIngestion/serverless-ingestion/audit-logs`
9. Elija Siguiente. Revise la configuración de la canalización y elija Crear canalización. La canalización tarda entre 5 y 10 minutos en activarse.

Paso 4: incorporar algunos datos de muestra

Cuando el estado de la canalización sea `Active`, puede empezar a incorporarle datos. Debe firmar todas las solicitudes HTTP que se envíen a la canalización mediante la versión 4 de Signature. Use una herramienta HTTP como Postman o awscurl para enviar algunos datos a la canalización. Al igual que ocurre con la indexación de datos directamente en una colección, la incorporación de datos a una canalización siempre requiere un rol de IAM o una clave de acceso y una clave secreta de IAM.

> **Note**
>
> La entidad principal que firma la solicitud debe tener el permiso de IAM `osis:Ingest`.

Primero, obtenga la URL de incorporación en la página de Configuración de canalización:



Luego, incorpore algunos datos de muestra. La siguiente solicitud de ejemplo usa awscurl para enviar un único archivo de registro al índice `my_logs`:

```
awscurl --service osis --region us-east-1 \
    -X POST \
    -H "Content-Type: application/json" \
    -d
 '[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","request":
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]' \
    https://{pipeline-endpoint}.us-east-1.osis.amazonaws.com/log-pipeline/
test_ingestion_path
```

Debería ver una respuesta `200 OK`.

Ahora, consulte el índice `my_logs` para asegurarse de que la entrada del registro se haya incorporado correctamente:

```
awscurl --service aoss --region us-east-1 \
     -X GET \
     https://{collection-id}.us-east-1.aoss.amazonaws.com/my_logs/_search | json_pp
```

Respuesta de ejemplo:

```
{
   "took":348,
   "timed_out":false,
   "_shards":{
      "total":0,
```

```
      "successful":0,
      "skipped":0,
      "failed":0
   },
   "hits":{
      "total":{
         "value":1,
         "relation":"eq"
      },
      "max_score":1.0,
      "hits":[
         {
            "_index":"my_logs",
            "_id":"1%3A0%3ARJgDvIcBTy5m12xrKE-y",
            "_score":1.0,
            "_source":{
               "time":"2014-08-11T11:40:13+00:00",
               "remote_addr":"122.226.223.69",
               "status":"404",
               "request":"GET http://www.k2proxy.com//hello.html HTTP/1.1",
               "http_user_agent":"Mozilla/4.0 (compatible; WOW64; SLCC2;)",
               "@timestamp":"2023-04-26T05:22:16.204Z"
            }
         }
      ]
   }
}
```


Recursos relacionados

Este tutorial presenta un caso práctico sencillo de incorporación de un único documento a través de HTTP. En los escenarios de producción, configurará las aplicaciones cliente (como Fluent Bit, Kubernetes o The OpenTelemetry Collector) para que envíen datos a una o más canalizaciones. Es probable que sus canalizaciones sean más complejas que en el ejemplo sencillo de este tutorial.

Para empezar a configurar sus clientes e incorporar datos, consulte los siguientes recursos:

- Creación y administración de canalizaciones
- Configurar sus clientes para que envíen datos a Ingestion OpenSearch
- Documentación de Data Prepper

Descripción general de las funciones de canalización en Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion aprovisiona las canalizaciones, que constan de una fuente, un búfer, cero o más procesadores y uno o más receptores. Las canalizaciones de incorporación funcionan con Data Prepper como motor de datos. Para obtener información general sobre los distintos componentes de una canalización, consulte the section called “Conceptos clave”.

En las siguientes secciones se ofrece información general sobre algunas de las funciones más utilizadas en Amazon OpenSearch Ingestion.

> **Note**
>
> No es una lista exhaustiva de las características disponibles para las canalización. Para obtener una documentación completa de todas las funciones de canalización disponibles, consulte Documentación de Data Prepper. Tenga en cuenta que OpenSearch Ingestion impone algunas restricciones a los complementos y las opciones que puede utilizar. Para obtener más información, consulte the section called “Complementos y opciones compatibles”.

Temas

Almacenamiento en búfer persistente

Un búfer persistente almacena los datos en un búfer basado en disco en varias zonas de disponibilidad para añadir durabilidad a los datos. Puede utilizar el almacenamiento en búfer persistente para ingerir datos de todas las fuentes push compatibles sin necesidad de configurar un

búfer independiente. Estas incluyen el HTTP y OpenTelemetry las fuentes de registros, seguimientos y métricas.

Para habilitar el almacenamiento en búfer persistente, selecciona Habilitar el búfer persistente al crear o actualizar una canalización. Para obtener más información, consulte. the section called "Creación de canalizaciones" OpenSearch La ingestión determina automáticamente la capacidad de almacenamiento en búfer requerida en función de las unidades de OpenSearch cómputo de ingestión (OCU de ingestión) que especifique para la canalización.

De forma predeterminada, las canalizaciones utilizan una para cifrar los datos del búfer. Clave propiedad de AWS Estas canalizaciones no necesitan ningún permiso adicional para desempeñar la función de canalización. Como alternativa, puedes especificar una clave gestionada por el cliente y añadir los siguientes permisos de IAM a la función de canalización:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "KeyAccess",
            "Effect": "Allow",
            "Action": [
              "kms:Decrypt",
              "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "arn:aws:kms:{region}:{aws-account-
id}:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

Para más información, consulte las claves administradas por el cliente en la Guía para desarrolladores de AWS Key Management Service .

> **Note**
>
> Si deshabilita el almacenamiento en búfer persistente, su canalización se actualizará para que se ejecute por completo con el almacenamiento en búfer en memoria.

Ajustar el tamaño máximo de la carga útil solicitada

Si habilitas el almacenamiento en búfer persistente para una canalización, tienes la opción de ajustar el tamaño máximo de la carga útil solicitada. Esta configuración limita el tamaño de los registros que se envían al receptor en una sola solicitud, lo que evita el envío de solicitudes enormes. Para ajustar el tamaño máximo de la carga útil, defina la `max_request_length` opción en la configuración de origen. Al igual que el almacenamiento en búfer persistente, esta opción solo es compatible con HTTP y OpenTelemetry las fuentes de registros, seguimientos y métricas.

Los únicos valores válidos para la `max_request_length` opción son 1 MB, 1,5 MB, 2 MB, 2,5 MB, 3 MB, 3,5 MB y 4 MB. Si especifica un valor diferente, recibirá un error.

El siguiente ejemplo muestra cómo configurar el tamaño máximo de carga útil dentro de una configuración de canalización:

```
...
log-pipeline:
  source:
    http:
      path: "/${pipelineName}/logs"
      max_request_length: "4mb"
  processor:
...
```

Si habilitas el almacenamiento en búfer persistente y no especificas la `max_request_length` opción, el valor predeterminado es 1 MB.

División

Puedes configurar una canalización de OpenSearch ingestión para dividir los eventos entrantes en una subcanalización, lo que te permitirá realizar diferentes tipos de procesamiento en el mismo evento entrante.

El siguiente ejemplo de canalización divide los eventos entrantes en dos subcanalizaciones. Cada subcanalización utiliza su propio procesador para enriquecer y manipular los datos y, a continuación, los envía a distintos índices. OpenSearch

```
version: "2"
log-pipeline:
```

```
  source:
    http:
    ...
  sink:
    - pipeline:
        name: "logs_enriched_one_pipeline"
    - pipeline:
        name: "logs_enriched_two_pipeline"

logs_enriched_one_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "enriched_one_logs"

logs_enriched_two_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_two_logs"
```

Encadenar

Puede encadenar varias subcanalizaciones para procesar y enriquecer los datos por partes. En otras palabras, puede enriquecer un evento entrante con determinadas capacidades de procesamiento en una subcanalización, luego enviarlo a otra subcanalización para enriquecerla aún más con un procesador diferente y, finalmente, enviarlo a su receptor. OpenSearch

En el siguiente ejemplo, la `log_pipeline` subcanalización enriquece un evento de registro entrante con un conjunto de procesadores y, a continuación, envía el evento a un índice denominado. OpenSearch `enriched_logs` La canalización envía el mismo evento a la `log_advanced_pipeline` subcanalización, que lo procesa y lo envía a un índice diferente OpenSearch denominado. `enriched_advanced_logs`

```
version: "2"
log-pipeline:
  source:
    http:
    ...
  processor:
    ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_logs"
    - pipeline:
        name: "log_advanced_pipeline"

log_advanced_pipeline:
  source:
    log-pipeline
  processor:
   ...
  sink:
    - opensearch:
        # Provide a domain or collection endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
          index: "enriched_advanced_logs"
```

Colas de mensajes fallidos

Las colas de mensajes fallidos (DLQ) son los destinos de los eventos que una canalización no logra registrar en un receptor. En OpenSearch Ingestion, debe especificar un bucket de Amazon S3 con

los permisos de escritura adecuados para usarlo como DLQ. Puede añadir una configuración de DLQ a cada receptor de una canalización. Cuando una canalización detecta errores de escritura, crea objetos de DLQ en el bucket de S3 configurado. Los objetos DLQ existen dentro de un archivo JSON como una matriz de eventos fallidos.

Una canalización escribe eventos en la DLQ cuando se cumple alguna de las siguientes condiciones:

- Los `max_retries` del OpenSearch fregadero están agotados. OpenSearch La ingestión requiere un mínimo de 16 para esta opción.
- El receptor rechaza los eventos debido a una condición de error.

Configuración

Para configurar una cola de mensajes fallidos para una subcanalización, especifique la opción `dlq` en la configuración del receptor `opensearch`:

```
apache-log-pipeline:
  ...
  sink:
    opensearch:
      dlq:
        s3:
          bucket: "my-dlq-bucket"
          key_path_prefix: "dlq-files"
          region: "us-west-2"
          sts_role_arn: "arn:aws:iam::123456789012:role/dlq-role"
```

Los archivos que se escriban en este DLQ de S3 tendrán el siguiente patrón de nomenclatura:

```
dlq-v${version}-${pipelineName}-${pluginId}-${timestampIso8601}-${uniqueId}
```

Para obtener más información, consulte Colas de mensajes fallidos (DLQ).

Para obtener las instrucciones de la configuración del rol `sts_role_arn`, consulte the section called “Escribir en una cola de mensajes fallidos”.

Ejemplo

Considere el siguiente ejemplo de archivo DLQ:

```
dlq-v2-apache-log-pipeline-opensearch-2023-04-05T15:26:19.152938Z-e7eb675a-
f558-4048-8566-dac15a4f8343
```

Este es un ejemplo de datos que no se pudieron escribir en el receptor y que se envían al bucket DLQ de S3 para su posterior análisis:

```
Record_0
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index    "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log      "sample log"
timestamp     "2023-04-14T10:36:01.070Z"

Record_1
pluginId            "opensearch"
pluginName          "opensearch"
pipelineName        "apache-log-pipeline"
failedData
index               "logs"
indexId   null
status    0
message  "Number of retries reached the limit of max retries (configured value 15)"
document
log                 "another sample log"
timestamp           "2023-04-14T10:36:01.071Z"
```

Administración de índices

Amazon OpenSearch Ingestion cuenta con numerosas funciones de administración de índices, entre las que se incluyen las siguientes.

Creación de índices

Puede especificar un nombre de índice en un colector de canalización e OpenSearch Ingestion crea el índice cuando aprovisiona la canalización. Si ya existe un índice, la canalización lo usa para

indexar los eventos entrantes. Si detiene y reinicia una canalización, o si actualiza su configuración de YAML, la canalización intentará crear nuevos índices si aún no existen. Una canalización nunca puede eliminar un índice.

En el siguiente ejemplo, los receptores crean dos índices cuando se aprovisiona la canalización:

```
sink:
  - opensearch:
      index: apache_logs
  - opensearch:
      index: nginx_logs
```

Creación de nombres y patrones de índice

Puede generar nombres de índice dinámicos mediante variables de los campos de los eventos entrantes. En la configuración del receptor, utilice el formato `string${}` para indicar la interpolación de cadenas y utilice un puntero JSON para extraer los campos de los eventos. Las opciones para `index_type` son `custom` o `management_disabled`. Como el `index_type` valor predeterminado es `custom` para los OpenSearch dominios y `management_disabled` para las colecciones OpenSearch sin servidor, se puede dejar sin configurar.

Por ejemplo, la siguiente canalización selecciona el campo `metadataType` entre los eventos entrantes para generar nombres de índice.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}"
```

La siguiente configuración sigue generando un índice nuevo cada día o cada hora.

```
pipeline:
  ...
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"

pipeline:
  ...
```

```
  sink:
    opensearch:
      index: "metadata-${metadataType}-%{yyyy.MM.dd.HH}"
```

El nombre del índice también puede ser una cadena simple con un patrón de fecha y hora como sufijo, por ejemplo `my-index-%{yyyy.MM.dd}`. Cuando el receptor envía datos a OpenSearch, reemplaza el patrón de fecha y hora por la hora UTC y crea un índice nuevo para cada día, por ejemplo. `my-index-2022.01.25` Para obtener más información, consulta la DateTimeFormatterclase.

Este nombre de índice también puede ser una cadena formateada (con o sin un sufijo de patrón de fecha y hora), como `my-${index}-name`. Cuando el receptor envía datos a OpenSearch, reemplaza la `"${index}"` parte por el valor en caso de que se esté procesando. Si el formato lo es `"${index1/index2/index3}"`, reemplaza el campo `index1/index2/index3` por su valor en el evento.

Creación de identificadores de documentos

Una canalización puede generar un identificador de documento mientras indexa los documentos en él. OpenSearch Puede deducir estos identificadores de documentos a partir de los campos incluidos en los eventos entrantes.

En este ejemplo, se utiliza el campo `uuid` de un evento entrante para generar un identificador de documento.

```
pipeline:
  ...
  sink:
    opensearch:
      index_type: custom
      index: "metadata-${metadataType}-%{yyyy.MM.dd}"
      document_id_field: "uuid"
```

En el ejemplo siguiente, el procesador Add entries combina los campos `uuid` y `other_field` del evento entrante para generar un identificador de documento.

La acción `create` garantiza que los documentos con identificadores idénticos no se sobrescriban. La canalización elimina los documentos duplicados sin ningún tipo de reintento ni ningún evento de DLQ. Esta es una expectativa razonable para los autores de canalización que utilizan esta acción, ya que el objetivo es evitar actualizar los documentos existentes.

```
pipeline:
  ...
  processor:
   - add_entries:
      entries:
        - key: "my_doc_id_field"
          format: "${uuid}-${other_field}"
  sink:
    - opensearch:
       ...
       action: "create"
       document_id_field: "my_doc_id_field"
```

Es posible que desee establecer el identificador del documento de un evento en un campo de un subobjeto. En el siguiente ejemplo, el complemento OpenSearch sink usa el subobjeto `info/id` para generar un ID de documento.

```
sink:
  - opensearch:
       ...
       document_id_field: info/id
```

Si se produce el siguiente evento, la canalización generará un documento con el campo `_id` establecido en `json001`:

```
{
   "fieldA":"arbitrary value",
   "info":{
      "id":"json001",
      "fieldA":"xyz",
      "fieldB":"def"
   }
}
```

Creación de identificadores de enrutamiento

Puedes usar la `routing_field` opción del complemento OpenSearch sink para establecer el valor de una propiedad de enrutamiento de documentos (`_routing`) en el valor de un evento entrante.

El enrutamiento admite la sintaxis de punteros JSON, por lo que también están disponibles campos anidados, no solo campos de nivel superior.

```
sink:
  - opensearch:
      ...
      routing_field: metadata/id
      document_id_field: id
```

Si se produce el siguiente evento, el complemento genera un documento con el campo `_routing` establecido en `abcd`:

```
{
   "id":"123",
   "metadata":{
      "id":"abcd",
      "fieldA":"valueA"
   },
   "fieldB":"valueB"
}
```

Para obtener instrucciones sobre cómo crear plantillas de índice que las canalizaciones puedan utilizar durante la creación del índice, consulte Plantillas de índice.

nd-to-end Reconocimiento electrónico

OpenSearch La ingestión garantiza la durabilidad y la fiabilidad de los datos al rastrear su entrega desde su origen hasta los sumideros de los oleoductos sin estado mediante el uso de acuse de recibo. end-to-end Actualmente, solo el complemento fuente de S3 admite el reconocimiento. end-to-end

Con el end-to-end acuse de recibo, el complemento Pipeline Source crea un conjunto de acuses de recibo para monitorear un lote de eventos. Recibe un reconocimiento positivo cuando esos eventos se envían correctamente a sus receptores, o un reconocimiento negativo cuando alguno de los eventos no se ha podido enviar a sus receptores.

En caso de fallo o caída de un componente de la canalización, o si un origen no recibe un reconocimiento, se agota el tiempo de espera y toma las medidas necesarias, como volver a intentarlo o registrar el fallo. Si la canalización tiene configurados varios receptores o subcanalizaciones, las confirmaciones a nivel de evento solo se envían después de que el evento se envíe a todos los receptores de todas las subcanalizaciones. Si un receptor tiene un DLQ configurado, los acuses de end-to-end recibo también rastrean los eventos escritos en el DLQ.

Para habilitar el end-to-end reconocimiento, incluya la `acknowledgments` opción en la configuración de origen:

```
s3-pipeline:
  source:
    s3:
      acknowledgments: true
...
```

Contrapresión de la fuente

Una canalización puede sufrir una contrapresión cuando está ocupada procesando datos o si sus sumideros están temporalmente inactivos o tardan en ingerir datos. OpenSearch La ingestión tiene diferentes formas de gestionar la contrapresión en función del complemento fuente que utilice la canalización.

Origen de HTTP

Las canalizaciones que utilizan el complemento origen de HTTP gestionan la contrapresión de forma diferente en función del componente de la canalización que esté congestionado:

- Búferes: cuando los búferes están llenos, la canalización comienza a devolver el estado HTTP `REQUEST_TIMEOUT` con el código de error 408 al punto de conexión de origen. A medida que se van liberando los búferes, la canalización vuelve a procesar los eventos HTTP.
- Subprocesos de origen: cuando todos los subprocesos de origen HTTP están ocupados ejecutando solicitudes y el tamaño de la cola de solicitudes sin procesar ha superado el número máximo de solicitudes permitido, la canalización comienza a devolver el estado HTTP `TOO_MANY_REQUESTS` con el código de error 429 al punto de conexión de origen. Cuando la cola de solicitudes cae por debajo del tamaño máximo permitido, la canalización vuelve a procesar las solicitudes.

Origen de OTel

Cuando los búferes están llenos para las canalizaciones que utilizan OpenTelemetry fuentes (registros de Otel, métricas de Otel y rastreo de Otel), la canalización comienza a devolver el estado HTTP `REQUEST_TIMEOUT` con el código de error 408 al punto final de origen. A medida que se van liberando los búferes, la canalización vuelve a procesar los eventos.

Fuente de S3

Cuando los búferes están llenos para las canalizaciones con un origen de S3, las canalizaciones dejan de procesar las notificaciones de SQS. A medida que se van liberando los búferes, la canalización vuelve a procesar las notificaciones.

Si un sumidero no funciona o no puede ingerir datos y el acuse de end-to-end recibo está activado para la fuente, la canalización deja de procesar las notificaciones de SQS hasta que reciba un acuse de recibo correcto de todos los sumideros.

Creación de canalizaciones OpenSearch de Amazon Ingestion

Una canalización es el mecanismo que Amazon OpenSearch Ingestion utiliza para mover los datos desde su origen (de donde provienen los datos) hasta su receptor (adonde van los datos). En OpenSearch Ingestion, el receptor siempre será un único dominio de Amazon OpenSearch Service, mientras que la fuente de los datos podrían ser clientes como Amazon S3, Fluent Bit o OpenTelemetry Collector.

Para obtener más información, consulte Pipelines en la OpenSearch documentación.

Temas

Requisitos previos y roles requeridos

Para crear una canalización OpenSearch de ingestión, debes disponer de los siguientes recursos:

- Una función de IAM que asumirá OpenSearch Ingestion para poder escribir en el receptor. Debe incluir este RNA de rol en la configuración de su canalización.
- Un dominio OpenSearch de servicio o una colección OpenSearch sin servidor que actúa como receptor. Si escribes en un dominio, debe ejecutar la OpenSearch versión 1.0 o una versión

posterior, o Elasticsearch 7.4 o una versión posterior. El receptor debe tener una política de acceso que conceda los permisos adecuados a su rol de canalización de IAM.

Si desea obtener instrucciones para crear estos recursos, consulte los siguientes temas:

- the section called “Otorgar a Pipelines acceso a los dominios”
- the section called “Otorgar a las canalizaciones acceso a las colecciones”

> **Note**
>
> Si escribe en un dominio que usa un control de acceso detallado, debe completar algunos pasos adicionales. Consulte the section called “Paso 3: asignar el rol de canalización (solo para dominios que utilicen un control de acceso detallado)”.

Permisos necesarios

OpenSearch Ingestion usa los siguientes permisos de IAM para crear canalizaciones:

- `osis:CreatePipeline`: Crear una canalización.
- `osis:ValidatePipeline`: Comprobar si la configuración de la canalización es válida.
- `iam:PassRole`— Transfiera la función de canalización a OpenSearch Ingestion para que pueda escribir datos en el dominio. Este permiso debe estar en el recurso de rol de canalización (el ARN que especifique para la opción `sts_role_arn` en la configuración de canalización) o simplemente `*` si planea usar diferentes roles en cada canalización.

Por ejemplo, la siguiente política concede permiso para crear una canalización:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:CreatePipeline",
            "osis:ListPipelineBlueprints",
            "osis:ValidatePipeline"
```

```
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
   ]
}
```

OpenSearch Ingestion también incluye un permiso denominado`osis:Ingest`, que es necesario para enviar solicitudes firmadas a la canalización mediante la versión 4 de Signature. Para obtener más información, consulte the section called “Creación de un rol de ingesta”.

> **Note**
>
> Además, el primer usuario que cree una canalización en una cuenta debe tener permisos para realizar la acción `iam:CreateServiceLinkedRole`. Para más información, consulte recurso de rol de canalización.

Para obtener más información sobre cada permiso, consulte las acciones, los recursos y las claves de condición de la OpenSearch ingestión en la Referencia de autorización de servicios.

Especificar la versión de la canalización

Al configurar una canalización, debe especificar la versión principal de Data Prepper en la que se ejecutará la canalización. Para especificar la versión, incluya la opción de `version` en la configuración de la canalización:

```
version: "2"
log-pipeline:
  source:
    ...
```

Al elegir Crear, OpenSearch Ingestion determina la última versión secundaria disponible de la versión principal que especifique y aprovisiona la canalización con esa versión. Por ejemplo, si lo especificas

`version: "2"` y la última versión compatible de Data Prepper es la 2.1.1, OpenSearch Ingestion aprovisiona tu canalización con la versión 2.1.1. No mostramos públicamente la versión secundaria que está ejecutando la canalización.

Para actualizar la canalización cuando haya disponible una nueva versión principal de Data Prepper, edite la configuración de la canalización y especifique la nueva versión. No puede cambiar una canalización a una versión anterior.

> **Note**
>
> OpenSearch Ingestion no ofrece soporte inmediato a las nuevas versiones de Data Prepper en cuanto se publican. Habrá cierto intervalo entre el momento en que una nueva versión esté disponible públicamente y el momento en OpenSearch que Ingestion la admita. Además, es posible que OpenSearch Ingestion no admita por completo determinadas versiones principales o secundarias de forma explícita. Para obtener una lista completa, consulte the section called “Versiones de Data Prepper admitidas”.

Cada vez que realices un cambio en tu canalización que inicie una implementación azul/verde, OpenSearch Ingestion podrá actualizarla a la última versión secundaria de la versión principal que esté configurada actualmente en el archivo YAML de la canalización. Para obtener más información, consulte. the section called “Implementaciones azul/verde para actualizaciones de canalización” OpenSearch La ingestión no puede cambiar la versión principal de tu canalización a menos que actualices explícitamente la `version` opción en la configuración de la canalización.

Especificación de la ruta de ingesta

Para las fuentes basadas en la extracción, como el rastreo de Otel y las métricas de Otel, OpenSearch Ingestion requiere la `path` opción adicional en la configuración de la fuente. La ruta es una cadena, por ejemplo`/log/ingest`, que representa la ruta del URI para la ingesta. Esta ruta define el URI que usa para enviar datos a la canalización.

Por ejemplo, supongamos que especifica la siguiente subcanalización de entrada para una canalización de ingesta denominada `logs`:

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

Al introducir datos de ingesta en la canalización, debe especificar el siguiente punto de conexión en la configuración de su cliente: `https://logs-abcdefgh.us-west-2.osis.amazonaws.com/my/test_path`.

La ruta debe empezar con una barra (/) y puede contener los caracteres especiales '-', '_', '.' y '/', así como el marcador de posición `${pipelineName}`. Si usa `${pipelineName}` (por ejemplo`path: "/${pipelineName}/test_path"`), la variable se sustituye por el nombre de la subcanalización asociada. En este ejemplo, sería `https://logs.us-west-2.osis.amazonaws.com/entry-pipeline/test_path`.

Creación de canalizaciones

En esta sección se describe cómo crear canalizaciones OpenSearch de ingestión mediante la consola de OpenSearch servicio y el. AWS CLI

Consola

Para crear una canalización

1. Inicia sesión en la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione Canalizaciones en el panel de navegación izquierdo y Seleccione Crear canalización.
3. Introduzca un nombre para la canalización.
4. (Opcional) Seleccione Habilitar búfer persistente. Un búfer persistente almacena los datos en un búfer basado en disco en varias zonas de disponibilidad. Para obtener más información, consulte Almacenamiento persistente. Si habilitas el búfer persistente, selecciona la AWS Key Management Service clave para cifrar los datos del búfer.
5. Configure la capacidad mínima y máxima de la canalización en las unidades de OpenSearch cómputo de ingestión (OCU). Para obtener más información, consulte the section called “Escala de canalizaciones”.
6. En Configuración de canalización, proporcione la configuración de la canalización en formato YAML. Un único archivo de configuración de canalización puede contener de 1 a 10 subcanalizaciones. Cada subcanalización es una combinación de una sola fuente, cero o más procesadores y un único receptor. En el OpenSearch caso de Ingestion, el receptor siempre debe ser un OpenSearch dominio de servicio. Para ver una lista de las opciones admitidas, consulte the section called “Complementos y opciones compatibles”.

> **Note**
>
> Debe incluir las opciones `sts_role_arn` y `sigv4` en cada subcanalización. La canalización asume la regla definida en `sts_role_arn` para firmar las solicitudes al dominio. Para obtener más información, consulte the section called “Otorgar a Pipelines acceso a los dominios”.

El siguiente archivo de configuración de ejemplo utiliza la fuente HTTP y los complementos Grok para procesar datos de registro no estructurados y enviarlos a un OpenSearch dominio de servicio. La subcanalización se denomina `log-pipeline`.

```
version: "2"
log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log: [ '%{COMMONAPACHELOG}' ]
    - date:
        from_time_received: true
        destination: "@timestamp"
  sink:
    - opensearch:
        hosts: [ "https://search-my-domain.us-east-1.es.amazonaws.com" ]
        index: "apache_logs"
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/{pipeline-role}"
          region: "us-east-1"
```

> **Note**
>
> Si especificas varios receptores dentro de una definición de canalización de YAML, todos deben pertenecer al mismo dominio de servicio. OpenSearch Una canalización OpenSearch de ingestión no puede escribir en varios dominios diferentes.

Puede crear su propia configuración de canalización o elegir Cargar archivo e importar una configuración existente para una canalización autoadministrada de Data Prepper. También puede utilizar un esquema de configuración.

7. Después de configurar la canalización, seleccione Validar canalización para confirmar que la configuración es correcta. Si la validación produce un error, corrija los errores y vuelva a ejecutar la validación.
8. En Red, seleccione Acceso a la VPC o Acceso público. Si elige Acceso público, vaya al siguiente paso. Si elige Acceso a la VCP, configure los siguientes ajustes:

Ajuste	Descripción
VPC	Seleccione el ID de la nube privada virtual (VPC) que desee utilizar. La VPC y la canalización deben estar en la misma Región de AWS.
Subredes	Elija una o más subredes. OpenSearch El servicio colocará un punto final de VPC e interfaces de red elásticas en las subredes.
Grupos de seguridad	Elija uno o más grupos de seguridad de VPC que permitan que la aplicación requerida llegue a la canalización de OpenSearch ingestión en los puertos (80 o 443) y protocolos (HTTP o HTTPs) expuestos por la canalización.

Para obtener más información, consulte the section called “Protección de canalizaciones dentro de una VPC”.

9. (Opcional) En Etiquetas, agregue una o más etiquetas (pares clave-valor) a su canalización. Para obtener más información, consulte the section called “Etiquetado de canalizaciones”.
10. (Opcional) En Opciones de publicación de registros, activa la publicación de registros de canalización en Amazon CloudWatch Logs. Le recomendamos que habilite la publicación de registros para poder solucionar más fácilmente los problemas de la canalización. Para más información, consulte the section called “Monitorear registros de canalización”.
11. Seleccione Siguiente.
12. Revise su configuración de canalización y seleccione Crear.

OpenSearch Ingestion ejecuta un proceso asíncrono para crear la canalización. Una vez que el estado de la canalización sea `Active`, puede empezar a incorporar datos.

AWS CLI

El comando create-pipeline acepta la configuración de la canalización como una cadena o dentro de un archivo .yaml. Si proporciona la configuración en forma de cadena, cada nueva línea debe ir acompañada de secuencias de escape `\n`. Por ejemplo, `"log-pipeline:\n source:\n http:\n processor:\n - grok:\n ..."`

El siguiente comando de ejemplo crea una canalización con la siguiente configuración:

- Mínimo de 4 OCU de ingesta, máximo de 10 OCU de ingesta
- Aprovisionada en una nube privada virtual (VPC)
- Publicación de registros habilitada

```
aws osis create-pipeline \
  --pipeline-name my-pipeline \
  --min-units 4 \
  --max-units 10 \
  --log-publishing-options
 IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="MyLogGroup"} \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

OpenSearch Ingestion ejecuta un proceso asíncrono para crear la canalización. Una vez que el estado de la canalización sea `Active`, puede empezar a incorporar datos. Para comprobar el estado de la canalización, usa el comando. GetPipeline

OpenSearch API de ingestión

Para crear una canalización OpenSearch de ingestión mediante la API de OpenSearch ingestión, llama a la operación. CreatePipeline

Una vez que la canalización se haya creado correctamente, puede configurar su cliente y empezar a ingerir datos en su OpenSearch dominio de servicio. Para obtener más información, consulte the section called “Trabajo con integraciones en canalización”.

Seguimiento del estado de creación de la canalización

Puede realizar un seguimiento del estado de una canalización a medida que OpenSearch Ingestion la aprovisiona y la prepara para ingerir datos.

Consola

Una vez creada inicialmente una canalización, ésta pasa por varias etapas a medida que OpenSearch Ingestion la prepara para la ingesta de datos. Para ver las distintas etapas de creación de la canalización, seleccione el nombre de la canalización para ver la página de Configuración de la canalización. En Estado, seleccione Ver detalles.

Una canalización pasa por las siguientes etapas antes de estar disponible para incorporar datos:

- Validación: se valida la configuración de la canalización. Cuando se complete esta etapa, todas las validaciones se han realizado correctamente.
- Crear entorno: preparar y aprovisionar recursos. Cuando se complete esta etapa, se habrá creado el nuevo entorno de canalización.
- Implementar canalización: implementar la canalización. Cuando se complete esta etapa, la canalización se habrá implementado correctamente.
- Comprobar el estado de la canalización: comprobación del estado de la canalización. Cuando se complete esta etapa, todas las comprobaciones de estado se habrán aprobado.
- Habilitar tráfico: permitir que la canalización incorpore datos. Cuando se complete esta etapa, puede empezar a incorporar datos a la canalización.

CLI

Usa el get-pipeline-change-progresscomando para comprobar el estado de una canalización. La siguiente AWS CLI solicitud comprueba el estado de una canalización denominada`my-pipeline`:

```
aws osis get-pipeline-change-progress \
    --pipeline-name my-pipeline
```

Respuesta:

```
{
   "ChangeProgressStatuses": {
```

```
      "ChangeProgressStages": [
         {
            "Description": "Validating pipeline configuration",
            "LastUpdated": 1.671055851E9,
            "Name": "VALIDATION",
            "Status": "PENDING"
         }
      ],
      "StartTime": 1.671055851E9,
      "Status": "PROCESSING",
      "TotalNumberOfStages": 5
   }
}
```

OpenSearch API de ingestión

Para realizar un seguimiento del estado de la creación de la canalización mediante la API OpenSearch de ingestión, llama a la GetPipelineChangeProgressoperación.

Uso de esquemas para crear una canalización

En lugar de crear una definición de canalización desde cero, puede usar esquemas de configuración, que son plantillas YAML preconfiguradas para escenarios de ingesta comunes, como los registros de Trace Analytics o Apache. Los esquemas de configuración le ayudan a aprovisionar canalizaciones fácilmente sin tener que crear una configuración desde cero.

Consola

Cómo usar un esquema de canalización

1. Inicia sesión en la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione Canalizaciones en el panel de navegación izquierdo y Seleccione Crear canalización.
3. En Configuración de canalización, seleccione Esquemas de configuración.
4. Seleccione un esquema. La configuración de la canalización se completa con una subcanalización para el caso de uso que haya seleccionado.
5. Revise el texto comentado que le guiará en la configuración del esquema.

> **Important**
>
> El esquema de la canalización no es válido tal como está. Debe realizar algunas modificaciones, como proporcionar el ARN Región de AWS y el rol que se utilizará para la autenticación; de lo contrario, la validación de la canalización fallará.

CLI

Para obtener una lista de todos los planos disponibles mediante el AWS CLI, envíe una list-pipeline-blueprintssolicitud.

```
aws osis list-pipeline-blueprints
```

La solicitud devuelve una lista de todos los esquemas disponibles.

Para obtener información más detallada sobre un plano específico, utilice el get-pipeline-blueprintcomando:

```
aws osis get-pipeline-blueprint --blueprint-name AWS-ApacheLogPipeline
```

Esta solicitud devuelve el contenido del esquema de la canalización de registro de Apache:

```
{
   "Blueprint":{
      "PipelineConfigurationBody":"###\n  # Limitations: https://docs.aws.amazon.com/
opensearch-service/latest/ingestion/ingestion.html#ingestion-limitations\n###\n###\n
 # apache-log-pipeline:\n    # This pipeline receives logs via http (e.g. FluentBit),
 extracts important values from the logs by matching\n    # the value in the 'log' key
 against the grok common Apache log pattern. The grokked logs are then sent\n    # to
 OpenSearch to an index named 'logs'\n###\n\nversion: \"2\"\napache-log-pipeline:\n
 source:\n    http:\n      # Provide the path for ingestion. ${pipelineName} will be
 replaced with pipeline name configured for this pipeline.\n      # In this case it
 would be \"/apache-log-pipeline/logs\". This will be the FluentBit output URI value.
\n      path: \"/${pipelineName}/logs\"\n  processor:\n    - grok:\n        match:\n
         log: [ \"%{COMMONAPACHELOG_DATATYPED}\" ]\n  sink:\n    - opensearch:\n
   # Provide an AWS OpenSearch Service domain endpoint\n        # hosts: [ \"https://
search-mydomain-1a2a3a4a5a6a7a8a9a0a9a8a7a.us-east-1.es.amazonaws.com\" ]\n
 aws:\n          # Provide a Role ARN with access to the domain. This role should have
```

```
 a trust relationship with osis-pipelines.amazonaws.com\n          # sts_role_arn:
 \"arn:aws:iam::123456789012:role/Example-Role\"\n          # Provide the region of the
 domain.\n          # region: \"us-east-1\"\n          # Enable the 'serverless' flag
 if the sink is an Amazon OpenSearch Serverless collection\n          # serverless:
 true\n        index: \"logs\"\n        # Enable the S3 DLQ to capture any failed
 requests in an S3 bucket\n        # dlq:\n          # s3:\n            # Provide an
 S3 bucket\n            # bucket: \"your-dlq-bucket-name\"\n            # Provide a key
 path prefix for the failed requests\n            # key_path_prefix: \"${pipelineName}/
logs/dlq\"\n            # Provide the region of the bucket.\n            # region:
 \"us-east-1\"\n            # Provide a Role ARN with access to the bucket. This role
 should have a trust relationship with osis-pipelines.amazonaws.com\n            #
 sts_role_arn: \"arn:aws:iam::123456789012:role/Example-Role\"\n",
      "BlueprintName":"AWS-ApacheLogPipeline"
    }
}
```

OpenSearch API de ingestión

Para obtener información sobre los planos de canalización mediante la API OpenSearch de ingestión, usa las ListPipelineBlueprintsoperaciones y. GetPipelineBlueprint

Visualización de canalizaciones de Amazon OpenSearch Ingestion

Puede ver los detalles sobre una canalización de Amazon OpenSearch Ingestion mediante la AWS Management Console, la AWS CLI o la API de OpenSearch Ingestion.

Consola

Para ver una canalización

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. Elija Canalizaciones en el panel de navegación izquierdo.
3. (Opcional) Para ver las canalizaciones con un estado determinado, elija Cualquier estado y seleccione un estado para filtrar.

   Una canalización puede tener los siguientes estados:

   - `Creating`: la canalización se está creando.
   - `Active`: la canalización está activa y lista para incorporar datos.

- `Updating`: la canalización se está actualizando.
- `Deleting`: la canalización se está eliminando.
- `Create failed`: la canalización no se pudo crear.
- `Update failed`: la canalización no se pudo actualizar.
- `Starting`: la canalización se está iniciando.
- `Start failed`: la canalización no se pudo iniciar.
- `Stopping`: la canalización se está deteniendo.
- `Stopped`: la canalización está detenida y se puede reiniciar en cualquier momento.

No se le facturan las OCU de ingesta cuando una canalización está en los estados `Create failed`, `Creating`, `Deleting` y `Stopped`.

CLI

Para ver las canalizaciones mediante la AWS CLI, envíe una solicitud de list-pipelines:

```
aws osis list-pipelines
```

La solicitud devuelve una lista de todas las canalizaciones existentes:

```
{
    "NextToken": null,
    "Pipelines": [
        {
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 4,
            "MinUnits": 2,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/log-pipeline",
            "PipelineName": "log-pipeline",
            "Status": "ACTIVE",
            "StatusReason": {
                "Description": "The pipeline is ready to ingest data."
            }
        },
            "CreatedAt": 1.671055851E9,
            "LastUpdatedAt": 1.671055851E9,
            "MaxUnits": 2,
```

```
            "MinUnits": 8,
            "PipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/another-
pipeline",
            "PipelineName": "another-pipeline",
            "Status": "CREATING",
            "StatusReason": {
                "Description": "The pipeline is being created. It is not able to ingest
 data."
            }
        }
    ]
}
```

Para ver información sobre una sola canalización, use el comando get-pipeline:

```
aws osis get-pipeline --pipeline-name "my-pipeline"
```

La solicitud devuelve la información de configuración de la canalización especificada:

```
{
    "Pipeline": {
        "PipelineName": "my-pipeline",
        "PipelineArn": "arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline",
        "MinUnits": 9,
        "MaxUnits": 10,
        "Status": "ACTIVE",
        "StatusReason": {
            "Description": "The pipeline is ready to ingest data."
        },
        "PipelineConfigurationBody": "log-pipeline:\n source:\n http:\n processor:\n
 - grok:\n match:\nlog: [ '%{COMMONAPACHELOG}' ]\n - date:\n from_time_received: true
\n destination: \"@timestamp\"\n  sink:\n - opensearch:\n hosts: [ \"https://search-
mdp-performance-test-duxkb4qnycd63rpy6svmvyvfpi.us-east-1.es.amazonaws.com\" ]\n index:
 \"apache_logs\"\n aws_sts_role_arn: \"arn:aws:iam::123456789012:role/my-domain-role
\"\n  aws_region: \"us-east-1\"\n  aws_sigv4: true",,
        "CreatedAt": "2022-10-01T15:28:05+00:00",
        "LastUpdatedAt": "2022-10-21T21:41:08+00:00",
        "IngestEndpointUrls": [
            "my-pipeline-123456789012.us-east-1.osis.amazonaws.com"
        ]
    }
}
```

API de OpenSearch Ingestion

Para ver las canalizaciones de ingesta de OpenSearch mediante la API de OpenSearch Ingestion, llame a las operaciones ListPipelines y GetPipeline.

Actualización de las canalizaciones OpenSearch de Amazon Ingestion

Puede actualizar las canalizaciones OpenSearch de Amazon Ingestion mediante la AWS Management Console, la o la AWS CLI API de OpenSearch ingestión. OpenSearch Ingestion inicia una implementación azul/verde al actualizar la configuración YAML de una canalización. Para obtener más información, consulte the section called “Implementaciones azul/verde para actualizaciones de canalización”.

Temas

Consideraciones

Tenga en cuenta lo siguiente cuando actualice una canalización:

- Puede editar los límites de capacidad, las opciones de publicación de registros y la configuración de YAML de una canalización. No puede editar su nombre ni su configuración de red.
- Si su canalización escribe en un receptor de dominio de VPC, no puede volver atrás y cambiar el receptor a un dominio de VPC diferente una vez creada la canalización. Debe eliminar y volver a crear manualmente la canalización con el nuevo receptor. Aún puede cambiar el receptor de un dominio de VPC a un dominio público, de un dominio público a un dominio de VPC o de un dominio público a otro dominio público.
- Puedes cambiar el receptor de canalización en cualquier momento entre un dominio de OpenSearch servicio público y una colección sin servidor. OpenSearch
- Al actualizar la configuración de YAML de una canalización, OpenSearch Ingestion inicia una implementación azul/verde. Para obtener más información, consulte the section called “Implementaciones azul/verde para actualizaciones de canalización”.

- Al actualizar la configuración YAML de una canalización, OpenSearch Ingestion la actualiza automáticamente a la última versión secundaria compatible de la versión principal de Data Prepper especificada en la configuración de la canalización. Este proceso mantiene su canalización actualizada con las últimas correcciones de errores y mejoras de rendimiento.
- Puede seguir actualizando su canalización cuando esté detenida.

Permisos necesarios

OpenSearch Ingestion utiliza los siguientes permisos de IAM para actualizar las canalizaciones:

- `osis:UpdatePipeline`: Actualizar una canalización.
- `osis:ValidatePipeline`: Comprobar si la configuración de la canalización es válida.
- `iam:PassRole`— Transfiera la función de canalización a OpenSearch Ingestion para que pueda escribir datos en el dominio. Este permiso solo es necesario si actualiza la configuración de YAML de la canalización, no si modifica otros ajustes, como la publicación de registros o los límites de capacidad.

Por ejemplo, la siguiente política concede permiso para actualizar una canalización:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Resource":"*",
         "Action":[
            "osis:UpdatePipeline",
            "osis:ValidatePipeline"
         ]
      },
      {
         "Resource":[
            "arn:aws:iam::{your-account-id}:role/{pipeline-role}"
         ],
         "Effect":"Allow",
         "Action":[
            "iam:PassRole"
         ]
      }
```

```
    ]
}
```

Actualización de las canalizaciones

Puede actualizar las canalizaciones OpenSearch de Amazon Ingestion mediante la AWS Management Console, la o la AWS CLI API de OpenSearch ingestión.

Consola

Cómo actualizar una canalización

1. Inicia sesión en la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione Canalizaciones en el panel de navegación izquierdo.
3. Seleccione una canalización para abrir su configuración. Puede editar los límites de capacidad, las opciones de publicación de registros y la configuración de YAML de una canalización. No puede editar su nombre ni su configuración de red.
4. Cuando termine de realizar los cambios, seleccione Guardar.

CLI

Para actualizar una canalización mediante el AWS CLI, envía una solicitud de actualización de la canalización. En el siguiente ejemplo de solicitud, se carga un nuevo archivo de configuración y se actualizan los valores de capacidad mínima y máxima:

```
aws osis update-pipeline \
  --pipeline-name "my-pipeline" \
  --pipline-configuration-body "file://new-pipeline-config.yaml" \
  --min-units 11 \
  --max-units 18
```

OpenSearch API de ingestión

Para actualizar una canalización OpenSearch de ingestión mediante la API de OpenSearch ingestión, llama a la operación. UpdatePipeline

Implementaciones azul/verde para actualizaciones de canalización

OpenSearch La ingestión inicia un proceso de despliegue azul o verde al actualizar la configuración YAML de una canalización.

Azul/Verde se refiere a la práctica de crear un nuevo entorno para actualizaciones de canalización y redirigir el tráfico al nuevo entorno una vez completadas dichas actualizaciones. La práctica minimiza el tiempo de inactividad y mantiene el entorno original en caso de que la implementación en el nuevo entorno no se produzca correctamente. Las implementaciones azul/verde en sí mismas no tienen ningún impacto en el rendimiento, pero este puede cambiar si la configuración de la canalización cambia de una manera que altere el rendimiento.

OpenSearch La ingestión bloquea el autoescalado durante las implementaciones azul/verde. Se le seguirá cobrando solo por el tráfico a la canalización anterior hasta que se redirija a la nueva canalización. Una vez que se haya redirigido el tráfico, solo se cobrará por la nueva canalización. Nunca se le cobrará por dos canalizaciones simultáneamente.

Al actualizar el archivo de configuración YAML de una canalización, OpenSearch Ingestion puede actualizarla automáticamente a la última versión secundaria compatible de la versión principal de Data Prepper especificada en la configuración de la canalización. Por ejemplo, es posible que tengas una `version: "2"` configuración de canalización e OpenSearch Ingestion aprovisionó inicialmente la canalización con la versión 2.1.0. Cuando se añade la compatibilidad con la versión 2.1.1 y realizas un cambio en la configuración de la canalización, OpenSearch Ingestion la actualiza a la versión 2.1.1.

Este proceso mantiene tu canalización actualizada con las últimas correcciones de errores y mejoras de rendimiento. OpenSearch Ingestion no puede actualizar la versión principal de tu canalización a menos que cambies manualmente la `version` opción en la configuración de la canalización.

Detener e iniciar canalizaciones de Amazon OpenSearch Ingestion

Detener e iniciar las canalizaciones de Amazon OpenSearch Ingestion le ayuda a administrar los costos de entornos de desarrollo y pruebas. Puede detener temporalmente una canalización en lugar de configurar y eliminar una canalización cada vez que la use.

Temas

- Información general de detener e iniciar una canalización de OpenSearch Ingestion
- Detener e iniciar una canalización de OpenSearch Ingestion

- Iniciar una canalización de OpenSearch Ingestion

Información general de detener e iniciar una canalización de OpenSearch Ingestion

Puede detener una canalización durante los períodos en los que no necesite incorporarle datos. Puede volver a iniciar la canalización en cualquier momento que necesite usarla. El inicio y la detención simplifican los procesos de configuración y eliminación de canalizaciones usadas para desarrollo, pruebas o actividades similares que no requieren disponibilidad continua.

Mientras su canalización esté detenida, no se le cobrará ninguna hora de Ingestion OCU. Puede seguir actualizando las canalizaciones detenidas y estas reciben actualizaciones automáticas de las versiones secundarias y revisiones de seguridad.

No use la opción de iniciar y detener si necesita mantener su canalización en ejecución pero tiene más capacidad de la que necesita. Si su proceso es demasiado costoso o no está muy ocupado, considere la posibilidad de reducir sus límites de capacidad máxima. Para obtener más información, consulte the section called “Escala de canalizaciones”.

Detener e iniciar una canalización de OpenSearch Ingestion

Para usar una canalización de OpenSearch Ingestion o realizar tareas de administración, siempre se empieza con una canalización activa, después se detiene la canalización y se vuelve a iniciar. Mientras su canalización esté detenida, no se le cobrará ninguna hora de Ingestion OCU.

Consola

Para detener una canalización

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación, elija Canalizaciones, y luego seleccione una canalización. Puede realizar la operación de detención desde esta página o navegar a la página de detalles de la canalización de datos que desea detener.
3. En Acciones, seleccione Detener canalización.

   Si no se puede detener ni iniciar una canalización, la acción Detener canalización no estará disponible.

AWS CLI

Para detener manualmente una canalización mediante AWS CLI, llame al comando stop-pipeline con los siguientes parámetros:

- `--pipeline-name`: el nombre de la canalización.

Example

```
aws osis stop-pipeline --pipeline-name my-pipeline
```

API de OpenSearch Ingestion

Para detener una canalización con la API de OpenSearch Ingestion, llame a la operación StopPipeline con el siguiente parámetro:

- `PipelineName`: el nombre de la canalización.

Iniciar una canalización de OpenSearch Ingestion

Para iniciar una canalización de OpenSearch Ingestion, siempre debe comenzar con una canalización que ya está en estado detenido. La canalización mantiene sus ajustes de configuración como límites de capacidad, configuración de red y opciones de publicación de registros.

El reinicio de la canalización suele tardar varios minutos.

Consola

Para iniciar una canalización

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación, elija Canalizaciones, y luego seleccione una canalización. Puede realizar la operación de inicio desde esta página o navegar a la página de detalles de la canalización que desea iniciar.
3. En Acciones, elija Iniciar canalización.

AWS CLI

Para iniciar una canalización con la AWS CLI, llame al comando start-pipeline con los siguientes parámetros:

- `--pipeline-name`: el nombre de la canalización.

Example

```
aws osis start-pipeline --pipeline-name my-pipeline
```

API de OpenSearch Ingestion

Para iniciar una canalización de OpenSearch Ingestion con la API de OpenSearch Ingestion, llame a la operación StartPipeline con el siguiente parámetro:

- `PipelineName`: el nombre de la canalización.

Eliminar canalizaciones de Amazon OpenSearch Ingestion

Puede eliminar una canalización de Amazon OpenSearch Ingestion mediante laAWS Management Console, la AWS CLI o la API de OpenSearch Ingestion. No puede eliminar una canalización si tiene un estado de `Creating` o `Updating`.

Consola

Para eliminar una canalización

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. Elija Canalizaciones en el panel de navegación izquierdo.
3. Seleccione la canalización que desee eliminar y seleccione Eliminar.
4. Confirme la eliminación y elija Eliminar.

CLI

Para eliminar una canalización mediante AWS CLI, envíe una solicitud de delete-pipeline:

```
aws osis delete-pipeline --pipeline-name "my-pipeline"
```

API de OpenSearch Ingestion

Para eliminar una canalización de OpenSearch Ingestion mediante la API de OpenSearch Ingestion, llame a la operación DeletePipeline con el siguiente parámetro:

- `PipelineName`: el nombre de la canalización

Plugins y opciones compatibles para las canalizaciones de Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion admite un subconjunto de fuentes, procesadores y receptores en comparación con Data Prepper de código abierto. Además, OpenSearch Ingestion impone algunas restricciones a las opciones disponibles para cada complemento compatible. En las siguientes secciones se describen los complementos y las opciones asociadas que admite OpenSearch Ingestion.

> **Note**
>
> OpenSearch Ingestion no admite ningún complemento de búfer porque configura automáticamente un búfer predeterminado. Si incluye un búfer en la configuración de la canalización, recibirá un error de validación.

Temas

Complementos compatibles

OpenSearch Ingestion es compatible con los siguientes complementos de Data Prepper:

Fuentes:

- Dynamodb
- OpenSearch

- HTTP
- Kafka
- Registros de OTel
- Métricas de OTel
- Rastreo de OTel
- S3

Procesadores:

- Aggregate
- Detector de anomalías
- CSV
- Fecha
- Descomprimir
- Diseccionar
- Soltar eventos
- Geo IP
- Grok
- Valor de clave
- Mapa para enumerar
- Evento de mutación (serie de procesadores)
- Muta la cadena (serie de procesadores)
- Obfuscate
- Métricas de OTel
- Grupo de rastreo OTel
- Rastreo de OTel
- Parse Ion

- Analizar JSON
- Analizar XML
- Seleccione las entradas
- Mapa de servicios
- Reenviador por pares de seguimiento
- Truncar
- Agente usuario

Receptores:

- OpenSearch(es compatible con OpenSearch Service, OpenSearch Serverless y Elasticsearch 6.8 o versiones posteriores)
- S3

Códecs de receptor:

- Avro
- NDJSON
- JSON
- Parquet

Procesadores sin estado frente a procesadores con estado

Los procesadores sin estado realizan operaciones como las transformaciones y el filtrado, mientras que los procesadores con estado realizan operaciones como las agregaciones, que recuerdan el resultado de la ejecución anterior. OpenSearch Ingestion es compatible con los procesadores con estado Aggregate y Service-map. Todos los demás procesadores compatibles no tienen estado.

En el caso de las canalizaciones que contienen únicamente procesadores sin estado, el límite máximo de capacidad es de 96 OCU de ingestión. Si una canalización contiene procesadores con estado, el límite máximo de capacidad es de 48 OCU de ingestión. Sin embargo, si una canalización tiene habilitado el almacenamiento en búfer persistente, puede tener un máximo de 384 OCU de ingestión solo con procesadores sin estado, o 192 OCU de ingestión si contiene algún procesador con estado. Para obtener más información, consulte the section called “Escala de canalizaciones”.

El nd-to-end reconocimiento electrónico solo es compatible con procesadores sin estado. Para obtener más información, consulte the section called “nd-to-end Reconocimiento electrónico”.

Requisitos y restricciones de configuración

A menos que se especifique lo contrario a continuación, todas las opciones descritas en la referencia de configuración de Data Prepper para los complementos compatibles enumerados anteriormente están permitidas en OpenSearch los procesos de ingestión. En las siguientes secciones, se explican las restricciones que OpenSearch Ingestion impone a determinadas opciones de los complementos.

> **Note**
>
> OpenSearch Ingestion no admite ningún complemento de búfer porque configura automáticamente un búfer predeterminado. Si incluye un búfer en la configuración de la canalización, recibirá un error de validación.

OpenSearch Ingestion configura y administra internamente muchas opciones, como y. `authentication` `acm_certificate_arn` Otras opciones, como `thread_count` `yrequest_timeout`, tienen un impacto en el rendimiento si se modifican manualmente. Por lo tanto, estos valores se establecen internamente para garantizar un rendimiento óptimo de sus canalizaciones.

Por último, algunas opciones no se pueden pasar a OpenSearch Ingestion, como `ism_policy_file` `ysink_template`, porque son archivos locales cuando se ejecutan en Data Prepper de código abierto. No se admiten estos valores.

Temas

- Opciones generales de canalización
- Procesador Grok
- Origen de HTTP
- OpenSearch sumidero
- Fuente de métricas de OTel, fuente de rastreo de OTel y fuente de registros de OTel
- Procesador de grupos de rastreo de OTel
- Procesador de rastreo de OTel
- Procesador de mapas de servicio

- Fuente de S3

Opciones generales de canalización

OpenSearch Ingestion establece las siguientes opciones generales de canalización y no se admiten en las configuraciones de canalización:

- `workers`
- `delay`

Procesador Grok

No se admiten las siguientes opciones de procesador Grok:

- `patterns_directories`
- `patterns_files_glob`

Origen de HTTP

El complemento fuente HTTP tiene los siguientes requisitos y restricciones:

- La opción `path` es obligatoria. La ruta es una cadena, por ejemplo `/log/ingest`, que representa la ruta del URI para la ingesta de registros. Esta ruta define el URI que usa para enviar datos a la canalización. Por ejemplo, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. La ruta debe empezar con una barra (/) y puede contener los caracteres especiales '-', '_', '.' y '/', así como el marcador de posición `${pipelineName}`.
- OpenSearch Ingestion establece las siguientes opciones de fuente HTTP y no se admiten en las configuraciones de canalización:
  - `port`
  - `ssl`
  - `ssl_key_file`
  - `ssl_certificate_file`
  - `aws_region`
  - `authentication`
  - `unauthenticated_health_check`

- `use_acm_certificate_for_ssl`
- `thread_count`
- `request_timeout`
- `max_connection_count`
- `max_pending_requests`
- `health_check_service`
- `acm_private_key_password`
- `acm_certificate_timeout_millis`
- `acm_certificate_arn`

OpenSearch sumidero

El complemento OpenSearchsink tiene los siguientes requisitos y limitaciones.

- La opción `aws` es obligatoria y debe contener las siguientes opciones:
  - `sts_role_arn`
  - `region`
  - `hosts`
  - `serverless`(si el sumidero es una colección OpenSearch sin servidor)
- La opción `sts_role_arn` debe apuntar al mismo rol para cada receptor de un archivo de definición YAML.
- La `hosts` opción debe especificar un punto final de dominio OpenSearch de servicio o un punto final de colección OpenSearch sin servidor. Todos los hosts de un archivo de definición YAML deben apuntar al mismo punto de conexión. No se puede especificar un punto de conexión personalizado para un dominio; este debe ser el punto de conexión estándar.
- Si la opción de `hosts` es un punto de conexión de la colección sin servidor, debe configurar la opción `serverless` en `true`. Además, si su archivo de definición YAML contiene la opción `index_type`, debe estar configurada en `management_disabled`, de lo contrario, la validación fallará.
- Las siguientes opciones no son compatibles:
  - `username`
  - `password`
  - `cert`

- `proxy`
- `dlq_file`: si quiere descargar los eventos fallidos a una cola de mensajes fallidos (DLQ), debe usar la opción `dlq` y especificar un bucket de S3.
- `ism_policy_file`
- `socket_timeout`
- `template_file`
- `insecure`
- `bulk_size`

Fuente de métricas de OTel, fuente de rastreo de OTel y fuente de registros de OTel

Los complementos de la fuente de métricas de OTel, la fuente de rastreo de OTel y los registros de OTel tienen los siguientes requisitos y limitaciones:

- La opción `path` es obligatoria. La ruta es una cadena, por ejemplo `/log/ingest`, que representa la ruta del URI para la ingesta de registros. Esta ruta define el URI que usa para enviar datos a la canalización. Por ejemplo, `https://log-pipeline.us-west-2.osis.amazonaws.com/log/ingest`. La ruta debe empezar con una barra (/) y puede contener los caracteres especiales '-', '_', '.' y '/', así como el marcador de posición `${pipelineName}`.
- OpenSearch Ingestion establece las siguientes opciones y no se admiten en las configuraciones de canalización:
  - `port`
  - `ssl`
  - `sslKeyFile`
  - `sslKeyCertChainFile`
  - `authentication`
  - `unauthenticated_health_check`
  - `useAcmCertForSSL`
  - `unframed_requests`
  - `proto_reflection_service`
  - `thread_count`
  - `request_timeout`
  - `max_connection_count`

- `acmPrivateKeyPassword`
- `acmCertIssueTimeOutMillis`
- `health_check_service`
- `acmCertificateArn`
- `awsRegion`

Procesador de grupos de rastreo de OTel

El procesador de grupos de rastreo de OTel tiene los siguientes requisitos y limitaciones:

- La opción `aws` es obligatoria y debe contener las siguientes opciones:
  - `sts_role_arn`
  - `region`
  - `hosts`
- La `sts_role_arn` opción especifica la misma función que la función de canalización que especificas en la configuración del OpenSearch receptor.
- No se admiten las opciones `username`, `password`, `cert`, y `insecure`.
- La opción `aws_sigv4` es obligatoria y se debe establecer en verdadero.
- No se admite la `serverless` opción incluida en el complemento de OpenSearch sumidero. El procesador Otel Trace Group no funciona actualmente con las colecciones OpenSearch Serverless.
- El número de procesadores `otel_trace_group` en el cuerpo de configuración de la canalización no puede ser superior a 8.

Procesador de rastreo de OTel

El procesador de rastreo de OTel tiene los siguientes requisitos y limitaciones:

- El valor de la opción `trace_flush_interval` no puede superar los 300 segundos.

Procesador de mapas de servicio

El procesador de Service-map tiene los siguientes requisitos y limitaciones:

- El valor de la opción `window_duration` no puede superar los 300 segundos.

Fuente de S3

El complemento fuente de S3 tiene los siguientes requisitos y limitaciones:

- La opción `aws` es obligatoria y debe contener las opciones `region` y `sts_role_arn`.
- El valor de la opción `records_to_accumulate` no puede ser superior a 200.
- El valor de la opción `maximum_messages` no puede ser superior a 10.
- Si se especifica, la opción `disable_bucket_ownership_validation` se debe establecer en falso.
- Si se especifica, la opción `input_serialization` se debe establecer en `parquet`.

Trabajar con las integraciones de Amazon OpenSearch Ingestion Pipeline

Para poder introducir datos correctamente en una canalización de Amazon OpenSearch Ingestion, debe configurar la aplicación cliente (la fuente) para enviar los datos al punto final de la canalización. Su fuente pueden ser clientes como los registros de Fluent Bit, el OpenTelemetry Collector o un simple bucket de S3. La configuración exacta es diferente para cada cliente.

Las diferencias importantes durante la configuración de la fuente (en comparación con el envío de datos directamente a un dominio de OpenSearch servicio o a una recopilación OpenSearch sin servidor) son el nombre del AWS servicio (`osis`) y el punto final del host, que debe ser el punto final de la canalización.

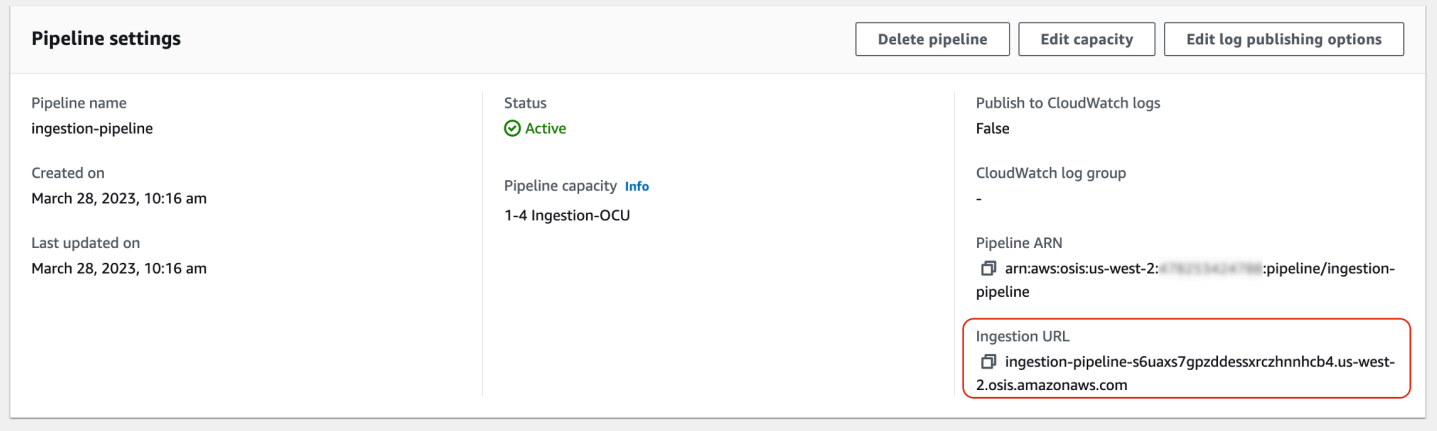
Temas

- Creación del punto de conexión de ingesta
- Creación de un rol de ingesta
- Uso de una canalización OpenSearch de ingestión con Amazon DynamoDB
- Uso de una canalización OpenSearch de ingestión con Amazon Managed Streaming for Apache Kafka
- Uso de una canalización OpenSearch de ingestión con Amazon S3
- Uso de una canalización de OpenSearch ingestión con Amazon Security Lake
- Uso de una canalización de ingestión con Fluent Bit OpenSearch
- Uso de una canalización OpenSearch de ingestión con Collector OpenTelemetry

- Siguientes pasos

Creación del punto de conexión de ingesta

Para incorporar datos a una canalización, envíelos al punto de conexión de ingesta. Para localizar la URL de ingesta, navegue a la página de Configuración de canalización y copie la URL de ingesta:



Para crear el punto de conexión de ingesta completo para fuentes basadas en pull, como el rastreo OTel y las métricas de OTel, añada la ruta de ingesta desde la configuración de la canalización hasta la URL de ingesta.

Por ejemplo, supongamos que su configuración de canalización tiene la siguiente ruta de ingesta:

```
entry-pipeline:
  source:
    http:
      path: "/my/test_path"
```

El punto de conexión de ingesta completo, que se especifica en la configuración de su cliente, tendrá el siguiente formato: `https://ingestion-pipeline-abcdefg.us-west-2.osis.amazonaws.com/my/test_path`.

Para más información, consulte the section called “Especificación de la ruta de ingesta”.

Creación de un rol de ingesta

Todas las solicitudes de OpenSearch ingestión deben firmarse con la versión 4 de Signature. Como mínimo, el rol que firma la solicitud debe tener permiso para realizar la `osis:Ingest` acción, lo que le permite enviar datos a una canalización de OpenSearch Ingestion.

Por ejemplo, la siguiente política AWS Identity and Access Management (IAM) permite que la función correspondiente envíe datos a una única canalización:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "osis:Ingest",
      "Resource": "arn:aws:osis:us-east-1:{account-id}:pipeline/pipeline-name"
    }
  ]
}
```

> **Note**
>
> Para usar el rol en todas las canalizaciones, sustituya el ARN del elemento `Resource` por un comodín (*).

Provisión de acceso de ingesta entre cuentas

> **Note**
>
> Solo puede proporcionar acceso de ingesta entre cuentas a las canalizaciones públicas, no a las canalizaciones de VPC.

Es posible que tengas que introducir datos en una canalización desde otra Cuenta de AWS, como una cuenta que aloje tu aplicación de origen. Si la entidad principal que escribe en una canalización está en una cuenta diferente a la de la propia canalización, debe configurar la entidad principal para que confíe en otro rol de IAM para incorporar los datos a la canalización.

Cómo configurar los permisos de ingesta entre cuentas

1. Crea el rol de ingesta con `osis:Ingest` permiso (descrito en la sección anterior) dentro de la Cuenta de AWS misma canalización. Para ver instrucciones, consulte Creación de roles de IAM.
2. Adjunte una política de confianza al rol de ingesta que permita que la entidad principal de otra cuenta lo asuma:

```
{
  "Version": "2012-10-17",
  "Statement": [{
     "Effect": "Allow",
     "Principal": {
       "AWS": "arn:aws:iam::{external-account-id}:root"
      },
     "Action": "sts:AssumeRole"
  }]
}
```

3. En la otra cuenta, configure la aplicación cliente (por ejemplo, Fluent Bit) para que asuma el rol de ingesta. Para que esto funcione, la cuenta de la aplicación debe conceder permisos al usuario o rol de la aplicación para que asuma el rol de ingesta.

   El siguiente ejemplo de política basada en identidad permite que la entidad principal adjunta asuma el `ingestion-role` de la cuenta de canalización:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::{account-id}:role/ingestion-role"
    }
  ]
}
```

A continuación, la aplicación cliente puede utilizar la AssumeRoleoperación para asumir `ingestion-role` e ingerir datos en la canalización asociada.

Uso de una canalización OpenSearch de ingestión con Amazon DynamoDB

Puede usar una canalización de OpenSearch ingestión con DynamoDB para transmitir eventos de tablas de DynamoDB (como crear, actualizar y eliminar) a los dominios y colecciones de Amazon Service. OpenSearch La canalización de OpenSearch ingestión incorpora una infraestructura de captura de datos de cambios (CDC) para proporcionar una forma de alta escala y baja latencia de transmitir datos de forma continua desde una tabla de DynamoDB.

Existen dos formas de utilizar DynamoDB como origen para procesar datos: con y sin una instantánea inicial completa.

Una instantánea inicial completa es una copia de seguridad de una tabla que DynamoDB realiza con point-in-time la función de recuperación (PITR). DynamoDB carga esta instantánea en Amazon S3. Desde allí, una canalización de OpenSearch ingestión la envía a un índice de un dominio o la divide en varios índices de un dominio. Para mantener la coherencia de los datos en DynamoDB OpenSearch , la canalización sincroniza todos los eventos de creación, actualización y eliminación de la tabla de DynamoDB con los documentos guardados en el índice o los índices. OpenSearch

Cuando utiliza una instantánea inicial completa, la canalización de OpenSearch ingestión ingiere primero la instantánea y, a continuación, comienza a leer los datos de DynamoDB Streams. Con el tiempo, recupera y mantiene la coherencia de los datos casi en tiempo real entre DynamoDB y. OpenSearch Si elige esta opción, debe habilitar tanto la PITR como una transmisión de DynamoDB en la tabla.

También puede usar la integración de OpenSearch Ingestion con DynamoDB para transmitir eventos sin necesidad de una instantánea. Elija esta opción si ya tiene una instantánea completa de algún otro mecanismo o si solo quiere transmitir los eventos actuales de una tabla de DynamoDB con DynamoDB Streams. Si elige esta opción, solo necesita habilitar una transmisión de DynamoDB en su tabla.

Para obtener más información sobre esta integración, consulte la integración de DynamoDB Zero-ETL con OpenSearch Amazon Service en la Guía para desarrolladores.Amazon DynamoDB

Temas

Requisitos previos

Para configurar la canalización, debe tener una tabla de DynamoDB con DynamoDB Streams activado. La transmisión debe usar el tipo de vista de transmisión `NEW_IMAGE`. Sin embargo, las

canalizaciones OpenSearch de ingestión también pueden transmitir eventos `NEW_AND_OLD_IMAGES` si este tipo de vista de transmisión se ajusta a su caso de uso.

Si utilizas instantáneas, también debes habilitar la point-in-time recuperación en tu mesa. Para obtener más información, consulte Crear una tabla, Habilitar la point-in-time recuperación y Habilitar una transmisión en la Guía para desarrolladores de Amazon DynamoDB.

Paso 1: configurar el rol de canalización

Una vez configurada la tabla de DynamoDB, configure el rol de canalización que desee usar en la configuración de canalización y añada los siguientes permisos de DynamoDB al rol:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "allowRunExportJob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeTable",
                "dynamodb:DescribeContinuousBackups",
                "dynamodb:ExportTableToPointInTime"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table"
            ]
        },
        {
            "Sid": "allowCheckExportjob",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeExport"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/export/*"
            ]
        },
        {
            "Sid": "allowReadFromStream",
            "Effect": "Allow",
            "Action": [
                "dynamodb:DescribeStream",
                "dynamodb:GetRecords",
```

```
                "dynamodb:GetShardIterator"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-east-1:{account-id}:table/my-table/stream/*"
            ]
        },
        {
            "Sid": "allowReadAndWriteToS3ForExport",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": [
                "arn:aws:s3:::my-bucket/export/*"
            ]
        }
    ]
}
```

También puede usar una clave administrada por el AWS KMS cliente para cifrar los archivos de datos de exportación. Para descifrar los objetos exportados, especifique `s3_sse_kms_key_id` para el ID de clave en la configuración de exportación de la canalización con el siguiente formato: `arn:aws:kms:us-west-2:{account-id}:key/my-key-id`.

Paso 2: crear la canalización

A continuación, puede configurar una canalización de OpenSearch ingestión como la siguiente, que especifica DynamoDB como origen. Este ejemplo de canalización incorpora los datos de la `table-a` con la instantánea de PITR, seguidos de los eventos de DynamoDB Streams. Una posición inicial de `LATEST` indica que la canalización debe leer los datos más recientes de DynamoDB Streams.

```
version: "2"
cdc-pipeline:
  source:
    dynamodb:
      tables:
      - table_arn: "arn:aws:dynamodb:us-west-2:{account-id}:table/table-a"
        export:
          s3_bucket: "my-bucket"
```

```
          s3_prefix: "export/"
        stream:
          start_position: "LATEST"
      aws:
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
  sink:
  - opensearch:
      hosts: ["https://search-mydomain.us-east-1.es.amazonaws.com"]
      index: "${getMetadata(\"table_name\")}"
      index_type: custom
      document_id: "${getMetadata(\"primary_key\")}"
      action: "${getMetadata(\"opensearch_action\")}"
      document_version: "${getMetadata(\"document_version\")}"
      document_version_type: "external"
```

Puede usar el blueprint de AWS-DynamoDB ChangeDataCapturePipeline o SingleTableDesignPipelineAWS-DynamoDB para crear esta canalización. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

Coherencia de datos

OpenSearch La end-to-end ingestión permite el reconocimiento para garantizar la durabilidad de los datos. Cuando una canalización lee instantáneas o transmisiones, crea particiones de forma dinámica para el procesamiento paralelo. La canalización marca una partición como completa cuando recibe un acuse de recibo después de ingerir todos los registros del dominio o la OpenSearch colección.

Si quieres incorporarlos a una colección de búsquedas OpenSearch sin servidor, puedes generar un identificador de documento en la canalización. Si quieres incorporarlo a una colección de series temporales OpenSearch sin servidor, ten en cuenta que la canalización no genera un identificador de documento.

Una canalización OpenSearch de ingestión también asigna las acciones de los eventos entrantes a las correspondientes acciones de indexación masiva para facilitar la ingesta de documentos. Esto mantiene la coherencia de los datos, de modo que cada cambio de datos en DynamoDB se concilia con los cambios correspondientes en el documento. OpenSearch

Asignación de tipos de datos

OpenSearch El servicio asigna dinámicamente los tipos de datos de cada documento entrante al tipo de datos correspondiente en DynamoDB. En la siguiente tabla se muestra cómo OpenSearch Service asigna automáticamente varios tipos de datos.

Tipo de datos	OpenSearch	DynamoDB
Número	OpenSearch mapea automáticamente los datos numéricos. Si el número es un número entero, lo OpenSearch asigna como un valor largo. Si el número es fraccionario, lo OpenSearch mapea como un valor flotante. OpenSearch mapea dinámicamente varios atributos en función del primer documento enviado. Si tiene una combinación de tipos de datos para el mismo atributo en DynamoDB, como un número entero y un número fraccionario, es posible que se produzca un error en la asignación. Por ejemplo, si el primer documento tiene un atributo que es un número entero y un documento posterior tiene el mismo atributo que un número fracciona rio, OpenSearch no podrá ingerir el segundo documento. En estos casos, debe proporcionar una plantilla de asignación explícita, como la siguiente: `{ "template": { "mappings": { "properties": {`	DynamoDB admite números.

Tipo de datos	OpenSearch	DynamoDB

	<pre>"MixedNumberAttribute": {
	"type": "float"
	}
	}
	}
	}
	}</pre>
	Si necesita una precisión doble, utilice la asignación de campos de tipo cadena. No hay ningún tipo numérico equivalente que admita una precisión de 38 dígitos. OpenSearch	

Conjunto de números	OpenSearch asigna automáticamente un conjunto de números a una matriz de valores largos o flotantes. Al igual que con los números escalares, esto depende de si el primer número incorporado es un número entero o un número fraccionario. Puede proporcio nar asignaciones para conjuntos de números de la misma manera que asigna cadenas escalares.	DynamoDB admite tipos que represent an conjuntos de números.

Tipo de datos	OpenSearch	DynamoDB
Cadena	OpenSearch mapea automáticamente los valores de cadena como texto. En algunas situaciones, como en el caso de los valores enumerados, puede asignarlos al tipo de palabra clave. El siguiente ejemplo muestra cómo asignar un atributo de DynamoDB `PartType` denominado a una palabra clave. OpenSearch `{ "template": { "mappings": { "properties": { "PartType": { "type": "keyword" } } } } }`	DynamoDB admite cadenas.
Conjunto de cadenas	OpenSearch asigna automáticamente un conjunto de cadenas a una matriz de cadenas. Puede proporcionar asignaciones para conjuntos de cadenas de la misma manera que asigna cadenas escalares.	DynamoDB admite tipos que representan conjuntos de cadenas.

Tipo de datos	OpenSearch	DynamoDB
Binario	OpenSearch mapea automáticamente los datos binarios como texto. Puede proporcionar un mapeo para escribirlos como campos binarios OpenSearch. El siguiente ejemplo muestra cómo asignar un atributo de DynamoDB `ImageData` denominado a OpenSearch un campo binario. `{ "template": { "mappings": { "properties": { "ImageData": { "type": "binary" } } } } }`	DynamoDB es compatible con los atributos de tipo binarios.
Conjunto binario	OpenSearch asigna automáticamente un conjunto binario a una matriz de datos binarios en forma de texto. Puede proporcionar asignaciones para conjuntos de números de la misma manera que asigna el binario escalar.	DynamoDB admite tipos que representan conjuntos de valores binarios.
Booleano	OpenSearch asigna un tipo booleano de DynamoDB a un tipo booleano. OpenSearch	DynamoDB admite atributos de tipo booleano.

Tipo de datos	OpenSearch	DynamoDB
Nulo	OpenSearch puede ingerir documentos del tipo null de DynamoDB. Guarda el valor como un valor nulo en el documento. No hay ninguna asignación para este tipo y este campo no está indexado ni se puede buscar en él. Si se utiliza el mismo nombre de atributo para un tipo nulo y, posteriormente, se cambia a un tipo diferente, como una cadena, OpenSearch crea una asignación dinámica para el primer valor no nulo. Los valores subsiguientes pueden seguir siendo valores nulos de DynamoDB.	DynamoDB admite atributos de tipo nulo.

Tipo de datos	OpenSearch	DynamoDB
Asignación	OpenSearch asigna los atributos del mapa de DynamoDB a campos anidados. Las mismas asignaciones se aplican dentro de un campo anidado. El siguiente ejemplo asigna una cadena de un campo anidado a un tipo de palabra clave en: OpenSearch `{ "template": { "mappings": { "properties": { "AdditionalDescriptions": { "properties": { "PartType": { "type": "keyword" } } } } } } }`	DynamoDB admite atributos de tipo asignación.

Tipo de datos	OpenSearch	DynamoDB
Enumeración	OpenSearch proporciona resultados diferentes para las listas de DynamoDB, según el contenido de la lista. Cuando una lista contiene todos los tipos escalares del mismo tipo (por ejemplo, una lista de todas las cadenas), OpenSearch ingiere la lista como una matriz de ese tipo. Esto funciona para los tipos cadena, número, booleano y nulo. Las restricciones para cada uno de estos tipos son las mismas que las restricciones para un escalar de ese tipo. También puede proporcionar asignaciones para listas de mapas con la misma asignación que usaría para un mapa. No puede proporcionar una lista de tipos mixtos.	DynamoDB admite atributos de tipo lista.

Tipo de datos	OpenSearch	DynamoDB
Establezca	OpenSearch proporciona resultados diferentes para los conjuntos de DynamoDB en función del contenido del conjunto. Cuando un conjunto contiene todos los tipos escalares del mismo tipo (por ejemplo, un conjunto de todas las cadenas), OpenSearch ingiere el conjunto como una matriz de ese tipo. Esto funciona para los tipos cadena, número, booleano y nulo. Las restricciones para cada uno de estos tipos son las mismas que las restricciones para un escalar de ese tipo. También puede proporcionar asignaciones para conjuntos de mapas con la misma asignación que usaría para un mapa. No puede proporcionar un conjunto de tipos mixtos.	DynamoDB admite tipos que representan conjuntos.

Le recomendamos que configure la cola de mensajes sin salida (DLQ) en su canalización de ingestión. OpenSearch Si has configurado la cola, el OpenSearch servicio envía a la cola todos los documentos fallidos que no se puedan ingerir debido a errores de mapeo dinámico.

En caso de que las asignaciones automáticos fallen, puede usar `template_type` y `template_content` en su configuración de canalización para definir reglas de asignación explícitas. Como alternativa, puede crear plantillas de asignación directamente en su dominio o colección de búsqueda antes de iniciar la canalización.

Limitaciones

Tenga en cuenta las siguientes limitaciones al configurar una canalización de OpenSearch ingestión para DynamoDB:

- La integración OpenSearch de ingestión con DynamoDB actualmente no admite la ingestión entre regiones. La tabla de DynamoDB OpenSearch y la canalización de ingestión deben estar en la misma posición. Región de AWS
- La tabla de DynamoDB OpenSearch y la canalización de ingestión deben estar en la misma posición. Cuenta de AWS
- Una canalización OpenSearch de ingestión solo admite una tabla de DynamoDB como fuente.
- DynamoDB Streams solo almacena datos en un registro durante un máximo de 24 horas. Si la ingesta de una instantánea inicial de una tabla grande demora 24 horas o más, se producirá una pérdida inicial de datos. Para mitigar esta pérdida de datos, calcule el tamaño de la tabla y configure las unidades informáticas adecuadas de las canalizaciones de OpenSearch ingestión.

Uso de una canalización OpenSearch de ingestión con Amazon Managed Streaming for Apache Kafka

Puede usar el complemento de Kafka para incorporar datos de Amazon Managed Streaming for Apache Kafka (Amazon MSK) OpenSearch a su canal de ingestión. Con Amazon MSK, puede crear y ejecutar aplicaciones que utilizan Apache Kafka para procesar datos de streaming. OpenSearch Ingestion utiliza AWS PrivateLink para conectarse a Amazon MSK.

Temas

Requisitos previos

Antes de crear su canalización OpenSearch de ingestión, lleve a cabo los siguientes pasos:

1. Cree un clúster de Amazon MSK siguiendo los pasos que se indican en Creación de un clúster de la Guía del desarrollador de Amazon Managed Streaming para Apache Kafka.
   - Para el tipo de clúster, selecciona Provisionado. OpenSearch La ingestión no es compatible con los clústeres de MSK sin servidor.
2. Cuando el clúster tenga el estado Activo, siga los pasos que se indican en Activar la conectividad de varias VPC.
3. Siga los pasos que se indican en Adjuntar una política de clúster al clúster de MSK para adjuntar una de las siguientes políticas, en función de si el clúster y la canalización están en la misma Cuenta de AWS. Esta política permite a OpenSearch Ingestion crear una AWS PrivateLink conexión con su clúster de Amazon MSK y leer datos de los temas de Kafka. Asegúrese de actualizar el `resource` con su propio ARN.

   Las siguientes políticas se aplican cuando el clúster y la canalización están en la misma Cuenta de AWS:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
```

```
      ],
      "Resource": "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-
id"
    }
  ]
}
```

Si su clúster de MSK se encuentra en un proceso Cuenta de AWS diferente al suyo, adjunte la siguiente política en su lugar. El ARN para el AWS `principal` debe ser el ARN del mismo rol de canalización que proporcionaste a la configuración de YAML de tu canalización:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "osis-pipelines.amazonaws.com"
      },
      "Action": [
        "kafka:CreateVpcConnection",
        "kafka:GetBootstrapBrokers",
        "kafka:DescribeCluster",
        "kafka:DescribeClusterV2"
      ],
      "Resource": "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-
name/cluster-id"
    },
    {
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::{pipeline-account-id}:role/pipeline-role"
      },
      "Action": [
        "kafka-cluster:*",
        "kafka:*"
      ],
      "Resource": [
        "arn:aws:kafka:us-east-1:{msk-account-id}:cluster/cluster-name/cluster-id",
        "arn:aws:kafka:us-east-1:{msk-account-id}:topic/cluster-name/cluster-id/*",
        "arn:aws:kafka:us-east-1:{msk-account-id}:group/cluster-name/*"
      ]
    }
  ]
}
```

4. Cree un tema de Kafka siguiendo los pasos de Creación de un tema. Asegúrese de que *BootstrapServerString* sea una de las URL de arranque del punto de conexión privado (VPC única). El valor de `--replication-factor` debe ser 2 o 3, en función del número de zonas que tenga su clúster de MSK. El valor de las `--partitions` debe ser como mínimo `10`.
5. Produzca y consuma datos siguiendo los pasos de Producir y consumir datos. De nuevo, asegúrese de que *BootstrapServerString* sea una de las URL de arranque del punto de conexión privado (VPC única).

Paso 1: configurar el rol de canalización

Una vez configurado el clúster de MSK, añada los siguientes permisos de Kafka al rol de canalización que desee usar en la configuración de canalización:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:Connect",
                "kafka-cluster:AlterCluster",
                "kafka-cluster:DescribeCluster",
                "kafka:DescribeClusterV2",
                "kafka:GetBootstrapBrokers"
            ],
```

```
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:cluster/cluster-name/cluster-id"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:*Topic*",
                "kafka-cluster:ReadData"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:topic/cluster-name/cluster-
id/topic-name"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "kafka-cluster:AlterGroup",
                "kafka-cluster:DescribeGroup"
            ],
            "Resource": [
                "arn:aws:kafka:us-east-1:{account-id}:group/cluster-name/*"
            ]
        }
    ]
}
```

Paso 2: crear la canalización

A continuación, puedes configurar una canalización de OpenSearch ingestión como la siguiente, en la que se especifica a Kafka como fuente:

```
version: "2"
log-pipeline:
  source:
    kafka:
      acknowledgements: true
      topics:
      - name: "topic-name"
        group_id: "group-id"
        serde_format: "json"/"plaintext"
      aws:
```

```
        msk:
          arn: "arn:aws:iam::{account-id}:role/cluster-role"
        region: "us-west-2"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      schema:                                # Optional
        type: "aws_glue"
  processor:
  - grok:
      match:
        log:
        - "%{COMMONAPACHELOG}"
  - date:
      destination: "@timestamp"
      from_time_received: true
  sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index: "index_name"
      aws_sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      aws_region: "us-east-1"
      aws_sigv4: true
```

Puede usar el esquema AWS-MSKPipeline para crear esta canalización. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

Paso 3: (opcional) Utilice el registro de esquemas AWS Glue

Al utilizar OpenSearch Ingestion con Amazon MSK, puede utilizar el formato de datos AVRO para los esquemas alojados en el registro de esquemas. AWS Glue Con AWS Glue Schema Registry, puede descubrir, controlar y evolucionar de forma centralizada los esquemas de flujo de datos.

Para usar esta opción, habilite el `type` de esquema en la configuración de su canalización:

```
schema:
  type: "aws_glue"
```

También debe proporcionar AWS Glue permisos de acceso de lectura en su rol de canalización. Puedes usar la política AWS gestionada llamada AWSGlueSchemaRegistryReadonlyAccess. Además, tu registro debe estar en la misma región Cuenta de AWS y en la misma región que tu canal OpenSearch de ingestión.

Paso 4: (opcional) configurar las unidades de cómputo (OCU) recomendadas para la canalización de Amazon MSK

Cada unidad de cómputo tiene un consumidor por tema. Los agentes equilibran las particiones entre estos consumidores para un tema determinado. Sin embargo, cuando el número de particiones es superior al número de consumidores, Amazon MSK aloja varias particiones en cada consumidor. OpenSearch Ingestion tiene un escalado automático incorporado para escalar hacia arriba o hacia abajo según el uso de la CPU o la cantidad de registros pendientes en proceso.

Para un rendimiento óptimo, distribuya las particiones entre varias unidades de cómputo para el procesamiento paralelo. Si los temas tienen un gran número de particiones (por ejemplo, más de 96, que es el número máximo de OCU por canalización), se recomienda configurar una canalización con 1–96 OCU. Esto se debe a que se escalará automáticamente según sea necesario. Si un tema tiene un número reducido de particiones (por ejemplo, menos de 96), mantenga la unidad de cómputo máxima igual a la cantidad de particiones.

Cuando una canalización tenga más de un tema, seleccione el tema con el mayor número de particiones como referencia para configurar las unidades de cómputo máximas. Al añadir otra canalización con un nuevo conjunto de OCU al mismo tema y grupo de consumidores, se puede escalar el rendimiento de forma casi lineal.

Uso de una canalización OpenSearch de ingestión con Amazon S3

Con OpenSearch Ingestion, puede utilizar Amazon S3 como origen o destino. Cuando utiliza Amazon S3 como fuente, envía datos a una canalización de OpenSearch ingestión. Cuando utiliza Amazon S3 como destino, escribe datos de una canalización de OpenSearch ingestión en uno o más buckets de S3.

Temas

- Amazon S3 como origen
- Amazon S3 como destino
- Cuenta cruzada de Amazon S3 como fuente

Amazon S3 como origen

Existen dos formas de utilizar Amazon S3 como origen para procesar datos: con el procesamiento S3-SQS y con análisis programados.

Utilice el procesamiento S3-SQS cuando necesite escanear los archivos casi en tiempo real una vez que se hayan escrito en S3. Puede configurar los buckets de Amazon S3 para que generen un evento cada vez que se almacene o modifique un objeto en el bucket. Utilice un escaneo programado único o recurrente para procesar por lotes los datos de un bucket de S3.

Temas

Requisitos previos

Para usar Amazon S3 como fuente de una canalización de OpenSearch ingestión tanto para un escaneo programado como para un procesamiento S3-SQS, cree primero un bucket de S3.

> **Note**
>
> Si el bucket de S3 utilizado como fuente en la canalización de OpenSearch ingestión se encuentra en otro Cuenta de AWS, también debe habilitar los permisos de lectura multicuenta en el bucket. Esto permite que la canalización lea y procese los datos. Para habilitar los permisos entre cuentas, consulte Propietario del bucket que concede permisos de bucket entre cuentas en la Guía del usuario de Amazon S3.
> Si tus buckets de S3 están en varias cuentas, usa un mapa. `bucket_owners` Para ver un ejemplo, consulte el acceso a S3 entre cuentas en la OpenSearch documentación.

Para configurar el procesamiento S3-SQS, también debe realizar los siguientes pasos:

1. Crear una cola de Amazon SQS.
2. Habilitar las notificaciones de eventos en el bucket de S3 con la cola SQS como destino.

Paso 1: configurar el rol de canalización

A diferencia de otros complementos de origen que envían datos a una canalización, el complemento de fuente de S3 tiene una arquitectura basada en lectura en la que la canalización extrae datos de la fuente.

Por lo tanto, para que una canalización pueda leer desde S3, debe especificar un rol dentro de la configuración de fuente de S3 de la canalización que tenga acceso tanto al bucket de S3 como a la cola de Amazon SQS. La canalización asumirá este rol para leer los datos de la cola.

> **Note**
>
> El rol que especifique en la configuración de fuente de S3 debe ser el rol de canalización. Por lo tanto, su rol de canalización debe contener dos políticas de permisos independientes: una para escribir en un receptor y otra para extraer de la fuente de S3. Debe usar el mismo `sts_role_arn` en todos los componentes de la canalización.

El siguiente ejemplo de política muestra los permisos necesarios para usar S3 como fuente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action":[
          "s3:ListBucket",
          "s3:GetBucketLocation",
          "s3:GetObject"
       ],
      "Resource": "arn:aws:s3:::my-bucket/*"
    },
    {
       "Effect":"Allow",
       "Action":"s3:ListAllMyBuckets",
       "Resource":"arn:aws:s3:::*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sqs:DeleteMessage",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility"
      ],
      "Resource": "arn:aws:sqs:us-west-2:{account-id}:MyS3EventSqsQueue"
    }
  ]
```

```
}
```

Debe adjuntar estos permisos al rol de IAM que especifique en la opción `sts_role_arn` dentro de la configuración del complemento de fuente de S3:

```
version: "2"
source:
  s3:
    ...
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Paso 2: crear la canalización

Una vez configurados los permisos, puede configurar una canalización de OpenSearch ingestión en función del caso de uso de Amazon S3.

Procesamiento S3-SQS

Para configurar el procesamiento S3-SQS, configure su canalización para especificar S3 como origen y configure las notificaciones de Amazon SQS:

```
version: "2"
s3-pipeline:
  source:
    s3:
      notification_type: "sqs"
      codec:
        newline: null
      sqs:
        queue_url: "https://sqs.us-east-1.amazonaws.com/{account-id}/ingestion-queue"
      compression: "none"
      aws:
        region: "us-east-1"
        # IAM role that the pipeline assumes to read data from the queue. This role
 must be the same as the pipeline role.
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

```
processor:
- grok:
    match:
      log:
      - "%{COMMONAPACHELOG}"
- date:
    destination: "@timestamp"
    from_time_received: true
sink:
- opensearch:
    hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
    index: "index-name"
    aws:
      # IAM role that the pipeline assumes to access the domain sink
      sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      region: "us-east-1"
```

Si observa un bajo uso de la CPU al procesar archivos pequeños en Amazon S3, considere la posibilidad de aumentar el rendimiento modificando el valor de la `workers` opción. Para obtener más información, consulte las opciones de configuración del complemento S3.

Escaneo programado

Para configurar un escaneo programado, configure su canalización con un cronograma a nivel de escaneo que se aplique a todos los buckets de S3 o a nivel de bucket. Una programación a nivel de bucket o una configuración de intervalos de escaneo siempre sobrescribe una configuración a nivel de escaneo.

Puede configurar los escaneos programados con un escaneo único, que es ideal para la migración de datos, o un escaneo periódico, que es ideal para el procesamiento por lotes.

Para configurar la canalización para que lea desde Amazon S3, utilice los blueprints de Amazon S3 denominados AWS-S3 o AWS-S3 ScanPipeline. ScanSchedulePipeline Puede editar la parte `scan` de la configuración de la canalización para adaptarla a sus necesidades de programación. Para más información, consulte the section called “Uso de esquemas para crear una canalización”.

Escaneo único

Un escaneo único programado se ejecuta una sola vez. En su configuración de YAML, puede usar una `start_time` y `end_time` para especificar cuándo quiere que se escaneen los objetos del bucket. O bien, puede usar un `range` para especificar el intervalo de tiempo en relación con la hora actual en el que desea que se escaneen los objetos del bucket.

Por ejemplo, un rango configurado para PT4H escanea todos los archivos creados en las últimas cuatro horas. Para configurar un escaneo único para que se ejecute por segunda vez, debe detener y reiniciar la canalización. Si no tiene un rango configurado, también debe actualizar las horas de inicio y finalización.

La siguiente configuración establece un escaneo único de todos los buckets y todos los objetos de esos buckets:

```
version: "2"
log-pipeline:
  source:
    s3:
      codec:
        csv:
      compression: "none"
      aws:
        region: "us-east-1"
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
      acknowledgments: true
      scan:
        buckets:
          - bucket:
              name: my-bucket-1
              filter:
                include_prefix:
                  - Objects1/
                exclude_suffix:
                  - .jpeg
                  - .png
          - bucket:
              name: my-bucket-2
              key_prefix:
                include:
                  - Objects2/
                exclude_suffix:
                  - .jpeg
                  - .png
      delete_s3_objects_on_read: false
  processor:
    - date:
        destination: "@timestamp"
        from_time_received: true
  sink:
```

```
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index-name"
        aws:
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
        dlq:
          s3:
            bucket: "my-bucket-1"
            region: "us-east-1"
            sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
```

La siguiente configuración establece un escaneo único de todos los buckets durante un período de tiempo específico. Esto significa que S3 procesa solo los objetos con tiempos de creación que se encuentran dentro de este período.

```
scan:
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

La siguiente configuración establece un escaneo único tanto a nivel de escaneo como a nivel del bucket. Las horas de inicio y finalización a nivel del bucket anulan las horas de inicio y finalización a nivel de escaneo.

```
scan:
```

```
  start_time: 2023-01-21T18:00:00.000Z
  end_time: 2023-04-21T18:00:00.000Z
  buckets:
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        start_time: 2023-01-21T18:00:00.000Z
        end_time: 2023-04-21T18:00:00.000Z
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Al detener una canalización, se elimina cualquier referencia preexistente de los objetos que la canalización escaneó antes de la parada. Si se detiene una sola canalización de escaneo, volverá a escanear todos los objetos una vez iniciada, incluso si ya estaban escaneados. Si necesita detener una sola canalización de escaneo, se recomienda cambiar el intervalo de tiempo antes de volver a iniciar la canalización.

Si necesitas filtrar los objetos por hora de inicio y hora de finalización, la única opción es detener e iniciar la canalización. Si no necesitas filtrar por hora de inicio y hora de finalización, puedes filtrar los objetos por nombre. Para filtrar por nombre no es necesario detener e iniciar la canalización. Para ello, usa `include_prefix` y. `exclude_suffix`

Escaneo periódico

Un escaneo periódico programado ejecuta un escaneo de los buckets de S3 especificados a intervalos regulares y programados. Solo puede configurar estos intervalos a nivel de escaneo, ya que no se admiten configuraciones individuales a nivel de bucket.

En la configuración de YAML, el `interval` especifica la frecuencia del escaneo periódico, que puede ser entre 30 segundos y 365 días. El primero de estos escaneos siempre se produce al crear la canalización. El `count` define el número total de instancias de escaneo.

La siguiente configuración establece un escaneo periódico, con un retraso de 12 horas entre los escaneos:

```
scan:
  scheduling:
    interval: PT12H
    count: 4
  buckets:
    - bucket:
        name: my-bucket-1
        filter:
          include:
            - Objects1/
          exclude_suffix:
            - .jpeg
            - .png
    - bucket:
        name: my-bucket-2
        filter:
          include:
            - Objects2/
          exclude_suffix:
            - .jpeg
            - .png
```

Amazon S3 como destino

Para escribir datos de una canalización de OpenSearch ingestión en un bucket de S3, utilice el esquema denominado AWS-S3 SinkLogPipeline para crear una canalización con un receptor de S3. Esta canalización dirige los datos selectivos a un OpenSearch sumidero y, al mismo tiempo, envía todos los datos para archivarlos en S3. Para obtener más información, consulte the section called "Uso de esquemas para crear una canalización".

Al crear el receptor de S3, puede especificar el formato que prefiera entre una variedad de códecs de receptor. Por ejemplo, si desea escribir datos en formato de columnas, seleccione el códec Parquet o Avro. Si prefiere un formato basado en filas, seleccione JSON o ND-JSON. Para escribir datos en

S3 en un esquema específico, también puede definir un esquema insertado dentro de los códecs de receptor usando el formato Avro.

El siguiente ejemplo define un esquema insertado en un receptor de S3:

```
- s3:
  codec:
    parquet:
      schema: >
        {
           "type" : "record",
           "namespace" : "org.vpcFlowLog.examples",
           "name" : "VpcFlowLog",
           "fields" : [
             { "name" : "version", "type" : "string"},
             { "name" : "srcport", "type": "int"},
             { "name" : "dstport", "type": "int"},
             { "name" : "start", "type": "int"},
             { "name" : "end", "type": "int"},
             { "name" : "protocol", "type": "int"},
             { "name" : "packets", "type": "int"},
             { "name" : "bytes", "type": "int"},
             { "name" : "action", "type": "string"},
             { "name" : "logStatus", "type" : "string"}
           ]
         }
```

Cuando defina este esquema, especifique un superconjunto de todas las claves que pueden estar presentes en los distintos tipos de eventos que su canalización envía a un receptor.

Por ejemplo, si en un evento existe la posibilidad de que falte una clave, añada esa clave al esquema con un valor `null`. Las declaraciones de valores nulos permiten que el esquema procese datos no uniformes (algunos eventos tienen estas claves y otros no). Cuando los eventos entrantes tienen estas claves presentes, sus valores se escriben en los receptores.

Esta definición de esquema actúa como un filtro que solo permite enviar las claves definidas a los receptores y elimina las claves indefinidas de los eventos entrantes.

También puede usar `include_keys` y `exclude_keys` en su receptor para filtrar los datos que se dirigen a otros receptores. Estos dos filtros se excluyen mutuamente, por lo que solo puede usar uno a la vez en su esquema. Además, no puede utilizarlos en esquemas definidos por el usuario.

Para crear canalizaciones con dichos filtros, utilice el AWSSinkFilterWithSchemaPipelineesquema. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

Cuenta cruzada de Amazon S3 como fuente

Puede conceder acceso a todas las cuentas con Amazon S3 para que las canalizaciones de OpenSearch ingestión puedan acceder a los buckets de S3 de otra cuenta como fuente. La siguiente configuración de YAML permite el acceso de todas las cuentas a un bucket de Amazon S3 como fuente:

```
s3-pipeline:
 source:
  s3:
   notification_type: "sqs"
   codec:
    csv:
     delimiter: ","
     quote_character: "\""
     detect_header: True
   sqs:
    queue_url: "https://sqs.ap-northeast-1.amazonaws.com/401447383613/test-s3-queue"
   bucket_owners:
    user-role-1234567890: 1234567890 # User1
    user-role-12345678891: 1234567891 # User2
   compression: "gzip"
```

Uso de una canalización de OpenSearch ingestión con Amazon Security Lake

Puede usar el complemento fuente de S3 para incorporar datos de Amazon Security Lake a su canalización de OpenSearch ingestión. Security Lake centraliza automáticamente los datos de seguridad de los AWS entornos, los entornos locales y los proveedores de SaaS en un lago de datos diseñado específicamente. Puede crear una suscripción que replique los datos de Security Lake en su canal de OpenSearch ingestion y, a continuación, los guarde en su dominio de servicio o en su colección Serverless. OpenSearch OpenSearch

Para configurar su canalización para que lea desde Security Lake, utilice el blueprint de Security Lake denominado AWS- SecurityLake S3ParquetoCSFPipeline. El esquema incluye una configuración predeterminada para incorporar los archivos Parquet de Open Cybersecurity Schema

Framework (OCSF) de Security Lake. Para más información, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

Requisitos previos

Antes de crear la canalización de ingestión, lleve a cabo los siguientes OpenSearch pasos:

- Habilitar Security Hub.
- Crear un suscriptor en Security Lake.
  - Seleccione las fuentes que quiere incorporar a su canalización.
  - En el caso de las Credenciales de suscriptor, añada el ID de la Cuenta de AWS donde desea crear la canalización. Para el ID externo, especifique `OpenSearchIngestion-{accountid}`.
  - Para el Método de acceso a los datos, seleccione S3.
  - Para los Detalles de notificación, seleccione Cola de SQS.

Al crear un suscriptor, Security Lake crea automáticamente dos políticas de permisos insertadas: una para S3 y otra para SQS. Las políticas adoptan el siguiente formato: `AmazonSecurityLake-{12345}-S3` y `AmazonSecurityLake-{12345}-SQS`. Para permitir que su canalización acceda a las fuentes del suscriptor, debe asociar los permisos necesarios a su rol de canalización.

Paso 1: configurar el rol de canalización

Cree una nueva política de permisos en IAM que combine solo los permisos necesarios de las dos políticas que Security Lake creó automáticamente. El siguiente ejemplo de política muestra los privilegios mínimos necesarios para que una canalización de OpenSearch ingestión lea datos de varias fuentes de Security Lake:

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

```
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/
LAMBDA_EXECUTION/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/S3_DATA/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/VPC_FLOW/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/ROUTE53/1.0/*",
            "arn:aws:s3:::aws-security-data-lake-{region}-abcde/aws/SH_FINDINGS/1.0/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "sqs:ReceiveMessage",
            "sqs:DeleteMessage"
         ],
         "Resource":[
            "arn:aws:sqs:{region}:{account-id}:AmazonSecurityLake-abcde-Main-Queue"
         ]
      }
   ]
}
```

> **Important**
>
> Security Lake no administra la política de roles de canalización por usted. Si agrega o elimina fuentes de su suscripción de Security Lake, debe actualizar la política manualmente. Security Lake crea particiones para cada fuente de registro, por lo que debe agregar o eliminar manualmente los permisos en el rol de canalización.

Debe adjuntar estos permisos al rol de IAM que especifique en la opción `sts_role_arn` incluida en la configuración del complemento fuente de S3, en `sqs`.

```
version: "2"
source:
  s3:
    ...
```

```
    sqs:
      queue_url: "https://sqs.{region}.amazonaws.com/{account-id}/
AmazonSecurityLake-abcde-Main-Queue"
    aws:
      ...
      sts_role_arn: arn:aws:iam::{account-id}:role/pipeline-role
processor:
  ...
sink:
  - opensearch:
      ...
```

Paso 2: crear la canalización

Después de añadir los permisos a la función de canalización, utilice el blueprint AWS- SecurityLake S3ParquetoCSFPipeline para crear la canalización. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

Debe especificar la opción `queue_url` en la configuración fuente de `s3`, que es la URL de la cola de Amazon SQS desde la que debe leerse. Para formatear la URL, localice el Punto de conexión de la suscripción en la configuración del suscriptor y cambie `arn:aws:` a `https://`. Por ejemplo, `https://sqs.{region}.amazonaws.com/{account-id}/AmazonSecurityLake-abdcef-Main-Queue`.

El `sts_role_arn` que especifica en la configuración de fuente de S3 debe ser el ARN del rol de canalización.

Uso de una canalización de ingestión con Fluent Bit OpenSearch

Este ejemplo de archivo de configuración de Fluent Bit envía los datos de registro de Fluent Bit a una canalización OpenSearch de ingestión. Para más información sobre la ingesta de datos de registro, consulte Log Analytics en la documentación de Data Prepper.

Tenga en cuenta lo siguiente:

- El valor `host` debe ser el punto de conexión de su canalización. Por ejemplo, *`pipeline-endpoint`*`.us-east-1.osis.amazonaws.com`.
- El valor `aws_service` debe ser `osis`.
- El `aws_role_arn` valor es el ARN de la función de AWS IAM que el cliente debe asumir y utilizar para la autenticación de la versión 4 de Signature.

```
[INPUT]
  name                tail
  refresh_interval    5
  path                /var/log/test.log
  read_from_head      true

[OUTPUT]
  Name http
  Match *
  Host pipeline-endpoint.us-east-1.osis.amazonaws.com
  Port 443
  URI /log/ingest
  Format json
  aws_auth true
  aws_region us-east-1
  aws_service osis
  aws_role_arn arn:aws:iam::{account-id}:role/ingestion-role
  Log_Level trace
  tls On
```

A continuación, puede configurar una canalización de OpenSearch ingestión como la siguiente, que tiene HTTP como origen:

```
version: "2"
unaggregated-log-pipeline:
  source:
    http:
      path: "/log/ingest"
  processor:
    - grok:
        match:
          log:
            - "%{TIMESTAMP_ISO8601:timestamp} %{NOTSPACE:network_node}
 %{NOTSPACE:network_host} %{IPORHOST:source_ip}:%{NUMBER:source_port:int} ->
 %{IPORHOST:destination_ip}:%{NUMBER:destination_port:int} %{GREEDYDATA:details}"
    - grok:
        match:
          details:
            - "'%{NOTSPACE:http_method} %{NOTSPACE:http_uri}' %{NOTSPACE:protocol}"
            - "TLS%{NOTSPACE:tls_version} %{GREEDYDATA:encryption}"
            - "%{NUMBER:status_code:int} %{NUMBER:response_size:int}"
    - delete_entries:
        with_keys: ["details", "log"]
```

```
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index: "index_name"
        index_type: custom
        bulk_size: 20
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

Uso de una canalización OpenSearch de ingestión con Collector OpenTelemetry

Este archivo de OpenTelemetry configuración de ejemplo exporta los datos de rastreo del OpenTelemetry recopilador y los envía a una canalización OpenSearch de ingestión. Para más información sobre la ingesta de datos de rastreo, consulte Trace Analytics en la documentación de Data Prepper.

Tenga en cuenta lo siguiente:

- El valor `endpoint` debe incluir el punto de conexión de la canalización. Por ejemplo, `https://pipeline-endpoint.us-east-1.osis.amazonaws.com`.
- El valor `service` debe ser `osis`.
- La `compression` opción del exportador OTLP/HTTP debe coincidir con la `compression` opción de la fuente de la canalización. OpenTelemetry

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
```

```
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/v1/traces"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

A continuación, puede configurar una canalización OpenSearch de ingestión como la siguiente, que especifica el complemento de rastreo Otel como fuente:

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
      path: "/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace-pipeline"
    - pipeline:
        name: "service-map-pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
```

```
source:
  pipeline:
    name: "otel-trace-pipeline"
processor:
  - service_map:
sink:
  - opensearch:
      hosts: ["https://search-domain-endpoint.us-east-1.es.amazonaws.com"]
      index_type: trace-analytics-service-map
      aws:
        # IAM role that the pipeline assumes to access the domain sink
        sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
        region: "us-east-1"
```

Para ver otro ejemplo de canalización, consulte el esquema de Canalización de Trace Analytics. Para más información, consulte the section called “Uso de esquemas para crear una canalización”.

Siguientes pasos

Tras exportar los datos a una canalización, puede consultarlos desde el dominio de OpenSearch servicio que está configurado como receptor de la canalización. Los siguientes recursos pueden ayudarle a comenzar:

- Observabilidad
- the section called “Análisis de seguimiento”
- the section called “Lenguaje de procesamiento de canalizaciones”

Migración de datos entre dominios y colecciones mediante Amazon OpenSearch Ingestion

Puedes usar las canalizaciones OpenSearch de ingestión para migrar datos entre dominios de Amazon OpenSearch Service o colecciones de VPC OpenSearch sin servidor. Para ello, debe configurar una canalización en la que configura un dominio o colección como origen y otro dominio o colección como receptor. Esto migra eficazmente los datos de un dominio o colección a otro.

Para migrar datos, debe disponer de los siguientes recursos:

- Un dominio de OpenSearch servicio de origen o una colección de VPC OpenSearch sin servidor. Este dominio o colección contiene los datos que deseas migrar. Si usas un dominio, debe ejecutar

la OpenSearch versión 1.0 o posterior, o Elasticsearch, la versión 7.4 o posterior. El dominio también debe tener una política de acceso que otorgue los permisos adecuados para tu rol de canalización.

- Un dominio o colección de VPC independiente al que desee migrar sus datos. Este dominio o colección actuará como colector de canalización.
- Una función de canalización que OpenSearch Ingestion utilizará para leer y escribir en tu colección o dominio. Debe incluir el nombre de recurso de Amazon (ARN) de este rol en la configuración de la canalización. Para obtener más información, consulte los siguientes recursos:
  - the section called “Otorgar a Pipelines acceso a los dominios”
  - the section called “Otorgar a las canalizaciones acceso a las colecciones”

Temas

Limitaciones

Cuando designa dominios de OpenSearch servicio o colecciones OpenSearch sin servidor como receptores, se aplican las siguientes limitaciones:

- Una canalización no puede escribir en más de un dominio de VPC.
- Solo puede migrar datos hacia o desde colecciones OpenSearch sin servidor que utilicen el acceso a la VPC. No se admiten las colecciones públicas.
- No puedes especificar una combinación de dominios públicos y de VPC en una única configuración de canalización.
- Puedes tener un máximo de 20 receptores que no sean de canalización en una sola configuración de canalización.
- Puedes especificar sumideros a partir de un máximo de tres diferentes Regiones de AWS en una sola configuración de canalización.
- Una canalización con varios sumideros puede experimentar una reducción de la velocidad de procesamiento con el tiempo si alguno de los sumideros permanece inactivo durante demasiado tiempo o si no cuenta con la capacidad suficiente para recibir los datos entrantes.

OpenSearch El servicio como fuente

El dominio o la colección que especifique como fuente es desde donde se migran los datos.

Creación de un rol de canalización en IAM

Para crear tu canalización de OpenSearch ingestión, primero debes crear una función de canalización que permita el acceso de lectura y escritura entre dominios o colecciones. Para ello, siga estos pasos:

1. Crea una nueva política de permisos en IAM para asociarla a la función de canalización. Asegúrese de permitir que los permisos lean desde la fuente y escriban en el receptor. Para obtener más información sobre cómo configurar los permisos de canalización de IAM para los dominios de OpenSearch servicio, consulte the section called “Otorgar a Pipelines acceso a los dominios” ythe section called “Otorgar a las canalizaciones acceso a las colecciones”.
2. Especifique los siguientes permisos dentro de la función de canalización para leer desde la fuente:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"es:ESHttpGet",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_cat/indices",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search"
         ]
      },
      {
         "Effect":"Allow",
         "Action":"es:ESHttpPost",
         "Resource":[
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/
point_in_time",
            "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/*/_search/scroll"
         ]
      },
      {
         "Effect":"Allow",
```

```
            "Action":"es:ESHttpDelete",
            "Resource":[
               "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/
point_in_time",
               "arn:aws:es:us-east-1:{account-id}:domain/{domain-name}/_search/scroll"
            ]
         }
      ]
}
```

Creación de una canalización

Después de adjuntar la política a la función de canalización, utilice el esquema de AWSOpenSearchDataMigrationPipelinemigración para crear la canalización. Este esquema incluye una configuración predeterminada para migrar datos entre dominios o colecciones OpenSearch de servicios. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

> **Note**
>
> OpenSearch Ingestion utiliza la versión y la distribución del dominio de origen para determinar qué mecanismo utilizar para la migración. Algunas versiones admiten `point_in_time` esta opción. OpenSearch Serverless usa la `search_after` opción porque no admite `point_in_time` o`scroll`.

Es posible que se estén creando nuevos índices durante el proceso de migración o que los documentos se estén actualizando mientras la migración está en curso. Por este motivo, es posible que deba escanear uno o varios escaneos de los datos del índice de su dominio para recoger datos nuevos o actualizados.

Especifique el número de escaneos que se van a ejecutar el configurar `index_read_count` y `interval` en la canalización. El siguiente de ejemplo muestra cómo realizar varios escaneos:

```
scheduling:
    interval: "PT2H"
    index_read_count: 3
    start_time: "2023-06-02T22:01:30.00Z"
```

OpenSearch Ingestion usa la siguiente configuración para garantizar que los datos se escriban en el mismo índice y mantengan el mismo ID de documento:

```
index: "${getMetadata(\"opensearch-index\")}"
document_id: "${getMetadata(\"opensearch-document_id\")}"
```

Especificar varios sumideros OpenSearch de dominio de servicio

Puede especificar varios dominios de OpenSearch servicio público como destinos de sus datos. Puede utilizar esta capacidad para realizar un enrutamiento condicional o replicar los datos entrantes en varios dominios OpenSearch de servicio. Puede especificar hasta 10 dominios de OpenSearch servicio público diferentes como receptores.

En el siguiente ejemplo, los datos entrantes se enrutan condicionalmente a diferentes OpenSearch dominios de servicio:

```
...
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        hosts: [ "https://search-response-2xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-2xx"
        routes:
          - 2xx_status
    - opensearch:
        hosts: [ "https://search-response-5xx.us-east-1.es.amazonaws.com" ]
        aws:
          sts_role_arn: "arn:aws:iam::123456789012:role/Example-Role"
          region: "us-east-1"
        index: "response-5xx"
        routes:
          - 5xx_status
```

Migración de datos a una colección de OpenSearch VPC sin servidor

Puede usar OpenSearch Ingestión para migrar datos de un dominio de OpenSearch servicio de origen o de una colección OpenSearch sin servidor a un receptor de recopilación de VPC. Debes proporcionar una política de acceso a la red en la configuración de la canalización. Para obtener más información sobre la ingesta de datos en colecciones de OpenSearch VPC sin servidor, consulte. the section called “Tutorial: incorporar datos en una colección”

Para migrar datos a una colección de VPC

1. Cree una colección OpenSearch sin servidor. Para ver instrucciones, consulte the section called “Tutorial: incorporar datos en una colección”.
2. Cree una política de red para la colección que especifique el acceso a la VPC tanto para el punto de conexión de la colección como para el punto de conexión de Dashboards. Para ver instrucciones, consulte the section called “Acceso a la red”.
3. Cree el rol de canalización si todavía no tiene uno. Para ver instrucciones, consulte the section called “Rol de canalización”.
4. Cree la canalización. Para obtener instrucciones, consulte the section called “Uso de esquemas para crear una canalización”.

Utilizar SDK de AWS para interactuar con Amazon OpenSearch Ingestion

En esta sección, se incluye un ejemplo de cómo utilizar los SDK de AWS para interactuar con Amazon OpenSearch Ingestion. El ejemplo de código muestra cómo crear un dominio y una canalización y, a continuación, incorporar datos a la canalización.

Temas

- Python

Python

En el siguiente script de ejemplo, se utiliza AWS SDK for Python (Boto3) para crear un rol de canalización de IAM, un dominio en el que escribir datos y una canalización a través de la cual se incorporan datos. A continuación, ingrese un archivo de registro de muestra en la canalización mediante la biblioteca HTTP `requests`.

Ejecute los siguientes comandos para asegurarse de que dispone de todas las dependencias necesarias:

```
pip install boto3
pip install botocore
pip install requests
pip install requests-auth-aws-sigv4
```

En el script, sustituya los ID de cuenta de las políticas de acceso por su ID de Cuenta de AWS. También puede modificar opcionalmente el archivo `region`.

```
import boto3
import botocore
from botocore.config import Config
import requests
from requests_auth_aws_sigv4 import AWSSigV4
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

opensearch = boto3.client('opensearch', config=my_config)
iam = boto3.client('iam', config=my_config)
osis = boto3.client('osis', config=my_config)

domainName = 'test-domain'  # The name of the domain
pipelineName = 'test-pipeline' # The name of the pipeline

def createPipelineRole(iam, domainName):
    """Creates the pipeline role"""
    response = iam.create_policy(
        PolicyName='pipeline-policy',
        PolicyDocument=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect
\":\"Allow\",\"Action\":\"es:DescribeDomain\",\"Resource\":\"arn:aws:es:us-
east-1:123456789012:domain\/{domainName}\"}},{{\"Effect\":\"Allow\",\"Action\":
\"es:ESHttp*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/{domainName}\/*
\"}}]}}'
```

```
    )
    policyarn = response['Policy']['Arn']

    response = iam.create_role(
        RoleName='PipelineRole',
        AssumeRolePolicyDocument='{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect
\":\"Allow\",\"Principal\":{\"Service\":\"osis-pipelines.amazonaws.com\"},\"Action\":
\"sts:AssumeRole\"}]}'
    )
    rolename=response['Role']['RoleName']

    response = iam.attach_role_policy(
        RoleName=rolename,
        PolicyArn=policyarn
    )

    print('Creating pipeline role...')
    time.sleep(10)
    print('Role created: ' + rolename)

def createDomain(opensearch, domainName):
    """Creates a domain to ingest data into"""
    response = opensearch.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_2.3',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies=f'{{\"Version\":\"2012-10-17\",\"Statement\":[{{\"Effect\":
\"Allow\",\"Principal\":{{\"AWS\":\"arn:aws:iam::123456789012:role\/PipelineRole
\"}},\"Action\":\"es:*\",\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain\/
{domainName}\/*\"}}]}}',
        NodeToNodeEncryptionOptions={
            'Enabled': True
```

```
        }
    )
    return(response)

def waitForDomainProcessing(opensearch, domainName):
    """Waits for the domain to be active"""
    try:
        response = opensearch.describe_domain(
            DomainName=domainName
        )
        # Every 30 seconds, check whether the domain is processing.
        while 'Endpoint' not in response['DomainStatus']:
            print('Creating domain...')
            time.sleep(60)
            response = opensearch.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is ready for ingestion.
        endpoint = response['DomainStatus']['Endpoint']
        print('Domain endpoint ready to receive data: ' + endpoint)
        createPipeline(osis, endpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found.')
        else:
            raise error

def createPipeline(osis, endpoint):
    """Creates a pipeline using the domain and pipeline role"""
    try:
        definition = f'version: \"2\"\nlog-pipeline:\n  source:\n    http:\n      path:
 \"/${{pipelineName}}/logs\"\n  processor:\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://{endpoint}\" ]\n        index: \"application_logs\"\n        aws:\n
     sts_role_arn: \"arn:aws:iam::123456789012:role/PipelineRole\"\n          region:
 \"us-east-1\"'
        response = osis.create_pipeline(
            PipelineName=pipelineName,
            MinUnits=4,
            MaxUnits=9,
            PipelineConfigurationBody=definition
        )
```

```
        response = osis.get_pipeline(
                PipelineName=pipelineName
        )

        # Every 30 seconds, check whether the pipeline is active.
        while response['Pipeline']['Status'] == 'CREATING':
            print('Creating pipeline...')
            time.sleep(30)
            response = osis.get_pipeline(
                PipelineName=pipelineName)

        # Once we exit the loop, the pipeline is ready for ingestion.
        ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
        print('Pipeline ready to ingest data at endpoint: ' + ingestionEndpoint)
        ingestData(ingestionEndpoint)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceAlreadyExistsException':
            print('Pipeline already exists.')
            response = osis.get_pipeline(
                PipelineName=pipelineName
            )
            ingestionEndpoint = response['Pipeline']['IngestEndpointUrls'][0]
            ingestData(ingestionEndpoint)
        else:
            raise error


def ingestData(ingestionEndpoint):
    """Ingests a sample log file into the pipeline"""
    endpoint = 'https://' + ingestionEndpoint
    r = requests.request('POST', f'{endpoint}/log-pipeline/logs',

 data='[{"time":"2014-08-11T11:40:13+00:00","remote_addr":"122.226.223.69","status":"404","requ
 http://www.k2proxy.com//hello.html HTTP/1.1","http_user_agent":"Mozilla/4.0
 (compatible; WOW64; SLCC2;)"}]',
    auth=AWSSigV4('osis'))
    print('Ingesting sample log file into pipeline')
    print('Response: ' + r.text)

def main():
    createPipelineRole(iam, domainName)
    createDomain(opensearch, domainName)
    waitForDomainProcessing(opensearch, domainName)
```

```
if __name__ == "__main__":
    main()
```

Casos de uso de Amazon OpenSearch Ingestion

En este capítulo, se indican algunos casos de uso frecuentes de Amazon OpenSearch Ingestion. Esta lista no es exhaustiva. Para conocer todas las capacidades de cada complemento compatible, consulte Fuentes, Procesadores y Receptores en la documentación de Data Prepper.

Temas

- El patrón de Grok coincide con Amazon OpenSearch Ingestion
- Enriquecimiento de registros con Amazon OpenSearch Ingestion
- Agregado de eventos con Amazon OpenSearch Ingestion
- Obtener métricas a partir de registros con Amazon OpenSearch Ingestion
- Trace Analytics con Amazon OpenSearch Ingestion
- Obtener métricas a partir de trazas con Amazon OpenSearch Ingestion
- Detección de anomalías con Amazon OpenSearch Ingestion
- Muestreo con Amazon OpenSearch Ingestion
- Descarga selectiva con Amazon OpenSearch Ingestion

El patrón de Grok coincide con Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion ofrece capacidades de coincidencia de patrones con el procesador Grok. El procesador Grok se basa en la biblioteca de `java-grok` y es compatible con todos los patrones compatibles. La biblioteca de `java-grok` se crea utilizando la biblioteca de expresiones regulares de `java.util.regex`.

Puede añadir patrones personalizados a sus canalizaciones mediante la opción `patterns_definitions`. Al depurar patrones personalizados, el depurador Grok puede resultar útil.

Además de estos ejemplos, también puede utilizar el esquema de canalización de registros de Apache. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

Uso básico

Para empezar con la coincidencia de patrones, cree la siguiente canalización:

```
version: "2"
patten-matching-pipeline:
  source
    ...
  processor:
    - grok:
        match:
          message: ['%{IPORHOST:clientip} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
  sink:
    - opensearch:
        # Provide an OpenSearch Service domain endpoint
        # Enable the 'serverless' flag if the sink is an OpenSearch Serverless
 collection
        aws:
          ...
        index: "metrics_for_traces"
        # serverless: true
```

Un mensaje entrante a la canalización puede tener el siguiente contenido:

```
{"message": "127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200"}
```

La canalización localizará el valor en la clave de `message` de cada evento entrante e intentará que coincida con el patrón. Las palabras clave `IPORHOST` `HTTPDATE` y `NUMBER` están integradas en el complemento.

Cuando un registro entrante coincide con el patrón, genera un evento interno como el siguiente, con claves de identificación extraídas del mensaje original.

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "response_status":200,
  "clientip":"198.126.12",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

La configuración `match` del procesador Grok especifica qué claves de un registro deben coincidir con qué patrones.

En el siguiente ejemplo, la configuración de coincidencia comprueba si hay una clave de `message` en los registros entrantes. Si la clave existe, compara el valor de la clave con el patrón de `SYSLOGBASE` y, después, con el patrón de `COMMONAPACHELOG`. A continuación, comprueba los registros en busca de una clave de `timestamp`. Si esa clave existe, intenta hacer coincidir el valor de la clave con el patrón de `TIMESTAMP_ISO8601`.

```
processor:
  - grok:
      match:
        message: ['%{SYSLOGBASE}', "%{COMMONAPACHELOG}"]
        timestamp: ["%{TIMESTAMP_ISO8601}"]
```

De forma predeterminada, el complemento continúa hasta que encuentre una coincidencia correcta. Por ejemplo, si hay una coincidencia correcta con el valor de la clave de `message` de un patrón `SYSLOGBASE`, el complemento no intentará hacer coincidir los demás patrones. Si quiere hacer coincidir los registros con todos los patrones, incluya la opción `break_on_match`.

Incluyendo capturas con nombre y vacías

Incluya la opción `keep_empty_captures` en la configuración de su canalización para incluir capturas nulas o la opción `named_captures_only` para incluir solo las capturas con nombre. Las capturas con nombre siguen el patrón `%{SYNTAX:SEMANTIC}`, mientras que las capturas sin nombre siguen el patrón `%{SYNTAX}`.

Por ejemplo, puede modificar la configuración de Grok anterior para eliminar `clientip` del patrón `%{IPORHOST}`:

```
processor:
  - grok:
      match:
        message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
```

El registro grokked resultante será como el siguiente:

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "response_status":200,
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Observe que la clave de `clientip` ya no existe, porque el patrón `%{IPORHOST}` ahora es una captura sin nombre.

Sin embargo, si establece `named_captures_only` para `false`:

```
processor:
  - grok:
      match:
        named_captures_only: false
        message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\] %{NUMBER:message:int}']
```

El registro grokked resultante será como el siguiente:

```
{
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "MONTH":"Oct",
  "YEAR":"2000",
  "response_status":200,
  "HOUR":"13",
  "TIME":"13:55:36",
  "MINUTE":"55",
  "SECOND":"36",
  "IPORHOST":"198.126.12",
  "MONTHDAY":"10",
  "INT":"-0700",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Tenga en cuenta que la captura `IPORHOST` ahora aparece como una nueva clave, junto con algunas capturas internas sin nombre, como `MONTH` y `YEAR`. La palabra clave `HTTPDATE` está usando estos patrones, que puede ver en el archivo de patrones predeterminado.

Sobrescribir las claves

Incluya la opción `keys_to_overwrite` para especificar qué claves existentes de un registro se sobrescribirán si hay una captura con el mismo valor de clave.

Por ejemplo, puede modificar la configuración de grok anterior para reemplazar `%{NUMBER:response_status:int}` con `%{NUMBER:message:int}` y añadir `message` a la lista de claves que se van a sobrescribir.

```
processor:
  - grok:
      match:
        keys_to_overwrite: ["message"]
        message: ['%{IPORHOST:clientip} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:message:int}']
```

En el registro grokked resultante, el mensaje original se sobrescribe con el número 200.

```
{
  "message":200,
  "clientip":"198.126.12",
  "timestamp":"10/Oct/2000:13:55:36 -0700"
}
```

Uso de patrones personalizados

Incluya la opción `pattern_definitions` en la configuración de grok para especificar patrones personalizados.

La siguiente configuración crea patrones de expresiones regulares personalizados denominados `CUSTOM_PATTERN-1` y `CUSTOM_PATTERN-2`. De forma predeterminada, el complemento continúa hasta que encuentre una coincidencia correcta.

```
processor:
  - grok:
      pattern_definitions:
        CUSTOM_PATTERN_1: 'this-is-regex-1'
```

```
        CUSTOM_PATTERN_2: '%{CUSTOM_PATTERN_1} REGEX'
      match:
        message: ["%{CUSTOM_PATTERN_2:my_pattern_key}"]
```

Si especifica `break_on_match` como `false`, la canalización intentará hacer coincidir todos los patrones y extraer las claves de los eventos entrantes:

```
processor:
  - grok:
      pattern_definitions:
        CUSTOM_PATTERN_1: 'this-is-regex-1'
        CUSTOM_PATTERN_2: 'this-is-regex-2'
        CUSTOM_PATTERN_3: 'this-is-regex-3'
        CUSTOM_PATTERN_4: 'this-is-regex-4'
      match:
        message: [ "%{PATTERN1}”, "%{PATTERN2}" ]
        log: [ "%{PATTERN3}", "%{PATTERN4}" ]
        break_on_match: false
```

Puede definir sus propios patrones personalizados para usarlos en la coincidencia de patrones en las canalizaciones. En el ejemplo anterior, se extraerá `my_pattern` después de hacer coincidir los patrones personalizados.

Almacenar las capturas con una clave principal

Incluya la opción `target_key` en su configuración de grok para agrupar todas las capturas de un registro en un valor clave externo adicional.

Por ejemplo, puede modificar la configuración de grok anterior para añadir una clave de destino denominada `grokked`.

```
processor:
   - grok:
       target_key: "grok"
       match:
         message: ['%{IPORHOST} \[%{HTTPDATE:timestamp}\]
 %{NUMBER:response_status:int}']
```

El registro grokked resultante será como el siguiente:

```
{
```

```
  "message":"127.0.0.1 198.126.12 [10/Oct/2000:13:55:36 -0700] 200",
  "grokked": {
     "response_status":200,
     "clientip":"198.126.12",
     "timestamp":"10/Oct/2000:13:55:36 -0700"
  }
}
```

Enriquecimiento de registros con Amazon OpenSearch Ingestion

Puede realizar distintos tipos de enriquecimiento de registros con Amazon OpenSearch Ingestion. Además de estos ejemplos, también puede utilizar el esquema de canalización de registros genérica. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

Filtrado

Utilice el procesador de Eventos de descarte para filtrar eventos de registro específicos antes de enviarlos a un receptor. Por ejemplo, supongamos que está recopilando registros de solicitudes web y solo desea almacenar las solicitudes fallidas. Se crea la siguiente canalización, que descarta las solicitudes en las que la respuesta es inferior a 400, de modo que solo quedan registrados los eventos con códigos de estado HTTP 400 o superiores.

```
version: "2"
log-pipeline:
  source:
  ...
  processor:
    - grok:
```

```
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - drop:
        drop_when: "/response < 400"
  sink:
    - opensearch:
        ...
        index: failure_logs
```

La opción `drop_when` especifica qué eventos se descartarán de la canalización.

Extracción de pares clave-valor de cadenas

A menudo, los datos de registro incluyen cadenas de pares clave-valor. Un escenario común es una cadena de consulta HTTP. Por ejemplo, si un usuario web consulta una URL paginable, los registros HTTP pueden tener la siguiente cadena de consulta HTTP:

```
page=3&q=my-search-term
```

Para realizar un análisis mediante los términos de búsqueda, puede extraer el valor de q de una cadena de consulta. El procesador de Valores clave ofrece un soporte sólido para extraer claves y valores de cadenas.

El siguiente ejemplo combina los procesadores `split_string` y `key_value` para extraer los parámetros de consulta de una línea de registro de Apache:

```
version: "2"
pipeline
 ...
  processor:
    - grok:
      match:
        message: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - split_string:
      entries:
        - source: request
          delimiter: "?"
    - key_value:
      source: "/request/1"
      field_split_characters: "&"
      value_split_characters: "="
```

```
      destination: query_params
```

Mutación de eventos

Los diferentes procesadores de Mutar evento permiten renombrar, copiar, añadir y eliminar entradas de eventos.

En este ejemplo, el primer procesador establece el valor de la clave de `debug` en `true` si la clave ya existe en el evento. El segundo procesador solo establece la clave de `debug` en `true` si la clave no existe en el caso, porque `overwrite_if_key_exists` está configurada en `true`.

```
...
processor:
  - add_entries:
    entries:
    - key: "debug"
      value: true
...
processor:
  - add_entries:
    entries:
    - key: "debug"
      value: true
      overwrite_if_key_exists: true
...
```

También puede utilizar una cadena de formato para crear nuevas entradas a partir de entradas existentes. Por ejemplo, `${date}-${time}` creará una nueva entrada basada en los valores de las entradas existentes `date` y `time`.

Por ejemplo, la siguiente canalización agrega nuevas entradas de eventos de forma dinámica a partir de eventos existentes:

```
processor:
  - add_entries:
    entries:
    - key: "key_three"
      format: "${key_one}-${key_two}
```

Por ejemplo, considere el siguiente evento de entrada:

```
{
   "key_one": "value_one",
   "key_two": "value_two"
}
```

El procesador lo transforma en un evento con un `key_three` con una clave nueva, que combina los valores de otras claves del evento original.

```
{
   "key_one": "value_one",
   "key_two": "value_two",
   "key_three": "value_one-value_two"
}
```

Mutación de cadenas

Los distintos procesadores de Mutar cadena ofrecen herramientas para manipular las cadenas de los datos entrantes. Por ejemplo, si necesita dividir una cadena en una matriz, utilice el procesador `split_string`:

```
...
processor:
  - split_string:
    entries:
    - source: "message"
      delimiter: "&"
...
```

El procesador transformará una cadena como, por ejemplo, `a&b&c` en `["a", "b", "c"]`.

Convertir listas en mapas

El procesador Lista a mapa, que es uno de los procesadores de Mutar eventos, convierte una lista de objetos de un evento en un mapa.

Por ejemplo, considere la siguiente configuración del procesador:

```
...
processor:
    - list_to_map:
```

```
        key: "name"
        source: "A-car-as-list"
        target: "A-car-as-map"
        value_key: "value"
        flatten: true
...
```

Este procesador convertirá un evento que contenga una lista de objetos como la siguiente:

```
{
  "A-car-as-list": [
    {
      "name": "make",
      "value": "tesla"
    },
    {
      "name": "model",
      "value": "model 3"
    },
    {
      "name": "color",
      "value": "white"
    }
  ]
}
```

En un mapa:

```
{
  "A-car-as-map": {
    "make": "tesla",
    "model": "model 3",
    "color": "white"
  }
}
```

Como otro ejemplo, suponga que tiene un evento entrante con la siguiente estructura:

```
{
  "mylist" : [
    {
      "somekey" : "a",
```

```
      "somevalue" : "val-a1",
      "anothervalue" : "val-a2"
    },
    {
      "somekey" : "b",
      "somevalue" : "val-b1",
      "anothervalue" : "val-b2"
    },
    {
      "somekey" : "b",
      "somevalue" : "val-b3",
      "anothervalue" : "val-b4"
    },
    {
      "somekey" : "c",
      "somevalue" : "val-c1",
      "anothervalue" : "val-c2"
    }
  ]
}
```

Puede definir las siguientes opciones en la configuración del procesador:

```
...
processor:
    - list_to_map:
        key: "somekey"
        source: "mylist"
        target: "myobject"
        value_key: "value"
        flatten: true
...
```

El procesador modifica el evento eliminando `mylist` y añadiendo el nuevo objeto `myobject`:

```
{
  "myobject" : {
    "a" : [
      {
        "somekey" : "a",
        "somevalue" : "val-a1",
        "anothervalue" : "val-a2"
      }
```

```
    ],
    "b" : [
      {
        "somekey" : "b",
        "somevalue" : "val-b1",
        "anothervalue" : "val-b2"
      },
      {
        "somekey" : "b",
        "somevalue" : "val-b3",
        "anothervalue" : "val-b4"
      }
    "c" : [
      {
        "somekey" : "c",
        "somevalue" : "val-c1",
        "anothervalue" : "val-c2"
      }
    ]
  }
}
```

En muchos casos, sería aconsejable aplanar la matriz para cada clave. En estas situaciones, debe elegir que solo quede un objeto. El procesador ofrece la posibilidad de elegir entre el primero o el último.

```
...
processor:
    - list_to_map:
        key: "somekey"
        source: "mylist"
        target: "myobject"
        flatten: true
...
```

A continuación, la estructura de eventos entrantes se aplana en consecuencia:

```
{
  "myobject" : {
    "a" : {
      "somekey" : "a",
      "somevalue" : "val-a1",
```

```
      "anothervalue" : "val-a2"
    },
    "b" : {
      "somekey" : "b",
      "somevalue" : "val-b1",
      "anothervalue" : "val-b2"
    }
    "c" : {
      "somekey" : "c",
      "somevalue" : "val-c1",
      "anothervalue" : "val-c2"
    }
  }
}
```

Puede utilizar el procesador Lista a mapa para procesar los registros de AWS WAF. Por ejemplo, fíjese en un registro de WAF de ejemplo como el siguiente:

```
{
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "httpRequest": {
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            }
        ]
    }
}
```

Si la siguiente canalización procesa el evento:

```
...
processor:
    - list_to_map:
        key: "name"
        source: "httpRequest/headers"
        value_key: "value"
```

```
        flatten: true
...
```

Creará el siguiente evento nuevo:

```
{
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "httpRequest": {
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            }
        ]
    },
    "Host": "localhost:1989",
    "User-Agent": "curl/7.61.1"
}
```

Procesar marcas de tiempo entrantes

El procesador de Fechas analiza la clave de marca de tiempo de los eventos entrantes convirtiéndola al formato ISO 8601.

```
...
  processor:
    - date:
        match:
          - key: timestamp
            patterns: ["dd/MMM/yyyy:HH:mm:ss"]
        destination: "@timestamp"
        source_timezone: "America/Los_Angeles"
        destination_timezone: "America/Chicago"
        locale: "en_US"
...
```

Si la canalización anterior procesa el siguiente evento:

```
{"timestamp": "10/Feb/2000:13:55:36"}
```

Convierte el evento en el siguiente formato:

```
{
  "timestamp":"10/Feb/2000:13:55:36",
  "@timestamp":"2000-02-10T15:55:36.000-06:00"
}
```

Crear marcas de tiempo

El procesador de fechas puede generar marcas de tiempo para los eventos entrantes si usted especifica `@timestamp` para la opción `destination`.

```
...
    processor:
    - date:
        from_time_received: true
        destination: "@timestamp"
...
```

Derivar patrones de puntuación

El procesador de Sustituir cadenas (que es uno de los procesadores de mutar cadenas) permite obtener un patrón de puntuación a partir de los eventos entrantes. En la siguiente canalización de ejemplo, el procesador escaneará los eventos de registro de Apache entrantes y obtendrá patrones de puntuación a partir de ellos.

```
processor:

    - substitute_string:

        entries:

          - source: "message"

            from: "[a-zA-Z0-9_]+"

            to: ""
```

```
          - source: "message"

            from: "[ ]+"

            to: "_"
```

El siguiente registro HTTP entrante de Apache generará un patrón de puntuación:

```
[{"message":"10.10.10.11 - admin [19/Feb/2015:15:50:36 -0500] \"GET /big2.pdf
 HTTP/1.1\" 200 33973115 0.202 \"-\" \"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10_1)
 AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.111 Safari/537.36\""}]

{"message":"..._-_[//:::_-]_\"_/._/.\"_._\"-\"_\"/._(;_)_/._(,_)_/..._/.\""}
```

Puede contar estos patrones generados pasándolos por el procesador Aggregate junto con la acción `count`.

Agregado de eventos con Amazon OpenSearch Ingestion

Puede utilizar Amazon OpenSearch Ingestion para agregar datos de diferentes eventos durante un período de tiempo. El agregado de eventos puede ayudar a reducir el volumen de registros innecesario y a gestionar casos de uso, como los registros multilínea que se presentan como eventos separados. El procesador Aggregate es un procesador con estado activo que agrupa los eventos en función de los valores de un conjunto de claves de identificación específicas y realiza una acción configurable en cada grupo.

El estado del procesador Aggregate se almacena en la memoria. Por ejemplo, para combinar cuatro eventos en uno, el procesador necesita conservar partes de los tres primeros eventos. El estado de un grupo agregado de eventos se mantiene durante un período de tiempo configurable. En función de los registros, de la acción agregada que se utilice y de la cantidad de opciones de memoria de la configuración del procesador, el agregado podría tener lugar durante un período de tiempo prolongado.

Además de estos ejemplos, también puede utilizar el esquema de agregado de registros con enrutamiento condicional. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

- Uso básico
- Eliminar duplicados

- Agregado de registros y enrutamiento condicional

Uso básico

El siguiente ejemplo de canalización extrae los campos `sourceIp`, `destinationIp` y `port` utilizando el procesador Grok y, a continuación, los agrega durante un período de 30 segundos con el procesador Aggregate y la acción `put_all`. Al final de los 30 segundos, el registro agregado se envía al receptor de OpenSearch.

```
version: "2"
aggregate_pipeline:
   source:
     http:
      path: "/${pipelineName}/logs"
   processor:
     - grok:
         match:
           log: ["%{IPORHOST:sourceIp} %{IPORHOST:destinationIp} %{NUMBER:port:int}"]
     - aggregate:
         group_duration: "30s"
         identification_keys: ["sourceIp", "destinationIp", "port"]
         action:
           put_all:
   sink:
     - opensearch:
         ...
         index: aggregated_logs
```

Por ejemplo, considere el siguiente lote de registros:

```
{ "log": "127.0.0.1 192.168.0.1 80", "status": 200 }
{ "log": "127.0.0.1 192.168.0.1 80", "bytes": 1000 }
{ "log": "127.0.0.1 192.168.0.1 80" "http_verb": "GET" }
```

El procesador Grok los extraerá el `identification_keys` para crear los siguientes registros:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "status": 200 }
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "bytes": 1000 }
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "http_verb":
 "GET" }
```

Cuando el grupo finalice 30 segundos después de que el procesador Aggregate reciba el primer registro, se escribirá el siguiente registro agregado en el receptor:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "port": 80, "status": 200,
 "bytes": 1000, "http_verb": "GET" }
```

Eliminar duplicados

Puede eliminar las entradas duplicadas derivando las claves de los eventos entrantes y especificando la opción `remove_duplicates` para el procesador Aggregate. Esta acción procesa inmediatamente el primer evento de un grupo y descarta todos los eventos siguientes de ese grupo.

En el ejemplo siguiente, el primer evento se procesa con las claves de identificación `sourceIp` y `destinationIp`:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "status": 200 }
```

A continuación, la canalización descartará el siguiente evento porque tiene las mismas claves:

```
{ "sourceIp": "127.0.0.1", "destinationIp": "192.168.0.1", "bytes": 1000 }
```

La canalización procesa este evento y crea un grupo nuevo porque `sourceIp` es diferente:

```
{ "sourceIp": "127.0.0.2", "destinationIp": "192.168.0.1", "bytes": 1000 }
```

Agregado de registros y enrutamiento condicional

Puede usar varios complementos para combinar el agregado de registros con enrutamiento condicional. En este ejemplo, la `log-aggregate-pipeline` de subcanalización recibe los registros a través de un cliente HTTP como FluentBit y extrae los valores importantes de los registros comparando el valor de la clave de `log` con el patrón de registro común de Apache.

Dos de los valores que extrae de los registros con un patrón grok incluyen `response` y `clientip`. Luego, el procesador Aggregate usa el valor de `clientip`, junto con la opción `remove_duplicates`, para eliminar cualquier registro que contenga un `clientip` que ya se haya procesado dentro del `group_duration` dado.

Existen tres rutas, o enunciados condicionales, en la canalización. Estas rutas separan el valor de la respuesta en respuestas 2xx/3xx, 4xx y 5xx. Los registros con un estado 2xx y 3xx se

envían al índice `aggregated_2xx_3xx`, los registros con un estado 4xx se envían al índice `aggregated_4xx` y los registros con un estado 5xx se envían al índice `aggregated_5xx`.

```
version: "2"
log-aggregate-pipeline:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/log-aggregate-pipeline/logs". This will be the
 FluentBit output URI value.
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
    - aggregate:
        identification_keys: ["clientip"]
        action:
          remove_duplicates:
        group_duration: "180s"
  route:
    - 2xx_status: "/response >= 200 and /response < 300"
    - 3xx_status: "/response >= 300 and /response < 400"
    - 4xx_status: "/response >= 400 and /response < 500"
    - 5xx_status: "/response >= 500 and /response < 600"
  sink:
    - opensearch:
        ...
        index: "aggregated_2xx_3xx"
        routes:
          - 2xx_status
          - 3xx_status
    - opensearch:
        ...
        index: "aggregated_4xx"
        routes:
          - 4xx_status
    - opensearch:
        ...
        index: "aggregated_5xx"
        routes:
          - 5xx_status
```

Obtener métricas a partir de registros con Amazon OpenSearch Ingestion

Puede utilizar Amazon OpenSearch Ingestion para obtener métricas de los registros. El siguiente ejemplo de canalización recibe los registros entrantes mediante el complemento fuente HTTP y el procesador Grok. A continuación, utiliza el procesador Aggregate para extraer la métrica `bytes` agregada en un intervalo de 30 segundos y obtiene histogramas a partir de los resultados.

La canalización general contiene dos subcanalizaciones:

- `apache-log-pipeline-with-metrics`: recibe los registros a través de un cliente HTTP como FluentBit, extrae los valores importantes de los registros comparando el valor de la clave `log` con el patrón de registro común de Apache y, a continuación, reenvía los registros grokked tanto a la subcanalización `log-to-metrics-pipeline` como a un índice de OpenSearch denominado `logs`.
- `log-to-metrics-pipeline`: recibe los registros grokked de la subcanalización `apache-log-pipeline-with-metrics`, los agrega y obtiene las métricas del histograma de `bytes` en función de los valores de las claves `clientip` y `request`. Por último, envía las métricas del histograma a un índice de OpenSearch denominado `histogram_metrics`.

```
version: "2"
apache-log-pipeline-with-metrics:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/apache-log-pipeline-with-metrics/logs". This will be
 the FluentBit output URI value.
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
  sink:
    - opensearch:
        ...
        index: "logs"
    - pipeline:
        name: "log-to-metrics-pipeline"

log-to-metrics-pipeline:
```

```
source:
  pipeline:
    name: "apache-log-pipeline-with-metrics"
processor:
  - aggregate:
      # Specify the required identification keys
      identification_keys: ["clientip", "request"]
      action:
        histogram:
          # Specify the appropriate values for each of the following fields
          key: "bytes"
          record_minmax: true
          units: "bytes"
          buckets: [0, 25000000, 50000000, 75000000, 100000000]
      # Pick the required aggregation period
      group_duration: "30s"
sink:
  - opensearch:
      ...
      index: "histogram_metrics"
```

Además de este ejemplo, también puede utilizar el esquema de canalización de registros a métrica. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Trace Analytics con Amazon OpenSearch Ingestion

Puede utilizar Amazon OpenSearch Ingestion para recopilar datos de rastreo de OpenTelemetry y transformarlos para utilizarlos en OpenSearch Service. El siguiente ejemplo de canalización usa tres subcanalizaciones para monitorear Trace Analytics: `entry-pipeline`, `span-pipeline` y `service-map-pipeline`.

Fuente de trazas de OpenTelemetry

El complemento de fuentes de trazas de OTel acepta datos de trazas del recopilador de OpenTelemetry. El complemento sigue el protocolo OpenTelemetry y es oficialmente compatible con el cifrado HTTPS estándar del sector.

Procesadores

Puede utilizar los siguientes procesadores para Trace Analytics:

- Trazas OTel: recibe una colección de registros de tramos de la fuente y realiza el procesamiento, la extracción y la finalización de los campos de forma continua.
- Grupo de trazas OTel: rellena los campos del grupo de trazas que faltan en la colección de registros de tramos.
- Mapa de servicios: realiza el preprocesamiento de los datos de trazas y crea metadatos para mostrar los paneles de mapa de servicios.

Receptor de OpenSearch

El complemento receptor de OpenSearch ofrece índices y plantillas de índices específicos de Trace Analytics. Los siguientes índices de OpenSearch son específicos de Trace Analytics:

- `otel-v1-apm-span`: almacena la salida del procesador de trazas OTel.
- `otel-v1-apm-service-map`: almacena la salida del procesador de mapa de servicios.

Configuración de canalización

El siguiente ejemplo de canalización es compatible con Observabilidad para OpenSearch Dashboards. La primera subcanalización (`entry-pipeline`) recibe datos del recopilador de OpenTelemetry y utiliza otras dos subcanalizaciones como receptores.

La subcanalización `span-pipeline` analiza los datos de trazas y enriquece e incorpora los documentos de tramos en un índice de tramos. La subcanalización `service-map-pipeline` agrega las trazas en un mapa de servicios y escribe los documentos en un índice de mapas de servicios.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. This will be the endpoint URI path in the
 OpenTelemetry Exporter configuration.
      # ${pipelineName} will be replaced with the sub-pipeline name. In this case it
 would be "/entry-pipeline/v1/traces".
      path: "/${pipelineName}/v1/traces"
  processor:
    - trace_peer_forwarder
  sink:
    - pipeline:
```

```
        name: "span-pipeline"
    - pipeline:
        name: "service-map-pipeline"

span-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - otel_traces
  sink:
    - opensearch:
        ...
        index_type: trace-analytics-raw

service-map-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - service_map
  sink:
    - opensearch:
        ...
        index_type: trace-analytics-service-map
```

Debe ejecutar el recopilador de OpenTelemetry en su entorno para enviar los datos al punto de conexión de ingesta. Para ver otro ejemplo de canalización, consulte el esquema de Canalización de Análisis de Trazas. Para obtener más información, consulte the section called “Uso de esquemas para crear una canalización”.

Obtener métricas a partir de trazas con Amazon OpenSearch Ingestion

Puede utilizar Amazon OpenSearch Ingestion para obtener métricas de las trazas de OpenTelemetry. El siguiente ejemplo de canalización recibe las trazas entrantes y extrae una métrica denominada `durationInNanos`, agregada a una ventana de saltos de tamaño constante de 30 segundos. A continuación, obtiene un histograma a partir de las trazas entrantes.

La canalización contiene las siguientes subcanalizaciones:

- `entry-pipeline`: recibe los datos de trazas del recopilador de OpenTelemetry y los reenvía a la subcanalización `trace_to_metrics_pipeline`.

- `trace-to-metrics-pipeline`: recibe los datos de trazas de la subcanalización `entry-pipeline`, los agrega y obtiene un histograma de `durationInNanos` a partir de las trazas en función del valor del campo `serviceName`. A continuación, envía las métricas obtenidas al índice de OpenSearch denominado `metrics_for_traces`.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. ${pipelineName} will be replaced with sub-
pipeline name.
      # In this case it would be "/entry-pipeline/v1/traces". This will be endpoint URI
 path in OpenTelemetry Exporter configuration.
      path: "/${pipelineName}/v1/traces"
  sink:
    - pipeline:
        name: "trace-to-metrics-pipeline"

trace-to-metrics-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - aggregate:
        # Pick the required identification keys
        identification_keys: ["serviceName"]
        action:
          histogram:
            # Pick the appropriate values for each of the following fields
            key: "durationInNanos"
            record_minmax: true
            units: "seconds"
            buckets: [0, 10000000, 50000000, 100000000]
        # Specify an aggregation period
        group_duration: "30s"
  sink:
    - opensearch:
        ...
        index: "metrics_for_traces"
```

Para ver otro ejemplo de canalización, consulte el esquema de canalización de anomalías de traza a métrica. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Detección de anomalías con Amazon OpenSearch Ingestion

Puede utilizar Amazon OpenSearch Ingestion para entrenar modelos y generar anomalías en casi tiempo real a partir de eventos agregados en series temporales. Puede generar anomalías en los eventos generados dentro de la canalización o en los eventos que lleguen directamente a la canalización, como las métricas de OpenTelemetry.

Puede enviar estos eventos de series temporales de ventanas agregadas de saltos de tamaño constante al procesador de Detector de anomalías, que entrena un modelo y genera anomalías con una puntuación. A continuación, escriba las anomalías en un índice independiente para crear monitores de documentos y activar alertas rápidas.

Además de estos ejemplos, también puede utilizar los esquemas de canalización de anomalías de registro a métrica y canalización de anomalías de trazas a métricas. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

- Métricas de los registros
- Métricas de trazas
- Métricas de OpenTelemetry

Métricas de los registros

La siguiente canalización recibe los registros a través de una fuente HTTP como FluentBit, extrae los valores importantes de los registros comparando el valor de la clave `log` con el patrón grok de registro común de Apache y, a continuación, reenvía los registros grokked tanto a la subcanalización `log-to-metrics-pipeline` como a un índice de OpenSearch denominado `logs`.

La `log-to-metrics-pipeline` subcanalización recibe los registros grokked de la `apache-log-pipeline-with-metrics`subcanalización , los agrega y obtiene las métricas del histograma en función de los valores `clientip` y `request`de las claves. A continuación, envía las métricas del histograma a un índice de OpenSearch denominado `histogram_metrics`, así como a la `log-to-metrics-anomaly-detector`subcanalización.

La `log-to-metrics-anomaly-detector-pipeline` subcanalización recibe las métricas agregadas del histograma de la `log-to-metrics-pipeline` subcanalización y las envía al procesador de Detector de anomalías para que las detecte mediante el algoritmo Random Cut Forest. Si detecta anomalías, las envía a un índice de OpenSearch denominado `log-metric-anomalies`.

```
version: "2"
apache-log-pipeline-with-metrics:
  source:
    http:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/apache-log-pipeline-with-metrics/logs". This will be
 the FluentBit output URI value.
      path: "/${pipelineName}/logs"
  processor:
    - grok:
        match:
          log: [ "%{COMMONAPACHELOG_DATATYPED}" ]
  sink:
    - opensearch:
        ...
        index: "logs"
    - pipeline:
        name: "log-to-metrics-pipeline"

log-to-metrics-pipeline:
  source:
    pipeline:
      name: "apache-log-pipeline-with-metrics"
  processor:
    - aggregate:
        # Specify the required identification keys
        identification_keys: ["clientip", "request"]
        action:
          histogram:
            # Specify the appropriate values for each the following fields
            key: "bytes"
            record_minmax: true
            units: "bytes"
            buckets: [0, 25000000, 50000000, 75000000, 100000000]
        # Pick the required aggregation period
        group_duration: "30s"
```

```
  sink:
    - opensearch:
        ...
        index: "histogram_metrics"
    - pipeline:
        name: "log-to-metrics-anomaly-detector-pipeline"

log-to-metrics-anomaly-detector-pipeline:
  source:
    pipeline:
      name: "log-to-metrics-pipeline"
  processor:
    - anomaly_detector:
        # Specify the key on which to run anomaly detection
        keys: [ "bytes" ]
        mode:
          random_cut_forest:
  sink:
    - opensearch:
        ...
        index: "log-metric-anomalies"
```

Métricas de trazas

Puede derivar métricas a partir de trazas y encontrar anomalías en estas métricas generadas. En este ejemplo, la `entry-pipeline` subcanalización recibe datos de trazas del recopilador de OpenTelemetry y los reenvía a las siguientes subcanalizaciones:

- `span-pipeline`: extrae los tramos sin procesar de las trazas. Envía los tramos sin procesar a cualquier índice con el que OpenSearch tenga el prefijo `otel-v1-apm-span`.
- `service-map-pipeline`: los agrega y analiza para crear documentos que representan conexiones entre servicios. Envía estos documentos a un índice de OpenSearch denominado `otel-v1-apm-service-map`. A continuación, puede ver una visualización del mapa de servicios a través del complemento Trace Analytics para OpenSearch Dashboards.
- `trace-to-metrics-pipeline`: agrega y obtiene las métricas del histograma a partir de las trazas en función del valor de `serviceName`. A continuación, envía las métricas obtenidas a un índice de OpenSearch denominado `metrics_for_traces`, así como a la `trace-to-metrics-anomaly-detector-pipeline`subcanalización .

La `trace-to-metrics-anomaly-detector-pipeline` subcanalización recibe las métricas agregadas del histograma de la `trace-to-metrics-pipeline` y las envía al procesador de Detector de anomalías para que las detecte mediante el algoritmo Random Cut Forest. Si detecta cualquier anomalía, la envía a un índice de OpenSearch denominado `trace-metric-anomalies`.

```
version: "2"
entry-pipeline:
  source:
    otel_trace_source:
      # Provide the path for ingestion. ${pipelineName} will be replaced with pipeline
 name configured for this pipeline.
      # In this case it would be "/entry-pipeline/v1/traces". This will be endpoint URI
 path in OpenTelemetry Exporter
      # configuration.
      # path: "/${pipelineName}/v1/traces"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "span-pipeline"
    - pipeline:
        name: "service-map-pipeline"
    - pipeline:
        name: "trace-to-metrics-pipeline"

span-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - otel_trace_raw:
  sink:
    - opensearch:
        ...
        index_type: "trace-analytics-raw"

service-map-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - service_map:
  sink:
```

```
    - opensearch:
        ...
        index_type: "trace-analytics-service-map"

trace-to-metrics-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
  processor:
    - aggregate:
        # Pick the required identification keys
        identification_keys: ["serviceName"]
        action:
          histogram:
            # Pick the appropriate values for each the following fields
            key: "durationInNanos"
            record_minmax: true
            units: "seconds"
            buckets: [0, 10000000, 50000000, 100000000]
        # Pick the required aggregation period
        group_duration: "30s"
  sink:
    - opensearch:
        ...
        index: "metrics_for_traces"
    - pipeline:
        name: "trace-to-metrics-anomaly-detector-pipeline"

trace-to-metrics-anomaly-detector-pipeline:
  source:
    pipeline:
      name: "trace-to-metrics-pipeline"
  processor:
    - anomaly_detector:
        # Below Key will find anomalies in the max value of histogram generated for
 durationInNanos.
        keys: [ "max" ]
        mode:
          random_cut_forest:
  sink:
    - opensearch:
        ...
        index: "trace-metric-anomalies"
```

Métricas de OpenTelemetry

Puede crear una canalización que reciba métricas de OpenTelemetry y detecte anomalías en estas métricas. En este ejemplo, `entry-pipeline` recibe datos de métricas del recopilador de OpenTelemetry. Si una métrica es de tipo `GAUGE` y su nombre es `totalApiBytesSent`, el procesador la envía a la subcanalización `ad-pipeline`.

La `ad-pipeline` subcanalización recibe los datos de las métricas de la canalización de entrada y realiza la detección de anomalías en el valor de la métrica mediante el procesador de Detector de anomalías.

```
entry-pipeline:
  source:
    otel_metrics_source:
  processor:
    - otel_metrics:
  route:
    - gauge_route: '/kind = "GAUGE" and /name = "totalApiBytesSent"'
  sink:
    - pipeline:
        name: "ad-pipeline"
        routes:
          - gauge_route
    - opensearch:
        ...
        index: "otel-metrics"

ad-pipeline:
  source:
    pipeline:
      name: "entry-pipeline"
    processor:
      - anomaly_detector:
        # Use "value" as the key on which anomaly detector needs to be run
        keys: [ "value" ]
        mode:
          random_cut_forest:
    sink:
      - opensearch:
        ...
        index: otel-metrics-anomalies
```

Además de este ejemplo, también puede utilizar el esquema de canalización de anomalías de trazas a métricas. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Muestreo con Amazon OpenSearch Ingestion

Amazon OpenSearch Ingestion ofrece las siguientes capacidades de muestreo. Además de estos ejemplos, también puede utilizar el esquema de muestreo de registros de Apache. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Temas

- Muestreo temporal
- Muestreo porcentual
- Muestreo de colas

Muestreo temporal

Puede utilizar la acción `rate_limiter` del procesador Aggregate para limitar la cantidad de eventos que se pueden procesar por segundo. Puede optar por descartar los eventos sobrantes o transferirlos al siguiente período de tiempo.

En este ejemplo, solo se envían 100 eventos por segundo con un código de estado de `200` al receptor desde una dirección IP determinada. Descarta todos los eventos sobrantes de la ventana de tiempo configurada.

```
...
  processor:
   - aggregate:

        identification_keys: ["clientip"]

        action:

          rate_limiter:

            events_per_second: 100

            when_exceeds: drop
```

```
        when: "/status == 200"
...
```

Si, por el contrario, establece la opción `when_exceeds` en `block`, el procesador procesará los eventos sobrantes en la siguiente ventana de tiempo.

Muestreo porcentual

Utilice la acción `percent_sampler` del procesador Aggregate para limitar la cantidad de eventos que se envían a un receptor. Se descartarán todos los eventos sobrantes.

En este ejemplo, solo se envía el 20 por ciento de los eventos con un código de estado de `200` al receptor desde una dirección IP determinada.

```
...
  processor:
  - aggregate:

        identification_keys: ["clientip"]
        duration :

        action:

          percent_sampler:

            percent: 20

        when: "/status == 200"
...
```

Muestreo de colas

Utilice la acción `tail_sampler` del procesador Aggregate para muestrear los eventos en función de un conjunto de políticas definidas. Esta acción espera a que se complete un agregado en diferentes períodos de agregado según el período de espera configurado. Cuando se completa un agregado y si coincide con la condición de error específica, se envía al receptor. De lo contrario, solo se envía al receptor un porcentaje configurado de eventos.

El siguiente ejemplo de canalización envía todas las trazas de OpenTelemetry con un estado de condición de error de 2 al receptor. Solo envía al receptor el 20 % de las trazas que no coinciden con esta condición de error.

```
...
  processor:
   - aggregate:

        identification_keys: ["traceId"]

        action:

          tail_sampler:

            percent: 20

            wait_period: "10s"

            condition: "/status == 2"


...
```

Si establece la condición de error en `false` o no la incluye, solo se permite la transmisión directa del porcentaje de eventos configurado, determinado por un resultado probabilístico.

Como es difícil determinar exactamente cuándo debe realizarse el muestreo de colas, puede utilizar la opción `wait_period` para medir el tiempo de inactividad tras recibir el último evento.

Descarga selectiva con Amazon OpenSearch Ingestion

Si su canalización utiliza una fuente de S3, puede utilizar expresiones de SQL para filtrar y calcular el contenido de los objetos de S3 antes de incorporarlos a una canalización.

La opción `s3_select` admite objetos en formato Parquet. También funciona con objetos comprimidos con GZIP o BZIP2 (solo para objetos CSV y JSON), así como con la compresión de columnas para Parquet con GZIP y Snappy.

El siguiente ejemplo de canalización descarga datos en objetos de S3 entrantes, codificados en formato Parquet:

```
pipeline:
  source:
    s3:
      s3_select:
```

```
        expression: "select * from s3object s"
        input_serialization: parquet
      notification_type: "sqs"
...
```

El siguiente ejemplo descarga solo los primeros 10,000 registros de los objetos:

```
pipeline:
  source:
    s3:
      s3_select:
        expression: "select * from s3object s LIMIT 10000"
        input_serialization: parquet
      notification_type: "sqs"
...
```

En el siguiente ejemplo, se comprueba el valor mínimo y máximo de `data_value` antes de incorporar los eventos a la canalización:

```
pipeline:
  source:
    s3:
      s3_select:
        expression: "select s.* from s3object s where s.data_value > 200 and
 s.data_value < 500 "
        input_serialization: parquet
      notification_type: "sqs"
...
```

Además de estos ejemplos, también puede utilizar el esquema de canalización de selección de S3. Para obtener más información acerca de los esquemas, consulte the section called “Uso de esquemas para crear una canalización”.

Para obtener más información, consulte los siguientes recursos:

- Filtrado y recuperación de datos con Amazon S3 Select
- Referencia de SQL para Amazon S3 Select

Seguridad en Amazon OpenSearch Ingestion

La seguridad en la nube de AWS es la mayor prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos que se han diseñado 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 que ejecuta los servicios de AWS en la nube de AWS. AWS también 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.
- Seguridad en la nube: su responsabilidad se determina según el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación lo ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando utiliza OpenSearch Ingestion. En los siguientes temas, se muestra cómo configurar OpenSearch Ingestion para cumplir sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayudan a monitorear y proteger los recursos de OpenSearch Ingestion.

Temas

- Protección de las canalizaciones OpenSearch de Amazon Ingestion dentro de una VPC
- Identity and Access Management en Amazon OpenSearch Ingestion
- Registro de llamadas a la API de Amazon OpenSearch Ingestion mediante AWS CloudTrail

Protección de las canalizaciones OpenSearch de Amazon Ingestion dentro de una VPC

Puede lanzar las canalizaciones OpenSearch de Amazon Ingestion en una nube privada virtual (VPC). Una VPC es una red virtual dedicada para Cuenta de AWS. Está aislado de forma lógica de otras redes virtuales de la nube. AWS La colocación de una canalización dentro de una VPC permite una comunicación segura entre OpenSearch Ingestion y otros servicios de la VPC sin necesidad de

una puerta de enlace a Internet, un dispositivo NAT o una conexión VPN. Todo el tráfico permanece de forma segura en la nube. AWS

El uso de una VPC le permite hacer cumplir el flujo de datos a través de sus canalizaciones de OpenSearch ingestión dentro de los límites de la VPC, en lugar de hacerlo a través de la Internet pública. Las canalizaciones que no están dentro de una VPC envían y reciben datos a través de puntos de conexión públicos e Internet.

Para obtener instrucciones sobre cómo aprovisionar una canalización dentro de una VPC, consulte the section called “Creación de canalizaciones”.

Temas

Consideraciones

Tenga en cuenta lo siguiente cuando configure el acceso mediante VPC para una canalización.

- Una canalización pública puede escribir en un dominio de VPC. De forma similar, una canalización de VPC puede escribir en un dominio público.
- No es necesario que una canalización esté en la misma VPC que su receptor de dominio. Tampoco es necesario establecer una conexión entre las dos VPC. OpenSearch Ingestion se encarga de conectarlos por ti.
- Solo puede especificar una VPC para la canalización.
- A diferencia de las canalizaciones públicas, una canalización de VPC debe estar en el mismo Región de AWS que el dominio en el que se escribe.
- Puede elegir implementar una canalización en una, dos o tres subredes de la VPC. Las subredes se distribuyen en las mismas zonas de disponibilidad en las que están desplegadas las unidades de OpenSearch cómputo de ingestión (OCU).
- Si solo implementa una canalización en una subred y la zona de disponibilidad deja de funcionar, no podrá incorporar datos. Para garantizar una alta disponibilidad, le recomendamos que configure las canalizaciones con dos o tres subredes.

- La especificación de grupos de seguridad es opcional. Si no se proporciona un grupo de seguridad, usaremos el grupo de seguridad predeterminado que se especifica en la VPC.

Limitaciones

Las canalizaciones dentro de una VPC presentan las siguientes limitaciones.

- No puede cambiar la configuración de red de una canalización después de crearla. Si lanza una canalización dentro de una VPC, no podrá cambiarla posteriormente a un punto de conexión público y viceversa.
- Es posible lanzar la canalización dentro de una VPC o utilizar un punto de conexión público, pero no es posible hacer las dos cosas. Se debe elegir una de ellas al crear una canalización.
- Después de proporcionar una canalización dentro de una VPC, no se puede mover a otra VPC, y no puede cambiar la configuración de sus subredes y grupos de seguridad.
- Si su canalización escribe en un receptor de dominio de VPC, no podrá volver atrás más adelante y cambiar el receptor a un dominio diferente (de VPC o público) una vez creada la canalización. Debe eliminar y volver a crear manualmente la canalización con el nuevo receptor. Aún puede cambiar un receptor de un dominio público a un dominio de VPC.
- No puede proporcionar acceso de incorporación entre cuentas a las canalizaciones de VPC.

Requisitos previos

Antes de poder aprovisionar una canalización dentro de una VPC, debe hacer lo siguiente:

- Creación de una VPC

  Para crear su VPC, puede utilizar la consola de Amazon VPC, la AWS CLI o uno de los SDK. AWS Para obtener más información, consulte Uso de VPC en la Guía del usuario de Amazon VPC. Si ya tiene una VPC, puede omitir este paso.

- Reservar direcciones IP

  OpenSearch La ingestión coloca una interface de red elástica en cada subred que especifique durante la creación de la canalización. Cada interfaz de red tiene asociada una dirección IP. Debe reservar una dirección IP por subred para las interfaces de red.

Configuración del acceso mediante VPC para una canalización

Puede habilitar el acceso a la VPC para una canalización desde la consola de OpenSearch servicio o mediante la. AWS CLI

Consola

El acceso a la VPC se configura durante la creación de la canalización. En Red, seleccione el Acceso a la VPC y realice los siguientes ajustes:

Opción	Descripción
VPC	Seleccione el ID de la nube privada virtual (VPC) que desee utilizar. La VPC y la canalización deben estar en la misma Región de AWS.
Subredes	Elija una o más subredes. OpenSearch El servicio colocará un punto final de VPC e interfaces de red elásticas en las subredes.
Grupos de seguridad	Elija uno o más grupos de seguridad de VPC que permitan que la aplicació n requerida llegue a la canalización de OpenSearch ingestión en los puertos (80 o 443) y protocolos (HTTP o HTTPs) expuestos por la canalización.

CLI

Para configurar el acceso a la VPC mediante AWS CLI, especifique el `--vpc-options` parámetro:

```
aws osis create-pipeline \
  --pipeline-name vpc-pipeline \
  --min-units 4 \
  --max-units 10 \
  --vpc-options
 SecurityGroupIds={sg-12345678,sg-9012345},SubnetIds=subnet-1212234567834asdf \
  --pipeline-configuration-body "file://pipeline-config.yaml"
```

Roles vinculados a servicios para el acceso mediante VPC

Un rol vinculado a un servicio es un tipo único de rol de IAM; que delega permisos en un servicio para que pueda crear y administrar recursos en nombre del usuario. OpenSearch La ingestión requiere un rol vinculado a un servicio llamado

AWSServiceRoleForAmazonOpenSearchIngestionpara acceder a la VPC, crear el punto final de la canalización y colocar las interfaces de red en una subred de la VPC. Para obtener más información acerca de los permisos de este rol y cómo eliminarlo, consulte the section called “Rol de creación de canalizaciones”.

OpenSearch La ingestión crea automáticamente la función al crear una canalización de ingestión. Para que esta creación automática se realice correctamente, el usuario que cree la primera canalización en una cuenta debe tener permisos para realizar la acción `iam:CreateServiceLinkedRole`. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM. Puede ver el rol en la consola AWS Identity and Access Management (IAM) una vez creado.

Identity and Access Management en Amazon OpenSearch Ingestion

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de OpenSearch Ingestion. IAM es un Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Políticas basadas en identidades de OpenSearch Ingestion

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y bajo qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidad de IAM, puede especificar las acciones y recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está asociado. Para obtener más información acerca de los elementos que puede utilizar en una política de JSON, consulte Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para OpenSearch Ingestion

Para ver ejemplos de políticas basadas en identidad de OpenSearch Ingestion, consulte the section called “Ejemplos de políticas basadas en identidad”.

Acciones de políticas de OpenSearch Ingestion

Admite acciones de política	Sí

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de OpenSearch Ingestion utilizan el siguiente prefijo antes de la acción:

```
osis
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
```

```
      "osis:action1",
      "osis:action2"
         ]
```

Puede especificar varias acciones utilizando caracteres comodín (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `List`, incluya la siguiente acción:

```
"Action": "osis:List*"
```

Para ver ejemplos de políticas basadas en identidad de OpenSearch Ingestion, consulte Ejemplos de políticas basadas en identidades para OpenSearch sin servidor.

Recursos de políticas de OpenSearch Ingestion

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Claves de condición de política de Amazon OpenSearch Ingestion

Admite claves de condición de política específicas del servicio	No

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y bajo qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para obtener más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para obtener una lista de las claves de condición de OpenSearch Ingestion, consulte Claves de condición de Amazon OpenSearch Ingestion en la Referencia de autorizaciones de servicio. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon OpenSearch Ingestion.

ABAC con OpenSearch Ingestion

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos. En AWS, estos atributos se denominan etiquetas. Puede asociar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Para obtener más información sobre el etiquetado de recursos OpenSearch Ingestion, consulte the section called “Etiquetado de canalizaciones”.

Uso de credenciales temporales con OpenSearch Ingestion

Compatible con el uso de credenciales temporales.	Sí

Algunos servicios de Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué servicios de Servicios de AWS funcionan con credenciales temporales, consulte Servicios de Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información acerca del cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda

generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM.

Roles vinculados a servicios para OpenSearch Ingestion

Compatible con roles vinculados a servicios	Sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

OpenSearch Ingestion utiliza un rol vinculado a servicios denominado `AWSServiceRoleForAmazonOpenSearchIngestion`. Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de OpenSearch Ingestion, consulte the section called "Rol de creación de canalizaciones".

Ejemplos de políticas basadas en identidades para OpenSearch Ingestion

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de OpenSearch Ingestion. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador puede crear políticas de IAM. Luego, el administrador puede agregar las políticas de IAM a roles, y los usuarios pueden asumir esos roles.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon OpenSearch Ingestion, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición para Amazon OpenSearch Ingestion en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de OpenSearch Ingestion en la consola

- Administración de canalizaciones de OpenSearch Ingestion
- Incorporación de datos en una canalización de OpenSearch Ingestion

Prácticas recomendadas relativas a políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de OpenSearch Ingestion de su cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar recursos de OpenSearch Ingestion de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidad:

- Comience con las políticas administradas por AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en la Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Use condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política JSON de IAM: condición en la Guía del usuario de IAM.
- Use el Analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el Analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas

recomendadas de IAM. IAM Access Analyzer proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para obtener más información, consulte la política de validación del Analizador de acceso de IAM en la Guía de usuario de IAM.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía de usuario de IAM.

Uso de OpenSearch Ingestion en la consola

Para acceder a OpenSearch Ingestion en la consola de OpenSearch Service, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de OpenSearch Ingestion en su cuenta de AWS. Si se crea una política basada en identidades que es más restrictiva que los permisos necesarios mínimos, la consola no funcionará del modo esperado para las entidades (tales como roles de IAM) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

La siguiente política permite al usuario acceder a OpenSearch Ingestion desde la consola de OpenSearch Service:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
```

```
                "osis:GetPipelineChangeProgress"
            ]
        }
    ]
}
```

Como alternativa, puede utilizar la política the section called "AmazonOpenSearchIngestionReadOnlyAccess" AWS gestionada, que concede acceso de solo lectura a todos los recursos de OpenSearch Ingestion por un Cuenta de AWS.

Administración de canalizaciones de OpenSearch Ingestion

Esta política es un ejemplo de la política de "administración de canalizaciones" que permite al usuario gestionar y administrar las canalizaciones de Amazon OpenSearch Ingestion. El usuario puede crear, ver y eliminar canalizaciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:CreatePipeline",
                "osis:DeletePipeline",
                "osis:UpdatePipeline",
                "osis:ValidatePipeline",
                "osis:StartPipeline",
                "osis:StopPipeline"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "osis:ListPipelines",
                "osis:GetPipeline",
                "osis:ListPipelineBlueprints",
                "osis:GetPipelineBlueprint",
                "osis:GetPipelineChangeProgress"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Incorporación de datos en una canalización de OpenSearch Ingestion

Este ejemplo de política permite a un usuario u otra entidad incorporar datos a una canalización de Amazon OpenSearch Ingestion de su cuenta. El usuario no puede modificar las canalizaciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:osis:region:123456789012:pipeline/*",
            "Action": [
                "osis:Ingest"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Registro de llamadas a la API de Amazon OpenSearch Ingestion mediante AWS CloudTrail

Amazon OpenSearch Ingestion se integra con AWS CloudTrail, un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un servicio de AWS en OpenSearch Ingestion.

CloudTrail captura todas las llamadas de la API para OpenSearch Ingestion como eventos. Las llamadas capturadas incluyen llamadas desde la sección de OpenSearch Ingestion de la consola de OpenSearch Service y llamadas de código a las operaciones de la API de OpenSearch Ingestion.

Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para OpenSearch Ingestion. Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos.

Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó en OpenSearch Ingestion, la dirección IP desde la cual se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de OpenSearch Ingestion en CloudTrail

CloudTrail se habilita en su Cuenta de AWS cuando la crea. Cuando se produce una actividad en OpenSearch Ingestion, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la Cuenta de AWS. Para más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos en su Cuenta de AWS, incluidos los eventos de OpenSearch Ingestion, 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 registra 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 más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de OpenSearch Ingestion que se documentan en la referencia de API de OpenSearch Ingestion. Por ejemplo, las llamadas a las acciones `CreateCollection`, `ListCollections` y `DeleteCollection` generan entradas en los archivos de log de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad le ayuda a determinar:

- Si la solicitud se realizó con credenciales de usuario de AWS Identity and Access Management (IAM) o credenciales de usuario raíz.
- 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 más información, consulte el elemento userIdentity de CloudTrail.

Descripción de las entradas del archivo de registro de OpenSearch Ingestion

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos de registro de CloudTrail contienen una o varias entradas de registro.

Un evento representa una única solicitud desde cualquier origen. Incluye 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 siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `DeletePipeline`.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDACKCEVSQ6C2EXAMPLE",
        "arn":"arn:aws:iam::123456789012:user/test-user",
        "accountId": "123456789012",
        "accessKeyId": "access-key",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDACKCEVSQ6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-04-21T16:48:33Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-04-21T16:49:22Z",
    "eventSource": "osis.amazonaws.com",
    "eventName": "UpdatePipeline",
    "awsRegion": "us-west-2",
```

```
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36",
    "requestParameters": {
        "pipelineName": "my-pipeline",
        "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
 http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:\n
        log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received: true
\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n"
    },
    "responseElements": {
        "pipeline": {
            "pipelineName": "my-pipeline",sourceIPAddress
            "pipelineArn": "arn:aws:osis:us-west-2:123456789012:pipeline/my-pipeline",
            "minUnits": 1,
            "maxUnits": 1,
            "status": "UPDATING",
            "statusReason": {
                "description": "An update was triggered for the pipeline. It is still
 available to ingest data."
            },
            "pipelineConfigurationBody": "version: \"2\"\nlog-pipeline:\n  source:\n
    http:\n        path: \"/test/logs\"\n  processor:\n    - grok:\n        match:
\n          log: [ '%{COMMONAPACHELOG}' ]\n    - date:\n        from_time_received:
 true\n        destination: \"@timestamp\"\n  sink:\n    - opensearch:\n        hosts:
 [ \"https://search-b5zd22mwxhggheqpj5ftslgyle.us-west-2.es.amazonaws.com\" ]\n
  index: \"apache_logs2\"\n        aws_sts_role_arn: \"arn:aws:iam::709387180454:role/
canary-bootstrap-OsisRole-J1BARLD26QKN\"\n        aws_region: \"us-west-2\"\n
 aws_sigv4: true\n",
            "createdAt": "Mar 29, 2023 1:03:44 PM",
            "lastUpdatedAt": "Apr 21, 2023 9:49:21 AM",
            "ingestEndpointUrls": [
                "my-pipeline-tu33ldsgdltgv7x7tjqiudvf7m.us-west-2.osis.amazonaws.com"
            ]
        }
    },
    "requestID": "12345678-1234-1234-1234-987654321098",
    "eventID": "12345678-1234-1234-1234-987654321098",
    "readOnly": false,
    "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "709387180454",
    "eventCategory": "Management",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "osis.us-west-2.amazonaws.com"
    },
    "sessionCredentialFromConsole": "true"
}
```

Etiquetado de canalizaciones de Amazon OpenSearch Ingestion

Las etiquetas permiten asignar información arbitraria a una canalización de Amazon OpenSearch Ingestion para poder categorizar y filtrar esa información. Una etiqueta es un elemento de metadatos que usted o AWS asigna a un recurso de AWS. Cada etiqueta consta de una key (clave) y un value (valor). En el caso de etiquetas que usted asigna, debe definir la clave y el valor. Por ejemplo, puede definir la clave como `stage` y el valor de un recurso como `test`.

Las etiquetas le ayudan a hacer lo siguiente:

- Identificar y organizar sus recursos de AWS. Muchos servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, podría asignarle la misma etiqueta a una canalización de OpenSearch Ingestion que le conceda a un dominio de Amazon OpenSearch Service.
- Realizar un seguimiento de los costos de AWS. Estas etiquetas se activan en el panel de AWS Billing and Cost Management. AWS usa las etiquetas para clasificar los costos y enviar un informe mensual de asignación de costos. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.
- Restrinja el acceso a las canalizaciones mediante el control de acceso basado en atributos. Para obtener más información, consulte Control de acceso basado en claves de etiquetas en la Guía del usuario de IAM.

En OpenSearch Ingestion, el recurso principal es una canalización. Puede utilizar la consola de OpenSearch Service, la CLI AWS, las API de OpenSearch Ingestion o los SDK de AWS para agregar, administrar y eliminar etiquetas de una canalización.

Temas

Permisos necesarios

OpenSearch Ingestion utiliza los siguientes permisos AWS Identity and Access Management Access Analyzer (IAM) para etiquetar las canalizaciones:

- `osis:TagResource`
- `osis:ListTagsForResource`
- `osis:UntagResource`

Para obtener más información sobre cada permiso, consulte Acciones, recursos y claves de condición de OpenSearch Ingestion en la Referencia de autorizaciones de servicio.

Uso de etiquetas (consola)

La consola es la forma más sencilla para etiquetar una canalización.

Para crear una etiqueta

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación izquierdo, elija Incorporación.
3. Seleccione una canalización a la que desee agregar etiquetas y vaya a la pestaña Etiquetas.
4. Elija Administrar y Agregar nueva etiqueta.
5. Introduzca una clave de etiqueta y un valor opcional.
6. Seleccione guardar.

Para eliminar una etiqueta, siga los mismos pasos y elija Quitar en la página Administrar etiquetas.

Para obtener más información sobre cómo utilizar la consola para trabajar con etiquetas, consulte Tag Editor en la Guía de introducción a la consola de administración de AWS.

Uso de etiquetas (AWS CLI)

Para etiquetar una canalización mediante el AWS CLI, envíe una solicitud `TagResource`:

```
aws osis tag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tags Key=service,Value=osis Key=source,Value=otel
```

Elimine las etiquetas de una canalización mediante el comando `UntagResource`:

```
aws osis untag-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
  --tag-keys service
```

Consulte las etiquetas existentes para una canalización con el comando `ListTagsForResource`:

```
aws osis list-tags-for-resource
  --arn arn:aws:osis:us-east-1:123456789012:pipeline/my-pipeline
```

Registro y monitoreo de Amazon OpenSearch Ingestion con Amazon CloudWatch

Amazon OpenSearch Ingestion publica métricas y registros en Amazon CloudWatch.

Temas

- Monitorear registros de canalización
- Monitoreo de métricas de canalización

Monitorear registros de canalización

Puede habilitar el registro de las canalizaciones de Amazon OpenSearch Ingestion para mostrar los mensajes de error y advertencia que se generen durante las operaciones de canalización y la actividad de incorporación. Amazon OpenSearch Ingestion publica todos los registros en Registros de Amazon CloudWatch. CloudWatch Logs puede monitorear información en los registros y enviarle una notificación cuando se llega a determinados umbrales. También se pueden archivar los datos

de los registros en un almacenamiento de larga duración. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch Logs.

Los registros de OpenSearch Ingestion pueden indicar un error en el procesamiento de solicitudes, errores de autenticación desde el origen hasta el receptor y otras advertencias que pueden resultar útiles para solucionar problemas. Para sus registros, OpenSearch Ingestion utiliza los niveles de registro de `INFO`, `WARN`, `ERROR` y `FATAL`. Recomendamos habilitar la publicación de registros en todas las canalizaciones.

Permisos necesarios

Para habilitar OpenSearch Ingestion a fin de enviar registros a Registros de CloudWatch, debe iniciar sesión como usuario con ciertos permisos de IAM.

Necesita los siguientes permisos de Registros de CloudWatch para crear y actualizar los recursos de entrega de registros:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:PutResourcePolicy",
                "logs:UpdateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:DescribeResourcePolicies",
                "logs:GetLogDelivery",
                "logs:ListLogDeliveries"
            ]
        }
    ]
}
```

Habilitación de la publicación de registros

Puede habilitar la publicación de registros en las canalizaciones existentes o mientras crea una canalización. Para ver los pasos para habilitar la publicación de registros durante la creación de la canalización, consulte the section called “Creación de canalizaciones”.

Consola

Para habilitar la publicación de registros en una canalización existente

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. Elija Incorporación en el panel de navegación izquierdo y seleccione la canalización para la que desea habilitar los registros.
3. Elija Editar opciones de publicación de registros.
4. Seleccione Publicar en Registros de CloudWatch.
5. Cree un grupo de registro nuevo o seleccione uno que ya exista. Se recomienda formatear el nombre como una ruta, por ejemplo`/aws/`**`vendedlogs`**`/OpenSearchIngestion/`*`pipeline-name`*`/audit-logs`. Este formato facilita la aplicación de una política de acceso a CloudWatch que concede permisos a todos los grupos de registros en una ruta específica, como `/aws/vendedlogs/OpenSearchService/OpenSearchIngestion`.

   > **Important**
   >
   > Debe incluir el prefijo `vendedlogs` en el nombre del grupo de registros; de lo contrario, se producirá un error en la creación.

6. Seleccione Save.

CLI

Para habilitar la publicación de registros mediante el AWS CLI, envíe la siguiente solicitud:

```
aws osis update-pipeline \
  --pipeline-name my-pipeline \
  --log-publishing-options  IsLoggingEnabled=true,CloudWatchLogDestination={LogGroup="/
aws/vendedlogs/OpenSearchIngestion/pipeline-name"}
```

Monitoreo de métricas de canalización

Puede monitorear las canalizaciones de Amazon OpenSearch Ingestion mediante Amazon CloudWatch, que recopila y procesa los datos sin procesar y los convierte en métricas legibles y casi en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su

aplicación web o servicio. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

La consola de OpenSearch Ingestion muestra una serie de gráficos basados en los datos sin procesar de CloudWatch en la pestaña Rendimiento de cada canalización.

OpenSearch Ingestion informa de las métricas de la mayoría de los complementos compatibles. Si algunos complementos no tienen su propia tabla a continuación, significa que no muestran ninguna métrica específica de los complementos. Las métricas de canalizaciones se publican en el espacio de nombres de `AWS/OSIS`.

Temas

Métricas comunes

Las siguientes métricas son comunes a todos los procesadores y receptores.

Cada métrica lleva el nombre de la subcanalización y el nombre del complemento, con el formato < *sub_pipeline_name* >< *plugin*><*metric_name* >. Por ejemplo, el nombre completo de la métrica `recordsIn.count` de una subcanalización denominada `my-pipeline` y la fecha del procesador sería `my-pipeline.date.recordsIn.count`.

Sufijo de la métrica	Descripción
`recordsIn.count`	El ingreso de registros a un componente de canalización. Esta métrica se aplica a procesadores y receptores. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`recordsOut.count`	El egreso de registros de un componente de canalización. Esta métrica se aplica a procesadores y orígenes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`timeElapsed.count`	Un recuento de los puntos de datos registrados durante la ejecución de un componente de canalización. Esta métrica se aplica a procesadores y receptores. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`timeElapsed.sum`	El tiempo total transcurrido durante la ejecución de un componente de canalización. Esta métrica se aplica a procesadores y receptores, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`timeElapsed.max`	El tiempo máximo transcurrido durante la ejecución de un componente de canalización. Esta métrica se aplica a procesadores y receptores, en milisegundos.

Sufijo de la métrica	Descripción
	Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas de búfer

Las siguientes métricas se aplican al búfer de bloqueo limitado predeterminado que OpenSearch Ingestion configura automáticamente para todas las canalizaciones.

Cada métrica lleva el prefijo de la subcanalización y el nombre del complemento, con el formato <*sub_pipeline_name*><*buffer_name*><*metric_name*>. Por ejemplo, el nombre completo de la métrica `recordsWritten.count` de una subcanalización denominada `my-pipeline` sería `my-pipeline.BlockingBuffer.recordsWritten.count`.

Sufijo de la métrica	Descripción
`recordsWritten.count`	El número de registros escritos en un búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`recordsRead.count`	El número de registros leídos de un búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`recordsInFlight.value`	El número de registros sin comprobar de un búfer. Estadísticas pertinentes: promedio Dimensión: `PipelineName`
`recordsInBuffer.value`	El número de registros que hay actualmente en un búfer. Estadísticas pertinentes: promedio Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`recordsProcessed.count`	El número de registros leídos de un búfer y procesados por una canalización. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`recordsWriteFailed.count`	El número de registros que la canalización no ha podido escribir en el receptor. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`writeTimeElapsed.count`	Recuento de puntos de datos registrados mientras se escribe en un búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`writeTimeElapsed.sum`	El tiempo total transcurrido durante la escritura en un búfer, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`writeTimeElapsed.max`	El tiempo máximo transcurrido durante la escritura en un búfer, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`writeTimeouts.count`	El recuento de tiempos de espera de escritura en un búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`readTimeElapsed.count`	Recuento de puntos de datos registrados mientras se lee de un búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`readTimeElapsed.sum`	El tiempo total transcurrido mientras se lee de un búfer, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`readTimeElapsed.max`	El tiempo máximo transcurrido mientras se lee de un búfer, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`checkpointTimeElapsed.count`	Un recuento de los puntos de datos registrados durante el punto de control. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`checkpointTimeElapsed.sum`	El tiempo total transcurrido durante el punto de control, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`checkpointTimeElapsed.max`	El tiempo máximo transcurrido durante el punto de control, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas de la V4 de Signature

Las siguientes métricas se aplican al punto de conexión de ingesta de una canalización y están asociadas a los complementos de origen (`http`, `otel_trace`, y `otel_metrics`). Todas las solicitudes al punto de conexión de ingesta deben firmarse con la versión 4 de Signature. Estas métricas pueden ayudarle a identificar los problemas de autorización al conectarse a su canalización o a confirmar que se está autenticando correctamente.

Cada métrica lleva el nombre de la subcanalización como prefijo y `osis_sigv4_auth`. Por ejemplo, *`sub_pipeline_name`*`.osis_sigv4_auth.httpAuthSuccess.count`.

Sufijo de la métrica	Descripción
`httpAuthSuccess.count`	El número de solicitudes de Signature V4 que se han enviado correctamente a la canalización. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`httpAuthFailure.count`	El número de solicitudes fallidas de Signature V4 enviadas a la canalización. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`httpAuthServerError.count`	El número de solicitudes de Signature V4 enviadas a la canalización que arrojaron errores en el servidor. Estadísticas pertinentes: suma

Sufijo de la métrica	Descripción
	Dimensión: `PipelineName`

Métricas del búfer de bloqueo limitado

Las siguientes métricas se aplican al búfer de bloqueo limitado. Cada métrica lleva el nombre de la subcanalización como prefijo y `BlockingBuffer`. Por ejemplo, *`sub_pipeline_name`*`.BlockingBuffer.bufferUsage.value`.

Sufijo de la métrica	Descripción
`bufferUsage.value`	El porcentaje de uso del `buffer_size` se basa en el número de registros del búfer. `buffer_size` represent a el número máximo de registros escritos en el búfer, así como los registros en movimiento que no se han comprobado. Estadísticas pertinentes: promedio Dimensión: `PipelineName`

Métricas de origen de trazas de Otel

Las siguientes métricas se aplican al orígen de trazas de OTel. Cada métrica lleva el nombre de la subcanalización como prefijo y `otel_trace_source`. Por ejemplo, *`sub_pipeline_name`*`.otel_trace_source.requestTimeouts.count`.

Sufijo de la métrica	Descripción
`requestTimeouts.count`	El número de solicitudes que agotaron el tiempo de espera. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestsReceived.count`	El número de solicitudes recibidas por el complemento.

Sufijo de la métrica	Descripción
	Estadísticas pertinentes: suma Dimensión: `PipelineName`
`successRequests.count`	El número de solicitudes que el complemento procesó correctamente. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`badRequests.count`	El número de solicitudes con un formato inválido procesadas por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestsTooLarge.count`	El número de solicitudes cuya cantidad de intervalos en el contenido es superior a la capacidad del búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`internalServerError.count`	El número de solicitudes procesadas por el complemento con un tipo de excepción personalizado. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.count`	Un recuento de los puntos de datos registrados durante el procesamiento de las solicitudes por parte del complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`requestProcessDuration.sum`	La latencia total de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.max`	La latencia máxima de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`payloadSize.count`	Un recuento de la distribución de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.sum`	La distribución total de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.max`	La distribución máxima de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas de OTel: métricas de origen

Las siguientes métricas se aplican al orígen de las métricas de OTel. Cada métrica lleva el nombre de la subcanalización como prefijo y `otel_metrics_source`. Por ejemplo, *`sub_pipeline_name`*`.otel_metrics_source.requestTimeouts.count`.

Sufijo de la métrica	Descripción
`requestTimeouts.count`	El número total de solicitudes al complemento que agotaron el tiempo de espera. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestsReceived.count`	El número total de solicitudes recibidas por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`successRequests.count`	El número de solicitudes procesadas correctamente (código de estado de respuesta de 200) por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.count`	Un recuento de la latencia de las solicitudes procesadas por el complemento, en segundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.sum`	La latencia total de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: suma

Sufijo de la métrica	Descripción
	Dimensión: `PipelineName`
`requestProcessDuration.max`	La latencia máxima de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`payloadSize.count`	Un recuento de la distribución de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.sum`	La distribución total de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.max`	La distribución máxima de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas de Http

Las siguientes métricas se aplican al orígen de HTTP. Cada métrica lleva el nombre de la subcanalización como prefijo y `http`. Por ejemplo, *`sub_pipeline_name`*`.http.requestsReceived.count`.

Sufijo de la métrica	Descripción
`requestsReceived.count`	El número de solicitudes recibidas por el punto de conexión de `/log/ingest` . Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestsRejected.count`	El número de solicitudes rechazadas (código de estado de respuesta de 429) por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`successRequests.count`	El número de solicitudes procesadas correctamente (código de estado de respuesta de 200) por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`badRequests.count`	El número de solicitudes con un tipo o formato de contenido no válido (código de estado de respuesta de 400) procesadas por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestTimeouts.count`	El número de solicitudes que agotan el tiempo de espera en el servidor origen de HTTP (código de estado de respuesta 415). Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`requestsTooLarge.count`	El número de solicitudes cuyo tamaño de eventos en el contenido es superior a la capacidad del búfer (código de estado de respuesta de 413). Estadísticas pertinentes: suma Dimensión: `PipelineName`
`internalServerError.count`	El número de solicitudes procesadas por el complemento con un tipo de excepción personalizado (código de estado de respuesta de 500). Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.count`	Un recuento de la latencia de las solicitudes procesadas por el complemento, en segundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.sum`	La latencia total de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`requestProcessDuration.max`	La latencia máxima de las solicitudes procesadas por el complemento, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`payloadSize.count`	Un recuento de la distribución de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.sum`	La distribución total de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`payloadSize.max`	La distribución máxima de los tamaños de carga útil de las solicitudes entrantes, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas de S3

Las siguientes métricas se aplican a la fuente de S3. Cada métrica lleva el nombre de la subcanalización como prefijo y `s3`. Por ejemplo, *`sub_pipeline_name`*`.s3.s3ObjectsFailed.count`.

Sufijo de la métrica	Descripción
`s3ObjectsFailed.count`	El número total de objetos S3 que el complemento no ha podido leer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectsNotFound.count`	El número de objetos S3 que el complemento no ha podido leer debido a un error `Not  Found` de S3. Estas

Sufijo de la métrica	Descripción
	métricas también se tienen en cuenta para la métrica `s3ObjectsFailed` . Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectsAccessDenied.count`	El número de objetos de S3 que el complemento no ha podido leer debido a un error `Access Denied` o `Forbidden` de S3. Estas métricas también se tienen en cuenta para la métrica `s3ObjectsFailed` . Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectReadTimeElapsed.count`	El tiempo que tarda el complemento en realizar una solicitud GET para un objeto de S3, analizarla y escribir los eventos en el búfer. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectReadTimeElapsed.sum`	El tiempo total que tarda el complemento en realizar una solicitud GET para un objeto de S3, analizarla y escribir los eventos en el búfer, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectReadTimeElapsed.max`	El tiempo máximo que tarda el complemento en realizar una solicitud GET para un objeto de S3, analizarla y escribir los eventos en el búfer, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`s3ObjectSizeBytes.count`	El recuento de la distribución de los tamaños de los objetos de S3, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectSizeBytes.sum`	La distribución de los tamaños de los objetos de S3, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectSizeBytes.max`	La distribución máxima de los tamaños de los objetos de S3, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`s3ObjectProcessedBytes.count`	El recuento de la distribución de los objetos de S3 procesados por el complemento, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectProcessedBytes.sum`	La distribución total de los objetos de S3 procesados por el complemento, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`s3ObjectProcessedBytes.max`	La distribución máxima de los objetos de S3 procesados por el complemento, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`s3ObjectsEvents.count`	El recuento de la distribución de los eventos de S3 recibidos por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectsEvents.sum`	La distribución total de los eventos de S3 recibidos por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3ObjectsEvents.max`	La distribución máxima de los eventos de S3 recibidos por el complemento. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`sqsMessageDelay.count`	Un recuento de puntos de datos registrados mientras S3 registra el tiempo de un evento desde la creación de un objeto hasta el momento en que se analiza por completo. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`sqsMessageDelay.sum`	La cantidad de tiempo total entre el momento en que S3 registra un evento para la creación de un objeto y el momento en que se analiza por completo, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`sqsMessageDelay.max`	La cantidad máxima de tiempo total entre el momento en que S3 registra un evento para la creación de un objeto y el momento en que se analiza por completo, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`s3ObjectsSucceeded.count`	El número de objetos de S3 que el complemento ha leído correctamente. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`sqsMessagesReceived.count`	El número de mensajes de Amazon SQS recibidos de la cola por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`sqsMessagesDeleted.count`	El número de mensajes de Amazon SQS eliminados de la cola por el complemento. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`sqsMessagesFailed.count`	El número de mensajes de Amazon SQS que el complemento no ha podido analizar. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Métricas agrupadas

Las siguientes métricas se aplican al procesador Aggregate. Cada métrica lleva el nombre de la subcanalización como prefijo y `aggregate`. Por ejemplo, *`sub_pipeline_name`*`.aggregate.actionHandleEventsOut.count`.

Sufijo de la métrica	Descripción
`actionHandleEvents Out.count`	El número de eventos que se devolvieron de la llamada `handleEvent` a la acción configurada. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`actionHandleEvents Dropped.count`	El número de eventos que se devolvieron de la llamada `handleEvent` a la acción configurada. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`actionHandleEvents ProcessingErrors.count`	El número de llamadas realizadas a `handleEvent` para la acción configurada que provocaron un error. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`actionConcludeGrou pEventsOut.count`	El número de eventos que se devolvieron de la llamada `concludeGroup` a la acción configurada.

Sufijo de la métrica	Descripción
	Estadísticas pertinentes: suma Dimensión: `PipelineName`
`actionConcludeGroupEventsDropped.count`	El número de eventos que no se devolvieron de la llamada `condludeGroup` a la acción configurada. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`actionConcludeGroupEventsProcessingErrors.count`	El número de llamadas realizadas a `concludeGroup` para la acción configurada que provocaron un error. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`currentAggregateGroups.value`	El número actual de grupos. Este indicador disminuye cuando se concluyen los grupos y aumenta cuando un evento inicia la creación de un grupo nuevo. Estadísticas pertinentes: promedio Dimensión: `PipelineName`

Métricas de fecha

Las siguientes métricas se aplican al procesador Date. Cada métrica lleva el nombre de la subcanalización como prefijo y `date`. Por ejemplo, *`sub_pipeline_name`*`.date.dateProcessingMatchSuccess.count`.

Sufijo de la métrica	Descripción
`dateProcessingMatchSuccess.count`	El número de registros que coinciden con al menos uno de los patrones especificados en la opción `match` de configuración.

Sufijo de la métrica	Descripción
	Estadísticas pertinentes: suma Dimensión: `PipelineName`
`dateProcessingMatchFailure.count`	El número de registros que no coinciden con ninguno de los patrones especificados en la opción `match` de configuración. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Métricas de Grok

Las siguientes métricas se aplican al procesador Grok. Cada métrica lleva el nombre de la subcanalización como prefijo y `grok`. Por ejemplo, *`sub_pipeline_name`*`.grok.grokProcessingMatch.count`.

Sufijo de la métrica	Descripción
`grokProcessingMatch.count`	El número de registros que encontraron con al menos un patrón coincidente en la opción `match` de configuración. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`grokProcessingMismatch.count`	El número de registros que no coinciden con ninguno de los patrones especificados en la opción `match` de configuración. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`grokProcessingErrors.count`	El número de errores de procesamiento de registros. Estadísticas pertinentes: suma

Sufijo de la métrica	Descripción
	Dimensión: `PipelineName`
`grokProcessingTimeouts.count`	El número de registros cuyo tiempo de espera se agotó durante la coincidencia. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`grokProcessingTime.count`	Un recuento de los puntos de datos registrados mientras un registro individual coincidía con los patrones de la opción `match` de configuración. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`grokProcessingTime.sum`	El tiempo total que tarda cada registro individual en coincidir con los patrones de la opción `match` de configuración, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`grokProcessingTime.max`	El tiempo máximo que tarda cada registro individual en coincidir con los patrones de la opción `match` de configuración, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas sin formato de trazas de OTel

Las siguientes métricas se aplican al procesador de trazas sin procesar de OTel. Cada métrica lleva el nombre de la subcanalización como prefijo y `otel_trace_raw`. Por ejemplo, *`sub_pipeline_name`*`.otel_trace_raw.traceGroupCacheCount.value`.

Sufijo de la métrica	Descripción
`traceGroupCacheCount.value`	El número de grupos de trazas en la memoria caché de grupos de trazas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`spanSetCount.value`	El número de conjuntos de intervalos de la colección de conjuntos de intervalos. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Métricas del grupo de trazas de OTel

Las siguientes métricas se aplican al procesador de grupo de trazas de OTel. Cada métrica lleva el nombre de la subcanalización como prefijo y `otel_trace_group`. Por ejemplo, *`sub_pipeline_name`*`.otel_trace_group.recordsInMissingTraceGroup.count`.

Sufijo de la métrica	Descripción
`recordsInMissingTraceGroup.count`	El número de registros de ingreso que faltan en los campos del grupo de trazas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`recordsOutFixedTraceGroup.count`	El número de registros de egreso con campos de grupos de trazas que se completaron correctamente. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`recordsOutMissingTraceGroup.count`	El número de registros de egreso que faltan en los campos del grupo de trazas. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Métricas de estado del mapa de servicio

Las siguientes métricas se aplican al procesador del estado del mapa de servicio. Cada métrica lleva el nombre de la subcanalización como prefijo y `service-map-stateful`. Por ejemplo, *`sub_pipeline_name`*`.service-map-stateful.spansDbSize.count`.

Sufijo de la métrica	Descripción
`spansDbSize.value`	Los tamaños de los bytes en memoria de los intervalos en MapDB durante la duración de la ventana actual y anterior. Estadísticas pertinentes: promedio Dimensión: `PipelineName`
`traceGroupDbSize.value`	Los tamaños de los bytes en memoria de los grupos de trazas en MapDB durante la duración de la ventana actual y anterior. Estadísticas pertinentes: promedio Dimensión: `PipelineName`
`spansDbCount.value`	El recuento de intervalos en MapDB durante la duración de la ventana actual y anterior. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`traceGroupDbCount.value`	El recuento de grupos de trazas en MapDB durante la duración de la ventana actual y anterior. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`relationshipCount.value`	El recuento de las relaciones almacenadas en la duración de la ventana actual y anterior. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Métricas de OpenSearch

Las siguientes métricas se aplican al receptor de OpenSearch. Cada métrica lleva el nombre de la subcanalización como prefijo y `opensearch`. Por ejemplo, *`sub_pipeline_name`*`.opensearch.bulkRequestErrors.count`.

Sufijo de la métrica	Descripción
`bulkRequestErrors.count`	El número total de errores encontrados al enviar solicitud es masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`documentsSuccess.count`	El número de documentos enviados correctamente a OpenSearch Service mediante solicitud masiva, incluidos los reintentos. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`documentsSuccessFirstAttempt.count`	El número de documentos enviados correctamente a OpenSearch Service mediante solicitud masiva en el primer intento. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`documentErrors.count`	El número de documentos que no se pudieron enviar mediante solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestFailed.count`	El número de solicitudes masivas que produjeron un error. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestNumberOfRetries.count`	El número de reintentos de solicitudes masivas fallidas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkBadRequestErrors.count`	El número de errores `Bad Request` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestNotAllowedErrors.count`	El número de errores `Request Not Allowed` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`bulkRequestInvalidInputErrors.count`	El número de errores `Invalid Input` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestNotFoundErrors.count`	El número de errores `Request Not Found` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestTimeoutErrors.count`	El número de errores `Request Timeout` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestServerErrors.count`	El número de errores `Server Error` encontrados al enviar solicitudes masivas. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestSizeBytes.count`	Un recuento de la distribución de los tamaños de carga útil de las solicitudes masivas, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`bulkRequestSizeBytes.sum`	La distribución total de los tamaños de carga útil de las solicitudes masivas, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestSizeBytes.max`	La distribución máxima de los tamaños de carga útil de las solicitudes masivas, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`bulkRequestLatency.count`	Un recuento de los puntos de datos registrados mientras se envían las solicitudes al complemento, incluidos los reintentos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestLatency.sum`	La latencia total de las solicitudes enviadas al complemen to, incluidos los reintentos, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`bulkRequestLatency.max`	La latencia máxima de las solicitudes enviadas al complemento, incluidos los reintentos, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`s3.dlqS3RecordsSuccess.count`	El número de registros que se enviaron correctamente a la cola de correos no solicitados de S3. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RecordsFailed.count`	El número de registros que no se pudieron enviar a la cola de mensajes fallidos de S3. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestSuccess.count`	El número de solicitudes que se enviaron correctamente a la cola de mensajes fallidos de S3. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestFailed.count`	El número de solicitudes fallidas que se enviaron a la cola de mensajes fallidos de S3. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestLatency.count`	Un recuento de los puntos de datos registrados mientras se envían las solicitudes a la cola de mensajes fallidos de S3, incluidos los reintentos. Estadísticas pertinentes: suma Dimensión: `PipelineName`

Sufijo de la métrica	Descripción
`s3.dlqS3RequestLatency.sum`	La latencia total de las solicitudes enviadas a la cola de mensajes fallidos de S3, incluidos los reintentos, en milisegundos. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestLatency.max`	La latencia máxima de las solicitudes enviadas a la cola de mensajes fallidos de S3, incluidos los reintentos, en milisegundos. Estadísticas pertinentes: máximo Dimensión: `PipelineName`
`s3.dlqS3RequestSizeBytes.count`	Un recuento de la distribución de los tamaños de carga útil de las solicitudes a la cola de mensajes fallidos de S3, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestSizeBytes.sum`	La distribución total de los tamaños de carga útil de las solicitudes a la cola de mensajes fallidos de S3, en bytes. Estadísticas pertinentes: suma Dimensión: `PipelineName`
`s3.dlqS3RequestSizeBytes.max`	La distribución máxima de los tamaños de carga útil de las solicitudes a la cola de mensajes fallidos de S3, en bytes. Estadísticas pertinentes: máximo Dimensión: `PipelineName`

Métricas del sistema y de medición

Las siguientes métricas de se aplican al sistema general de OpenSearch Ingestion. Estas métricas no llevan ningún prefijo.

Métrica	Descripción
`system.cpu.usage.value`	El porcentaje de uso de CPU disponible para todos los nodos de datos. Estadísticas pertinentes: promedio Dimensión: `PipelineName` , `area`, `id`
`system.cpu.count.value`	La cantidad total de uso de la CPU para todos los nodos de datos. Estadísticas pertinentes: promedio Dimensión: `PipelineName` , `area`, `id`
`jvm.memory.max.value`	La cantidad máxima de memoria que se puede usar para la administración de la memoria, en bytes. Estadísticas pertinentes: promedio Dimensión: `PipelineName` , `area`, `id`
`jvm.memory.used.value`	La cantidad total de memoria usada, en bytes. Estadísticas pertinentes: promedio Dimensión: `PipelineName` , `area`, `id`signa
`jvm.memory.committ ed.value`	La cantidad de memoria asignada para el uso de la máquina virtual Java (JVM), en bytes. Estadísticas pertinentes: promedio Dimensión: `PipelineName` , `area`, `id`

Métrica	Descripción
`computeUnits`	El número de unidades de cómputo de OpenSearch Ingestion (OCU de ingestión) que utiliza una canalización. Estadísticas relevantes: máximo, suma, promedio Dimensión: `PipelineName`

Prácticas recomendadas para Amazon OpenSearch Ingestion

En este tema se explican las prácticas recomendadas sobre la creación y administración de canalizaciones de Amazon OpenSearch Ingestion e incluye instrucciones generales que se aplican a muchos casos de uso. Cada carga de trabajo es única, con características únicas, por lo que ninguna recomendación genérica es exactamente adecuada para cada caso de uso.

Temas

Prácticas recomendadas generales

Las siguientes prácticas recomendadas generales se aplican a la creación y administración de canalizaciones.

- Para garantizar una alta disponibilidad, configure las canalizaciones de VPC con dos o tres subredes. Si solo implementa una canalización en una subred y la zona de disponibilidad deja de funcionar, no podrá incorporar datos.
- Dentro de cada canalización, recomendamos limitar la cantidad de subcanalizaciones a 5 o menos.
- Si utiliza el complemento de fuente de S3, utilice archivos S3 de tamaño uniforme para obtener un rendimiento óptimo.
- Si utiliza el complemento de fuente de S3, añada 30 segundos de tiempo de espera de visibilidad adicional por cada 0,25 GB de tamaño de archivo del bucket de S3 para obtener un rendimiento óptimo.

- Incluya una cola de mensajes fallidos (DLQ) en la configuración de canalización para poder descargar los eventos fallidos y hacerlos accesibles para su análisis. Si los receptores rechazan los datos debido a mapeos incorrectos u otros problemas, puede enrutar los datos al DLQ para solucionar el problema.

Alarmas de CloudWatch recomendadas

Las alarmas de CloudWatch realizan una acción cuando una métrica de CloudWatch supera un valor especificado para un periodo de tiempo determinado. Por ejemplo, es posible que desee que AWS envíe un email si el estado del clúster es `red` durante más de un minuto. En esta sección se incluyen algunas alarmas recomendadas para Amazon OpenSearch Ingestion y cómo responder a ellas.

Para obtener más información sobre la configuración de las alarmas, consulte Creación de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Alarma	Problema
`computeUnits` máximas es = las `maxUnits` configuradas durante 15 minutos, 3 veces consecutivas	La canalización ha alcanzado su capacidad máxima y es posible que necesite una actualización de `maxUnits`. Aumente la capacidad máxima de su canalización
Suma de `opensearch.documentErrors.count` es = suma de *`{sub_pipeline_name}`*`.opensearch.recordsIn.count` durante 1 minuto, 1 periodo consecutivo	La canalización no puede escribir en el receptor de OpenSearch. Compruebe los permisos de la canalización y confirme que el dominio o la colección están en buen estado. También puede comprobar si hay eventos fallidos en la cola de mensajes fallidos (DLQ), si está configurada.

Alarma	Problema
`bulkRequestLatency.max` máximo es >= x durante 1 minuto, 1 periodo consecutivo	La canalización está experimentando una latencia alta al enviar datos al receptor de OpenSearch. Es probable que esto se deba a que el receptor tiene un tamaño insuficiente o a una mala estrategia de partición, lo que provoca que el receptor quede rezagado. Una latencia alta y sostenida puede afectar el rendimiento de la canalización y es probable que genere una contrapresión para los clientes.
Suma de `httpAuthFailure.count` >= 1 durante 1 minuto, 1 periodo consecutivo	Las solicitudes de ingesta no se autentican. Confirme que todos los clientes tengan habilitada correctamente la autenticación de Signature Version 4.
`system.cpu.usage.value` promedio es >= 80% durante 15 minutos, 3 periodos consecutivos	Un uso elevado y sostenido de la CPU puede resultar problemático. Considere aumentar la capacidad máxima de la canalización.
`bufferUsage.value` promedio es >= 80% durante 15 minutos, 3 periodos consecutivos	Un uso elevado y sostenido del búfer puede resultar problemático. Considere aumentar la capacidad máxima de la canalización.

Otras alarmas para tener en cuenta

Considere configurar las siguientes alarmas en función de las características de Amazon OpenSearch Ingestion que utilice habitualmente.

Alarma	Problema
Suma `dynamodb.exportJobFailure.count` 1	El intento de activar una exportación a Amazon S3 ha fallado.

Alarma	Problema
El promedio es `opensearch.EndtoEndLatency.avg` > X durante 15 minutos, 4 periodos consecutivos	El valor `EndtoEndLatency` es superior al deseado para la lectura de las transmisiones de DynamoDB. Esto puede deberse a un clúster de OpenSearch con una escala insuficiente o a una capacidad máxima de OCU de canalización demasiado baja para el rendimiento de la WCU de la tabla de DynamoDB. `EndtoEndLatency` será mayor después de una exportación, pero debería disminuir con el tiempo a medida que se vaya actualizando con las últimas transmisiones de DynamoDB.
Suma `dyanmodb.changeEventsProcessed.count` == 0 durante X minutos	No se está recopilando ningún registro de las transmisiones de DynamoDB. Esto puede deberse a una falta de actividad en la mesa o a un problema al acceder a las transmisiones de DynamoDB.
Suma de `opensearch.s3.dlqS3RecordsSuccess.count` >= suma de `opensearch.documentSuccess.count` durante 1 minuto, 1 periodo consecutivo	Se envía un número mayor de registros al DLQ que al receptor de OpenSearch. Revise las métricas del complemento del receptor de OpenSearch para investigar y determinar la causa raíz.
Suma de `grok.grokProcessingTimeouts.count` = suma de recordsIn .count durante 1 minuto, 5 períodos consecutivos	Se agota el tiempo de espera de todos los datos mientras el procesador Grok intenta hacer coincidir el patrón. Es probable que esto afecte el rendimiento y ralentice la canalización. Considere ajustar los patrones para reducir los tiempos de espera.

Alarma	Problema
Suma de `grok.grokProcessingErrors.count` es >= 1 durante 1 minuto, 1 periodo consecutivo	El procesador Grok no consigue hacer coincidir los patrones con los datos de la canalización, lo que provoca errores. Revise los datos y las configuraciones del complemento de Grok para asegurarse de que se espera que coincidan los patrones.
Suma de `grok.grokProcessingMismatch.count` = suma de recordsIn.count durante 1 minuto, 5 períodos consecutivos	El procesador Grok no puede hacer coincidir los patrones con los datos de la canalización. Revise los datos y las configuraciones del complemento de Grok para asegurarse de que se espera que coincidan los patrones.
Suma de `date.dateProcessingMatchFailure.count` = suma de recordsIn.count durante 1 minuto, 5 períodos consecutivos	El procesador Date no puede hacer coincidir ningún patrón con los datos de la canalización. Revise los datos y las configuraciones del complemento de Date para asegurarse de que se espera el patrón.
Suma de `s3.s3ObjectsFailed.count` >= 1 durante 1 minuto, 1 periodo consecutivo	Este problema se debe a que el objeto S3 no existe o a que la canalización no tiene privilegios suficientes. Revise las métricas `s3ObjectsNotFound.count` y `s3ObjectsAccessDenied.count` para determinar la causa raíz. Confirme que el objeto S3 existe o actualice los permisos.
Suma de `s3.sqsMessagesFailed.count` >= 1 durante 1 minuto, 1 periodo consecutivo	El complemento S3 no pudo procesar un mensaje de Amazon SQS. Si tiene una DLQ activada en la cola de SQS, revise el mensaje de error. Es posible que la cola esté recibiendo datos no válidos que la canalización está intentando procesar.

Alarma	Problema
Suma de `http.badRequests.count` >= 1 durante 1 minuto, 1 periodo consecutivo	El cliente está enviando una solicitud errónea. Confirme que todos los clientes están enviando la carga útil adecuada.
Suma de `http.requestsTooLarge.count` >= 1 durante 1 minuto, 1 periodo consecutivo	Las solicitudes del complemento de fuente HTTP contienen demasiados datos, lo que supera la capacidad del búfer. Ajuste el tamaño del lote para sus clientes.
Suma de `http.internalServerError.count` >= 0 durante 1 minuto, 1 periodo consecutivo	El complemento de fuente HTTP tiene problemas para recibir eventos.
Suma de `http.requestTimeouts.count` >= 0 durante 1 minuto, 1 periodo consecutivo	Es probable que los tiempos de espera de la fuente se deban a que la canalización está mal aprovisionada. Considere aumentar las `maxUnits` de la canalización para gestionar la carga de trabajo adicional.
Suma de `otel_trace.badRequests.count` >= 1 durante 1 minuto, 1 periodo consecutivo	El cliente está enviando una solicitud errónea. Confirme que todos los clientes están enviando la carga útil adecuada.
Suma de `otel_trace.requestsTooLarge.count` >= 1 durante 1 minuto, 1 periodo consecutivo	Las solicitudes del complemento de fuente de OTel contienen demasiados datos, lo que supera la capacidad del búfer. Ajuste el tamaño del lote para sus clientes.

Alarma	Problema
Suma de `otel_trace.internalServerError.count` >= 0 durante 1 minuto, 1 periodo consecutivo	El complemento de fuente HTTP tiene problemas para recibir eventos.
Suma de `otel_trace.requestTimeouts.count` >= 0 durante 1 minuto, 1 periodo consecutivo	Es probable que los tiempos de espera de la fuente se deban a que la canalización está mal aprovisionada. Considere aumentar las `maxUnits` de la canalización para gestionar la carga de trabajo adicional.
Suma de `otel_metrics.requestTimeouts.count` >= 0 durante 1 minuto, 1 periodo consecutivo	Es probable que los tiempos de espera de la fuente se deban a que la canalización está mal aprovisionada. Considere aumentar las `maxUnits` de la canalización para gestionar la carga de trabajo adicional.

Amazon OpenSearch Serverless

Amazon OpenSearch Serverless es una configuración de autoescalado bajo demanda para Amazon OpenSearch Service. Una colección OpenSearch sin servidor es un OpenSearch clúster que escala la capacidad de cómputo en función de las necesidades de la aplicación. Esto contrasta con los OpenSearch dominios aprovisionados por el OpenSearch servicio, para los que se administra la capacidad de forma manual.

OpenSearch Serverless ofrece una opción sencilla y rentable para cargas de trabajo poco frecuentes, intermitentes o impredecibles. Es rentable porque escala la capacidad de cómputo de forma automática en función del uso de la aplicación.

OpenSearch Las colecciones sin servidor tienen el mismo tipo de volumen de almacenamiento de alta capacidad, distribuido y de alta disponibilidad que utilizan los dominios de servicio aprovisionados. OpenSearch

OpenSearch Las colecciones sin servidor siempre están cifradas. Puede elegir la clave de cifrado, pero no puede desactivar el cifrado. Para obtener más información, consulte the section called “Cifrado”.

Temas

Ventajas

OpenSearch La tecnología sin servidor ofrece las siguientes ventajas:

- Más simple que el aprovisionamiento: OpenSearch sin servidor elimina gran parte de la complejidad de administrar los OpenSearch clústeres y la capacidad. Ajusta y dimensiona de forma automática los clústeres, y se encarga de la administración del ciclo de vida de las particiones y los índices. También gestiona las actualizaciones del software de servicio y las actualizaciones de OpenSearch versiones. Todas las actualizaciones y mejoras no son disruptivas.
- Rentable: cuando utiliza OpenSearch Serverless, solo paga por los recursos que consume. Esto elimina la necesidad del aprovisionamiento inicial y del aprovisionamiento excesivo para las cargas de trabajo máximas.
- Alta disponibilidad: OpenSearch Serverless admite cargas de trabajo de producción con redundancia para proteger contra las interrupciones en las zonas de disponibilidad y los fallos de infraestructura.
- Escalable: OpenSearch Serverless escala automáticamente los recursos para mantener tasas de ingesta de datos y tiempos de respuesta a las consultas consistentemente rápidos.

¿Qué es Amazon OpenSearch Serverless?

Amazon OpenSearch Serverless es una configuración sin servidor bajo demanda para Amazon OpenSearch Service. Serverless elimina las complejidades operativas del aprovisionamiento, la configuración y el ajuste de los clústeres. OpenSearch Es una buena opción para las organizaciones que no desean administrar sus OpenSearch clústeres por sí mismas o para las organizaciones que no cuentan con los recursos o la experiencia dedicados para operar clústeres de gran tamaño. Con OpenSearch Serverless, puede buscar y analizar fácilmente un gran volumen de datos sin tener que preocuparse por la infraestructura subyacente ni por la administración de datos.

Una colección OpenSearch sin servidor es un grupo de OpenSearch índices que funcionan en conjunto para respaldar una carga de trabajo o un caso de uso específicos. Las colecciones son más fáciles de usar que los OpenSearch clústeres autogestionados, que requieren un aprovisionamiento manual.

Las colecciones tienen el mismo tipo de volumen de almacenamiento de alta capacidad, distribuido y de alta disponibilidad que utilizan los dominios de OpenSearch servicio aprovisionados, pero eliminan la complejidad porque no requieren configuración ni ajustes manuales. Los datos se cifran en tránsito dentro de una colección. OpenSearch Serverless también es compatible con los OpenSearch paneles de control, que proporcionan una interfaz intuitiva para analizar los datos.

Las colecciones sin servidor funcionan OpenSearch actualmente con la versión 2.0.x. A medida que se publiquen nuevas versiones, OpenSearch Serverless actualizará automáticamente sus colecciones para incluir nuevas funciones, correcciones de errores y mejoras de rendimiento.

Temas

Casos de uso de OpenSearch Serverless

OpenSearch Serverless admite dos casos de uso principales:

- Análisis de registros: el segmento de análisis de registros se centra en analizar grandes volúmenes de datos de series temporales semiestructurados y generados por máquinas para obtener información operativa y sobre el comportamiento de los usuarios.
- Búsqueda de texto completo: el segmento de búsqueda de texto completo potencia las aplicaciones de sus redes internas (sistemas de administración de contenido, documentos legales) y las aplicaciones orientadas a Internet, como la búsqueda de contenido de sitios web de comercio electrónico.

Al crear una colección, debe elegir uno de estos casos de uso. Para obtener más información, consulte the section called “Elección de un tipo de colección”.

Introducción

Para empezar a usar OpenSearch Serverless, cree una o más colecciones mediante la consola de OpenSearch servicio AWS CLI, el o uno de los AWS SDK. Para ver un tutorial para poner en marcha una colección de forma rápida, consulte the section called “Cómo empezar a usar Serverless OpenSearch ”.

OpenSearch Serverless admite las mismas operaciones de API de ingesta y consulta que la suite de código OpenSearch abierto, por lo que puede seguir utilizando sus clientes y aplicaciones actuales. Sus clientes deben ser compatibles con la versión OpenSearch 2.x para poder funcionar con Serverless. OpenSearch Para obtener más información, consulte the section called “Ingesta de datos en las colecciones”.

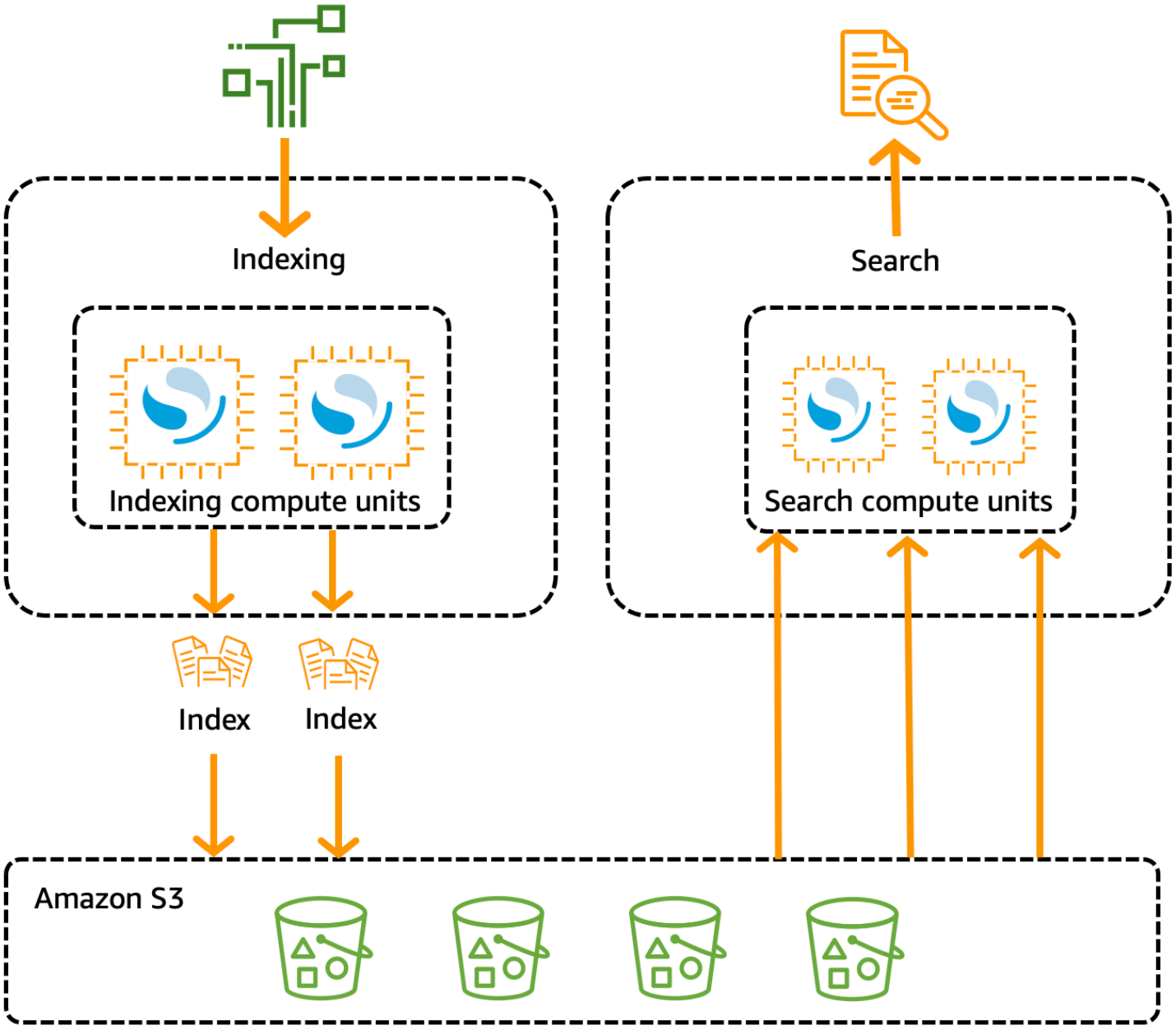
Cómo funcionan

OpenSearch Los clústeres tradicionales tienen un único conjunto de instancias que realizan operaciones de indexación y búsqueda, y el almacenamiento de índices está estrechamente relacionado con la capacidad de procesamiento. Por el contrario, OpenSearch Serverless utiliza una arquitectura nativa de la nube que separa los componentes de indexación (ingesta) de los componentes de búsqueda (consulta), con Amazon S3 como almacenamiento de datos principal para los índices.

Esta arquitectura desacoplada permite escalar las funciones de búsqueda e indexación de forma independiente entre ellas y de los datos indexados en S3. La arquitectura también proporciona aislamiento para las operaciones de ingesta y consulta, de modo que puedan ejecutarse de forma simultánea sin contención de recursos.

Cuando escribe datos en una colección, OpenSearch Serverless los distribuye a las unidades informáticas de indexación. Las unidades de computación de indexación ingieren los datos entrantes y mueven los índices a S3. Al realizar una búsqueda en los datos de la recopilación, OpenSearch Serverless dirige las solicitudes a las unidades de cálculo de búsqueda que contienen los datos que se están consultando. Las unidades de computación de búsqueda descargan los datos indexados de forma directa desde S3 (si aún no están almacenados en la memoria caché local), ejecutan operaciones de búsqueda y realizan agregaciones.

La siguiente imagen ilustra esta arquitectura desacoplada:



OpenSearch La capacidad de cómputo sin servidor para la ingesta, búsqueda y consulta de datos se mide en unidades de OpenSearch cómputo (OCU). Cada OCU es una combinación de 6 GiB de memoria y la CPU virtual (vCPU) correspondiente, así como la transferencia de datos a Amazon S3. Cada OCU incluye suficiente almacenamiento efímero en caliente para 120 GiB de datos de índice.

Al crear la primera colección, OpenSearch Serverless crea una instancia de dos OCU: uno para la indexación y otro para la búsqueda. Para garantizar la alta disponibilidad, también lanza un conjunto de nodos en espera en otra zona de disponibilidad. Para fines de desarrollo y pruebas, puede deshabilitar la configuración Habilitar redundancia para una colección, lo que elimina las dos réplicas en espera y solo crea instancias de dos OCU. De forma predeterminada, las réplicas activas

redundantes están habilitadas, lo que significa que se crean instancias para un total de cuatro OCU para la primera colección de una cuenta.

Estas OCU existen incluso cuando no hay actividad en ningún punto de conexión de la colección. Todas las colecciones posteriores comparten estas OCU. Al crear colecciones adicionales en la misma cuenta, OpenSearch Serverless solo agrega OCU adicionales para buscar e ingerir según sea necesario para respaldar las colecciones, de acuerdo con los límites de capacidad que especifique. La capacidad se reduce a medida que disminuye el uso de la computación.

Para obtener más información sobre cómo se facturan estas OCU, consulte the section called "Precios de Serverless OpenSearch ".

Elección de un tipo de colección

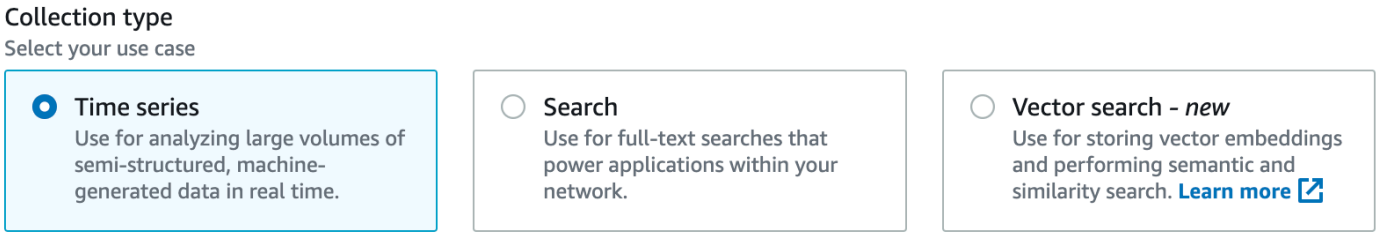
OpenSearch Serverless admite tres tipos de recopilación principales:

Series temporales: el segmento de análisis de registros que se centra en analizar grandes volúmenes de datos semiestructurados generados por máquinas en tiempo real para obtener información operativa, de seguridad, del comportamiento de los usuarios y empresarial.

Búsqueda: búsqueda de texto completo que potencia las aplicaciones de sus redes internas (sistemas de administración de contenido, documentos legales) y las aplicaciones orientadas a Internet, como la búsqueda en sitios web de comercio electrónico y la búsqueda de contenido.

Búsqueda vectorial: búsqueda semántica en incrustaciones vectoriales que simplifica la gestión de datos vectoriales y potencia las experiencias de búsqueda aumentada de machine learning (ML) y las aplicaciones de IA generativa, como chatbots, asistentes personales y detección de fraudes.

El tipo de colección se elige cuando se crea una colección por primera vez:



El tipo de colección que elija dependerá del tipo de datos que piensa incorporar a la colección y de cómo piensa consultarlos. No puede cambiar el tipo de colección después de crearla.

Los tipos de colecciones presentan las siguientes diferencias notables:

- En el caso de las colecciones de búsqueda y de búsqueda vectorial, todos los datos se almacenan en un almacenamiento en caliente para garantizar tiempos de respuesta rápidos a las consultas. Las colecciones de series temporales utilizan una combinación de almacenamiento en caliente y templado, donde los datos más recientes se guardan en un almacenamiento en caliente para optimizar los tiempos de respuesta a las consultas para los datos a los que se accede con más frecuencia.
- En el caso de las colecciones de series temporales y de búsqueda vectorial, no puede indexar por identificador de documento personalizado ni actualizarlas mediante solicitudes indirectas. Esta operación se reserva para los casos de uso de búsqueda. En su lugar, puede actualizar por ID de documento. Para obtener más información, consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.
- Para las recopilaciones de series temporales y de búsqueda, no puede utilizar índices de tipo k-NN.

Precios de Serverless OpenSearch

En OpenSearch Serverless, se cobran los siguientes componentes:

- Computación de la ingesta de datos
- Computación de búsquedas y consultas
- Almacenamiento retenido en Amazon S3

Las OCU se facturan por hora, con un grado de detalle por segundo. En su estado de cuenta, aparece una entrada para la computación en horas de OCU con una etiqueta para la ingesta de datos y otra para la búsqueda. También se cobra de manera mensual por los datos almacenados en Amazon S3. No se le cobrará por usar los OpenSearch paneles de control.

Al crear una colección y habilitar las réplicas activas redundantes, se facturará por un mínimo de cuatro OCU asignadas a las cargas de trabajo. Se facturará por un mínimo de dos OCU para la primera colección de su cuenta si deshabilita las réplicas activas redundantes. Todas las colecciones posteriores pueden compartir esas OCU.

OpenSearch Serverless agrega OCU adicionales en función de la computación necesaria para respaldar sus colecciones. Si su carga de trabajo utiliza una OCU fraccionada, el precio es proporcional. Puede configurar un número máximo de OCU para su cuenta con el fin de controlar los costos.

> **Note**
>
> Las colecciones con OCU únicas no AWS KMS keys pueden compartirse con otras colecciones.

OpenSearch Serverless intenta utilizar los recursos mínimos necesarios para tener en cuenta los cambios en las cargas de trabajo. La cantidad de OCU aprovisionadas en un momento dado puede variar y no es exacta. Con el tiempo, el algoritmo que utiliza OpenSearch Serverless seguirá mejorando para minimizar mejor el uso del sistema.

Para obtener información completa sobre los precios, consulta los precios OpenSearch de Amazon Service.

Soportado Regiones de AWS

OpenSearch Serverless está disponible en un subconjunto de Regiones de AWS ese OpenSearch servicio en el que está disponible. Para ver una lista de las regiones admitidas, consulta los puntos de conexión y las cuotas de Amazon OpenSearch Service en. Referencia general de AWS

Limitaciones

OpenSearch Serverless tiene las siguientes limitaciones:

- Algunas operaciones OpenSearch de la API no son compatibles. Consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.
- Algunos OpenSearch complementos no son compatibles. Consulte the section called “ OpenSearch Plugins compatibles”.
- Actualmente, no hay forma de migrar automáticamente los datos de un dominio de OpenSearch servicio gestionado a una colección sin servidor. Debe volver a indexar los datos desde un dominio a una colección.
- No se admiten el acceso entre cuentas a las colecciones. No puede incluir colecciones de otras cuentas en las políticas de cifrado o de acceso a los datos.
- No se admiten los OpenSearch complementos personalizados.
- No puedes tomar ni restaurar instantáneas de colecciones OpenSearch sin servidor.
- No se admiten la búsqueda y la replicación entre regiones.

- Hay límites para la cantidad de recursos sin servidor que puede tener en una sola cuenta y región. Consulte Cuotas OpenSearch sin servidor.
- El intervalo de actualización de los índices en la búsqueda vectorial y en las colecciones de series temporales es de aproximadamente 60 segundos. El intervalo de actualización de los índices de las colecciones de búsqueda es de aproximadamente 10 segundos.
- El número de fragmentos, el número de intervalos y el intervalo de actualización no se pueden modificar y son gestionados por Serverless. OpenSearch La estrategia de partición se basa en el tipo de colección y el tráfico. Por ejemplo, una colección de series temporales escala las particiones principales en función de los cuellos de botella del tráfico de escritura.
- Se admiten las funciones geoespaciales disponibles en OpenSearch las versiones anteriores a la 2.1.

Comparación entre OpenSearch servicio y sin servidor OpenSearch

En OpenSearch Serverless, algunos conceptos y características son diferentes de su característica correspondiente para un dominio de servicio aprovisionado OpenSearch . Por ejemplo, una diferencia importante es que OpenSearch Serverless no tiene el concepto de clúster o nodo.

En la siguiente tabla se describe en qué se diferencian las funciones y los conceptos importantes de OpenSearch Serverless de la función equivalente de un dominio de servicio aprovisionado OpenSearch .

Característica	OpenSearch Servicio	OpenSearch Sin servidor
Dominios frente a colecciones	Los índices se guardan en dominios, que son clústeres aprovisionados previamente OpenSearch . Para obtener más información, consulte Creación y administración de dominios.	Los índices se encuentran en colecciones, que son agrupaciones lógicas de índices que representan una carga de trabajo o un caso de uso específicos. Para obtener más información, consulte the section called “Crear, mostrar y eliminar colecciones”.
Tipos de nodos y administr	Crea un clúster con tipos de nodos que cumplen con sus especificaciones de coste y rendimiento. Debe calcular	OpenSearch Serverless escala y aprovisiona automáticamente unidades de cómputo adicionales para su cuenta en función del uso de la capacidad.

Característica	OpenSearch Servicio	OpenSearch Sin servidor
ación de la capacidad	sus propios requisitos de almacenamiento y elegir un tipo de instancia para su dominio. Para obtener más informaci ón, consulte the section called “Determinación del tamaño de dominios”.	Para obtener más información, consulte the section called “Administración de los límites de capacidad”.
Facturación	Paga por cada hora de uso de una instancia EC2 y por el tamaño acumulado de cualquier volumen de almacenamiento de EBS adjunto a sus instancias. Para obtener más informaci ón, consulte the section called “Precios de Amazon OpenSearch Service”.	Se le cobrará en horas de OCU por la computación para la ingesta de datos, la computación para las búsquedas y las consultas y el almacenamiento retenido en S3. Para obtener más información, consulte the section called “Precios de Serverless OpenSearch ”.
Cifrado	El cifrado en reposo es opcional para los dominios. Para obtener más informaci ón, consulte the section called “Cifrado en reposo”.	El cifrado en reposo es obligatorio para las colecciones. Para obtener más información, consulte the section called “Cifrado”.
Control de acceso a los datos	El acceso a los datos dentro de los dominios se determina mediante políticas de IAM y un control de acceso detallado.	El acceso a los datos dentro de las colecciones se determina mediante las políticas de acceso a los datos.

Característica	OpenSearch Servicio	OpenSearch Sin servidor
Operaciones compatibles OpenSearch	OpenSearch El servicio admite un subconjunto de todas las operaciones de la OpenSearch API. Para obtener más informaci ón, consulte the section called “Operaciones admitidas”.	OpenSearch Serverless admite un subconjunto diferente de operaciones de OpenSearch API. Para obtener más información, consulte the section called “Operaciones y complementos compatibles”.
Inicio de sesión en Dashboards	Inicio de sesión con un nombre de usuario y una contraseña. Para obtener más informaci ón, consulte the section called “Acceder a los OpenSearc h paneles de control como usuario maestro”.	Si has iniciado sesión en la AWS consola y accedes a la URL de tu panel de control, iniciarás sesión automáticamente. Para obtener más información, consulte the section called “Acceder a los OpenSearch paneles”.
API	Interactúa programáticamente con el OpenSearch Servicio mediante las operaciones de la API del OpenSearch Servicio.	Interactúe mediante programación con OpenSearch Serverless mediante las operaciones de la API Serverless. OpenSearch
Acceso a la red	La configuración de red de un dominio se aplica tanto al punto final del dominio como al punto final de Dashboards. OpenSearch El acceso a la red para ambos está vinculado de forma estrecha.	La configuración de red para el punto final del dominio y el punto final de OpenSearc h Dashboards está disociada. Puede optar por no configurar el acceso a la red para los OpenSearch paneles. Para obtener más información, consulte the section called “Acceso a la red”.

Característica	OpenSearch Servicio	OpenSearch Sin servidor
Firma de solicitudes	Utilice los clientes REST de nivel OpenSearch alto y bajo para firmar las solicitudes. Especifique el nombre del servicio como `es`.	En este momento, OpenSearch Serverless admite un subconjunto de clientes compatibles OpenSearch con Service. Al firmar las solicitudes, especifique el nombre del servicio como `aoss`. El encabezado `x-amz-content-sha256` es obligatorio. Para obtener más información, consulte the section called “Firma de solicitudes HTTP con otros clientes”.
OpenSearch actualizaciones de versión	Los dominios se actualizan manualmente a medida que hay nuevas versiones OpenSearch disponibles de. Es responsable de garantizar que su dominio cumpla con los requisitos de actualización y de que solucionar cualquier cambio importante.	OpenSearch Serverless actualiza automáticamente tus colecciones a nuevas OpenSearch versiones. Las actualizaciones no siempre se producen en cuanto está disponible una nueva versión.
Actualizaciones del software del servicio	De forma manual, aplique las actualizaciones del software del servicio a su dominio a medida que estén disponibles.	OpenSearch Serverless actualiza automáticamente sus colecciones para incluir las últimas correcciones de errores, funciones y mejoras de rendimiento.
Acceso mediante VPC	Puede aprovisionar su dominio dentro de una VPC. También puede crear puntos finales de OpenSearch VPC gestionados por el servicio adicionales para acceder al dominio.	Usted crea uno o más puntos de enlace de VPC OpenSearch gestionados por Serverless para su cuenta. A continuación, incluya estos puntos de conexión dentro de las políticas de red.

Característica	OpenSearch Servicio	OpenSearch Sin servidor
Autenticación SAML	La autenticación SAML se habilita por dominio. Para obtener más informaci ón, consulte the section called “Autenticación SAML para paneles OpenSearch ”.	Configure uno o más proveedores de SAML a nivel de cuenta y, a continuación, incluya los ID de usuario y de grupo asociados dentro de las políticas de acceso a los datos. Para obtener más información, consulte the section called “Autenticación SAML”.
Capa de seguridad de transporte (TSL)	OpenSearch El servicio es compatible con TLS 1.2, pero se recomienda usar TLS 1.3.	OpenSearch Serverless es compatible con TLS 1.2, pero se recomienda usar TLS 1.3.

Introducción a Amazon OpenSearch Serverless

En este tutorial, se explican los pasos básicos para poner en marcha rápidamente una colección de búsquedas de Amazon OpenSearch Serverless. Una colección de búsqueda le permite potenciar las aplicaciones de sus redes internas y las aplicaciones orientadas a Internet, como la búsqueda en sitios web de comercio electrónico y la búsqueda de contenido.

Para obtener información sobre cómo utilizar una colección de búsqueda vectorial, consulte. the section called “Trabajo con colecciones de búsqueda vectorial” Para obtener información detallada sobre el uso de colecciones, consulte the section called “Crear, mostrar y eliminar colecciones” y los demás temas de esta guía.

En este tutorial, deberá completar los siguientes pasos:

1. Configurar permisos
2. Crear una colección
3. Cargar y buscar datos
4. Eliminar la colección

Paso 1: configurar permisos

Para completar este tutorial y utilizar OpenSearch Serverless en general, debe tener los permisos de IAM correctos. En este tutorial, creará una colección, cargará y buscará datos y, a continuación, eliminará la colección.

Su usuario o rol debe tener adjunta una política basada en la identidad con los siguientes permisos mínimos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:UpdateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obtener más información sobre los permisos de IAM OpenSearch sin servidor, consulte. the section called “Identity and Access Management”

Paso 2: crear una colección

Una colección es un grupo de OpenSearch índices que funcionan juntos para respaldar una carga de trabajo o un caso de uso específicos.

Para crear una colección OpenSearch sin servidor

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione Colecciones en el panel de navegación de la izquierda y elija Crear colección.
3. Asigne un nombre a las películas de la colección.
4. Para el tipo de colección, seleccione Buscar. Para obtener más información, consulte Choosing a collection type (Elección de un tipo de recopilación).
5. En Seguridad, selecciona Creación estándar.
6. En Cifrado, selecciona Usar Clave propiedad de AWS. Esto es AWS KMS key lo que OpenSearch Serverless utilizará para cifrar sus datos.
7. En Red, configure los ajustes de red para la colección.
   - Para el tipo de acceso, seleccione Público.
   - Para el tipo de recurso, elija Habilitar el acceso a los OpenSearch puntos finales y Habilitar el acceso a los paneles. OpenSearch Como cargará y buscará datos mediante los OpenSearch paneles de control, debe habilitar ambas opciones.
8. Seleccione Siguiente.
9. En Configurar el acceso a los datos, defina los ajustes de acceso a la colección. Las políticas de acceso a los datos le permiten a los usuarios y a los roles acceder a los datos de una colección. En este tutorial, le brindaremos a un solo usuario los permisos necesarios para indexar y buscar datos en la colección de películas.

   Cree una sola regla que proporcione acceso a la colección películas. Asígnele a la regla el nombre Acceso a la colección de películas.
10. Elija Agregar directores, usuarios y roles de IAM y seleccione el usuario o rol que usará para iniciar sesión en los OpenSearch paneles e indexar datos. Seleccione Guardar.
11. En Indexar permisos, seleccione todos los permisos.
12. Seleccione Siguiente.
13. En la configuración de la política de acceso, seleccione Crear una nueva política de acceso a datos y póngale el nombre películas a la política.
14. Seleccione Siguiente.
15. Revise la configuración de la colección y seleccione Enviar. Espere unos minutos hasta que el estado de la colección cambie a `Active`.

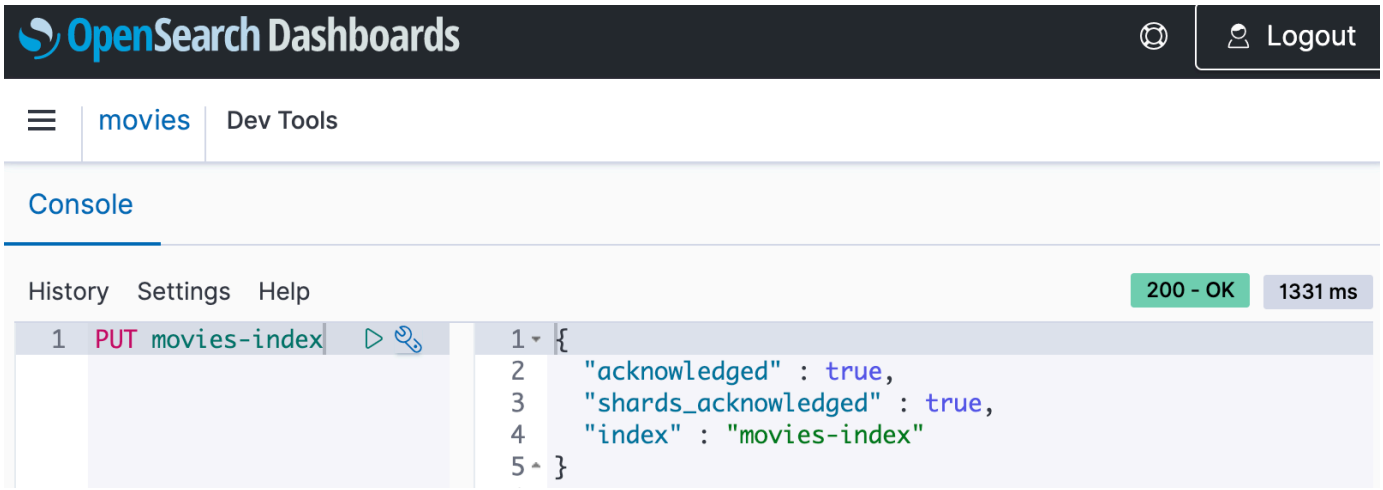
Paso 3: cargar y buscar datos

Puedes cargar datos a una colección OpenSearch sin servidor mediante Postman o cURL. Para abreviar, en estos ejemplos se utilizan las herramientas de desarrollo de la consola de Dashboards. OpenSearch

Para indexar y buscar datos en la colección de películas

1. Seleccione Colecciones en el panel de navegación de la izquierda y elija la colección de películas para abrir su página de detalles.
2. Elija la URL de los OpenSearch paneles de control para la colección. La URL toma el formato `https://dashboards.{region}.aoss.amazonaws.com/_login/?collectionId={collection-id}`.
3. En OpenSearch Dashboards, abra el panel de navegación izquierdo y elija Dev Tools.
4. Para crear un índice único llamado índice de películas, envíe la siguiente solicitud:

```
PUT movies-index
```



5. Para indexar un solo documento en índice de películas, envíe la siguiente solicitud:

```
PUT movies-index/_doc/1
{
  "title": "Shawshank Redemption",
  "genre": "Drama",
  "year": 1994
}
```

6. Para buscar datos en los OpenSearch paneles de control, debe configurar al menos un patrón de índice. OpenSearch utiliza estos patrones para identificar los índices que desea analizar. Abra el menú principal del panel, seleccione Administración de pilas. Luego, seleccione Patrones de índices y, a continuación, seleccione Crear patrón de índice. Para este tutorial, escriba Películas.
7. seleccione Siguiente paso y, a continuación, seleccione Crear patrón de índice. Una vez creado el patrón, puede ver los diversos campos de documento, como `title` y `genre`.
8. Para comenzar a buscar los datos, abra el panel de navegación izquierdo y elija Explorar o utilice la API de búsqueda dentro de Herramientas de desarrollo.

Paso 4: eliminar la colección

Dado que la colección de películas es para hacer pruebas, debe eliminarla cuando termine de experimentar.

Para eliminar una colección OpenSearch sin servidor

1. Vuelve a la consola OpenSearch de Amazon Service.
2. Seleccione Colecciones en el panel de navegación de la izquierda y elija la colección de películas.
3. Seleccione Eliminar y confirme la eliminación.

Siguientes pasos

Ahora que sabe cómo crear una colección e indexar datos, puede que desee probar algunos de los siguientes ejercicios:

- Consulte opciones más avanzadas para crear una colección. Para obtener más información, consulte the section called “Crear, mostrar y eliminar colecciones”.
- Aprenda a configurar las políticas de seguridad para gestionar la seguridad de las colecciones a escala. Para obtener más información, consulte the section called “Seguridad en Serverless OpenSearch ”.
- Descubra otras formas de indexar datos en las colecciones. Para obtener más información, consulte the section called “Ingesta de datos en las colecciones”.

Creación y administración de colecciones de Amazon OpenSearch sin servidor

Puede crear colecciones de Amazon OpenSearch sin servidor mediante la consola, la API y la AWS CLI, los AWS SDK y AWS CloudFormation.

Temas

Crear, publicar y eliminar colecciones de Amazon OpenSearch Serverless

Una colección en Amazon OpenSearch Serverless es una agrupación lógica de uno o más índices que representan una carga de trabajo de análisis. OpenSearch El servicio administra y ajusta automáticamente la recopilación, lo que requiere una intervención manual mínima.

Temas

Permisos necesarios

OpenSearch Serverless utiliza los siguientes permisos AWS Identity and Access Management (IAM) para crear y administrar colecciones. Puede especificar las condiciones de IAM para restringir a los usuarios a colecciones específicas.

- `aoss:CreateCollection`: cree una colección.
- `aoss:ListCollections`: enumere las colecciones en la cuenta actual.

- `aoss:BatchGetCollection`: obtenga detalles sobre una o más colecciones.
- `aoss:UpdateCollection`: modifique una colección.
- `aoss:DeleteCollection`: elimine una colección.

El siguiente ejemplo de política de acceso basada en la identidad proporciona los permisos mínimos necesarios para que un usuario administre una única colección denominada `Logs`:

```
[
   {
      "Sid":"Allows managing logs collections",
      "Effect":"Allow",
      "Action":[
         "aoss:CreateCollection",
         "aoss:ListCollections",
         "aoss:BatchGetCollection",
         "aoss:UpdateCollection",
         "aoss:DeleteCollection",
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringEquals":{
            "aoss:collection":"Logs"
         }
      }
   }
]
```

`aoss:CreateAccessPolicy` y `aoss:CreateSecurityPolicy` se incluyen porque se requieren las políticas de cifrado, de red y de acceso a los datos para que una colección funcione de forma correcta. Para más información, consulte the section called “Identity and Access Management”.

> **Note**
>
> Al crear la primera colección en su cuenta, también necesitará el permiso `iam:CreateServiceLinkedRole`. Para más información, consulte the section called “Rol de creación de colecciones”.

Creación de colecciones

Puede usar la consola o la AWS CLI para crear una colección sin servidor. En estos pasos se explica cómo crear una búsqueda o una colección de series temporales. Para crear una colección de búsquedas vectoriales, consulte the section called “Trabajo con colecciones de búsqueda vectorial”.

Crear una colección (consola)

Para crear una colección mediante la consola

1. Dirígete a la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/.
2. Expanda Sin servidor en el panel de navegación de la izquierda y seleccione Colecciones.
3. Seleccione Crear colección.
4. Escriba un nombre y una descripción para la colección. El nombre debe cumplir los siguientes criterios:
   - Es exclusivo de tu cuenta y Región de AWS
   - Comenzar por una letra minúscula.
   - Contener entre 3 y 32 caracteres
   - Contener solo letras minúsculas de la a a la z, números del 0 al 9 y un guion (-)
5. Seleccione un tipo de colección:
   - Búsqueda: búsqueda de texto completo que potencia las aplicaciones de sus redes internas y las aplicaciones orientadas a Internet. Todos los datos de búsqueda se almacenan en almacenamiento en caliente para garantizar un tiempo de respuesta rápido a las consultas.
   - Series temporales: segmento de análisis de registros que se centra en analizar grandes volúmenes de datos semiestructurados generados por máquinas. Se almacenan al menos 24 horas de datos en los índices calientes y el resto permanece en almacenamiento templado.
   - Búsqueda vectorial: búsqueda semántica en incrustaciones vectoriales que simplifica la administración de datos vectoriales. Impulsa las experiencias de búsqueda aumentada con machine learning (ML) y las aplicaciones de IA generativa, como los chatbots, los asistentes personales y la detección de fraudes.

   Para obtener más información, consulte the section called “Elección de un tipo de colección”.

6. En Tipo de implementación, elige la configuración de redundancia para tu colección. De forma predeterminada, cada colección se crea con redundancia, lo que significa que cada una de las unidades de OpenSearch procesamiento (OCU) de indexación y búsqueda tiene sus propias réplicas en espera en una zona de disponibilidad diferente. Para fines de desarrollo y pruebas, puede optar por deshabilitar la redundancia, lo que reduce a dos el número de OCU de su colección. Para obtener más información, consulte the section called “Cómo funcionan”.
7. En Cifrado, elige una AWS KMS clave con la que cifrar tus datos. OpenSearch Serverless le notifica si el nombre de la colección que ha introducido coincide con un patrón definido en una política de cifrado. Puede optar por mantener esta coincidencia o anularla con una configuración de cifrado única. Para más información, consulte the section called “Cifrado”.
8. En Configuración de acceso a la red, configure el acceso a la red para la colección.

   - En Tipo de acceso, seleccione público o privado. A continuación, especifique qué puntos finales de VPC Servicios de AWS pueden acceder a la colección.
     - Puntos de enlace de VPC para el acceso: especifique uno o más puntos de enlace de VPC para permitir el acceso. Para crear un punto de conexión de VPC, consulte the section called “Puntos de conexión de VPC”.
     - Servicio de AWS acceso privado: seleccione uno o más servicios compatibles a los que permitir el acceso.
   - En el tipo de recurso, seleccione si se podrá acceder a la colección a través de su OpenSearchpunto de enlace (para realizar llamadas a la API mediante curl, Postman, etc.), a través del punto de conexión de OpenSearch Dashboards (para trabajar con las visualizaciones y realizar llamadas a la API a través de la consola) o a través de ambos.

   > **Note**
   >
   > Servicio de AWS El acceso privado solo se aplica al OpenSearch punto final, no al punto final de Dashboards. OpenSearch

   OpenSearch Serverless le notifica si el nombre de la colección que ha introducido coincide con un patrón definido en una política de red. Puede optar por mantener esta coincidencia o anularla con una configuración de red personalizada. Para más información, consulte the section called “Acceso a la red”.
9. (Opcional) Agregue una o varias etiquetas a la colección. Para más información, consulte the section called “Etiquetado de colecciones”.

10. Seleccione Siguiente.
11. Configure las reglas de acceso a los datos de la colección, que definen quién puede acceder a los datos de la colección. Para cada regla que cree, ejecute los siguientes pasos:

    - Seleccione Agregar entidades principales, y luego uno o varios roles de IAM o usuarios y grupos de SAML para proporcionarles acceso a los datos.
    - En Conceder, seleccione los permisos de alias, plantillas e índices que desea conceder a las entidades principales correspondientes. Para obtener una lista completa de los permisos y el acceso que permiten, consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.

    OpenSearch Serverless le notifica si el nombre de la colección que ha introducido coincide con un patrón definido en una política de acceso a datos. Puede optar por mantener esta coincidencia o bien anularla con una configuración de acceso a datos exclusiva. Para más información, consulte the section called “Control de acceso a los datos”.
12. Seleccione Siguiente.
13. En Configuración de la política de acceso a datos, seleccione qué hacer con las reglas que acaba de crear. Puede utilizarlos para crear una nueva política de acceso a datos o bien agregarlos a una política existente.
14. Revise la configuración de la colección y seleccione Enviar.

El estado de la colección cambia a `Creating` cuando OpenSearch Serverless crea la colección.

Para crear una colección (CLI)

Antes de crear una colección mediante el AWS CLI, debe disponer de una política de cifrado con un patrón de recursos que coincida con el nombre previsto de la colección. Por ejemplo, si planea nombrar la colección como registros de la aplicación, puede crear una política de cifrado como esta:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource
\":[\"collection\/logs-application\"]}],\"AWSOwnedKey\":true}"
```

Si piensa utilizar la política para colecciones adicionales, puede hacer que la regla sea más amplia, como `collection/logs*` o `collection/*`.

También debe configurar los ajustes de la red para la colección en forma de política de red. Para seguir con el ejemplo anterior, logs-application, puede crear la siguiente política de red:

```
aws opensearchserverless create-security-policy \
  --name logs-policy \
  --type network --policy "[{\"Description\":\"Public access for logs collection
\",\"Rules\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/logs-
application\"]},{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/logs-
application\"]}],\"AllowFromPublic\":true}]"
```

> **Note**
>
> Es posible crear políticas de red después de crear una colección, pero le recomendamos que lo haga de antemano.

Para crear una colección, envía una CreateCollectionsolicitud:

```
aws opensearchserverless create-collection --name "logs-application" --type SEARCH --
description "A collection for storing log data"
```

En `type`, especifique `SEARCH` o `TIMESERIES`. Para más información, consulte the section called "Elección de un tipo de colección".

Respuesta de ejemplo

```
{
    "createCollectionDetail": {
        "id": "07tjusf2h91cunochc",
        "name": "books",
        "description":"A collection for storing log data",
        "status": "CREATING",
        "type": "SEARCH",
        "kmsKeyArn": "auto",
        "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
        "createdDate": 1665952577473
    }
}
```

Si no especifica ningún tipo de colección en la solicitud, se usa `TIMESERIES` de forma predeterminada. Si su colección está cifrada con un Clave propiedad de AWS, el `kmsKeyArn` es un `auto` en lugar de un ARN.

> **Important**
>
> Después de crear una colección, no podrá acceder a ella a menos que coincida con una política de acceso a los datos. Para obtener instrucciones sobre cómo crear políticas de acceso a los datos, consulte the section called “Control de acceso a los datos”.

Acceder a los OpenSearch paneles

Después de crear una colección con AWS Management Console, puede navegar hasta la URL de los OpenSearch paneles de control de la colección. Para encontrar la URL de Dashboards, seleccione Colecciones en el panel de navegación izquierdo y elija la colección para abrir su página de detalles. La URL toma el formato `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc`. Cuando navegue hasta la URL, iniciará sesión automáticamente en Dashboards.

Si ya tiene disponible la URL de los OpenSearch paneles, pero no está en ella AWS Management Console, si llama a la URL de los paneles desde el navegador, se redirigirá a la consola. Una vez que introduzcas tus AWS credenciales, iniciarás sesión automáticamente en Dashboards. Para obtener información sobre cómo acceder a las colecciones para SAML, consulte Acceder a los OpenSearch paneles de control con SAML.

El tiempo de espera de la consola de OpenSearch Dashboards es de una hora y no se puede configurar.

> **Note**
>
> El 10 de mayo de 2023, OpenSearch introdujimos un punto final global común para los OpenSearch paneles. Ahora puede navegar a los OpenSearch paneles de control en el navegador con una URL que adopte el formato. `https://dashboards.us-east-1.aoss.amazonaws.com/_login/?collectionId=07tjusf2h91cunochc` Para garantizar la compatibilidad con versiones anteriores, seguiremos admitiendo los puntos finales de OpenSearch Dashboards específicos de la colección existente con este formato. `https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/_dashboards`

Visualización de colecciones

Puedes ver las colecciones existentes Cuenta de AWS en la pestaña Colecciones de la consola de Amazon OpenSearch Service.

Para enumerar las colecciones junto con sus ID, envía una ListCollectionssolicitud.

```
aws opensearchserverless list-collections
```

Respuesta de ejemplo

```
{
   "collectionSummaries":[
      {
         "arn":"arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "id":"07tjusf2h91cunochc",
         "name":"my-collection",
         "status":"CREATING"
      }
   ]
}
```

Para limitar los resultados de la búsqueda, utilice filtros de colección. Esta solicitud filtra la respuesta a las colecciones en estado `ACTIVE`:

```
aws opensearchserverless list-collections --collection-filters '{ "status": "ACTIVE" }'
```

Para obtener información más detallada sobre una o más colecciones, incluidos el OpenSearch punto final y el punto final de OpenSearch Dashboards, envía una BatchGetCollectionsolicitud:

```
aws opensearchserverless batch-get-collection --ids ["07tjusf2h91cunochc",
 "1iu5usc4rame"]
```

> **Note**
>
> Puede incluir `--names` o `--ids` en la solicitud, pero no ambos.

Respuesta de ejemplo

```
{
   "collectionDetails":[
      {
         "id": "07tjusf2h91cunochc",
         "name": "my-collection",
         "status": "ACTIVE",
         "type": "SEARCH",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/07tjusf2h91cunochc",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://07tjusf2h91cunochc.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://07tjusf2h91cunochc.us-east-1.aoss.amazonaws.com/
_dashboards"
      },
      {
         "id": "178ukvtg3i82dvopdid",
         "name": "another-collection",
         "status": "ACTIVE",
         "type": "TIMESERIES",
         "description": "",
         "arn": "arn:aws:aoss:us-east-1:123456789012:collection/178ukvtg3i82dvopdid",
         "kmsKeyArn": "arn:aws:kms:us-
east-1:123456789012:key/1234abcd-12ab-34cd-56ef-1234567890ab",
         "createdDate": 1667446262828,
         "lastModifiedDate": 1667446300769,
         "collectionEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com",
         "dashboardEndpoint": "https://178ukvtg3i82dvopdid.us-
east-1.aoss.amazonaws.com/_dashboards"
      }
   ],
   "collectionErrorDetails":[]
}
```


Eliminación de colecciones

Al eliminar una colección, se eliminan todos los datos e índices en la colección. No se pueden recuperar las colecciones después de eliminarlas.

Para eliminar una colección mediante la consola

1. En el panel Colecciones de la consola de Amazon OpenSearch Service, selecciona la colección que deseas eliminar.
2. Seleccione Eliminar y confirme la eliminación.

Para eliminar una colección mediante el AWS CLI, envía una DeleteCollectionsolicitud:

```
aws opensearchserverless delete-collection --id 07tjusf2h91cunochc
```

Respuesta de ejemplo

```
{
   "deleteCollectionDetail":{
      "id":"07tjusf2h91cunochc",
      "name":"my-collection",
      "status":"DELETING"
   }
}
```

Trabajo con colecciones de búsqueda vectorial

El tipo de colección de búsqueda vectorial en OpenSearch Serverless proporciona una capacidad de búsqueda por similitud que es escalable y de alto rendimiento. Le facilita la creación de experiencias de búsqueda aumentada de machine learning (ML) modernas y aplicaciones de inteligencia artificial (IA) generativa sin tener que gestionar la infraestructura de base de datos vectorial subyacente.

Los casos de uso de las colecciones de búsquedas vectoriales incluyen búsquedas de imágenes, búsquedas de documentos, recuperación de música, recomendaciones de productos, búsquedas de vídeos, búsquedas basadas en la ubicación, detección de fraudes y detección de anomalías.

Como el motor vectorial de OpenSearch Serverless funciona con la función de búsqueda del vecino más cercano (k-NN) de la empresa OpenSearch, se obtiene la misma funcionalidad con la sencillez de un entorno sin servidor. El motor admite las operaciones de la API k-NN. OpenSearch Con estas operaciones, puede sacar provecho de la búsqueda de texto completo, el filtrado avanzado, las agregaciones, las consultas geoespaciales, las consultas anidadas para una recuperación más rápida de los datos y la mejora de los resultados de búsqueda.

El motor vectorial proporciona métricas de distancia, como la distancia euclidiana, la similitud de coseno y la similitud de productos de puntos, y puede acomodar 16 000 dimensiones. Puede almacenar campos con varios tipos de datos para los metadatos, como números, valores booleanos, fechas, palabras clave y geopuntos. También puede almacenar campos con texto para obtener información descriptiva y añadir más contexto a los vectores almacenados. La ubicación de los tipos de datos reduce la complejidad, aumenta la capacidad de mantenimiento y evita la duplicación de datos, los problemas de compatibilidad de versiones y los problemas de licencia.

Introducción a las colecciones de búsqueda vectorial

En este tutorial, debe completar los siguientes pasos para almacenar, buscar y recuperar incrustaciones vectoriales en tiempo real:

1. Configurar permisos
2. Crear una colección
3. Cargar y buscar datos
4. Eliminar la colección

Paso 1: configurar permisos

Para completar este tutorial (y para usar OpenSearch Serverless en general), debe tener los permisos AWS Identity and Access Management (de IAM) correctos. En este tutorial, crea una colección, carga y busca datos y, a continuación, elimina la colección.

Su usuario o rol debe tener adjunta una política basada en la identidad con los siguientes permisos mínimos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "aoss:CreateCollection",
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:DeleteCollection",
        "aoss:CreateAccessPolicy",
        "aoss:ListAccessPolicies",
        "aoss:UpdateAccessPolicy",
```

```
        "aoss:CreateSecurityPolicy",
        "iam:ListUsers",
        "iam:ListRoles"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obtener más información sobre los permisos de IAM OpenSearch sin servidor, consulte. the section called “Identity and Access Management”

Paso 2: crear una colección

Una colección es un grupo de OpenSearch índices que funcionan juntos para respaldar una carga de trabajo o un caso de uso específicos.

Para crear una colección OpenSearch sin servidor

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione Colecciones en el panel de navegación de la izquierda y elija Crear colección.
3. Asigne un nombre a la carcasa de la colección.
4. Para el tipo de colección, seleccione Búsqueda vectorial. Para obtener más información, consulte the section called “Elección de un tipo de colección”.
5. En Tipo de implementación, elimine Habilitar redundancia (réplicas activas). Esto crea una colección en modo de desarrollo o prueba y reduce el número de unidades de OpenSearch cómputo (OCU) de la colección a dos. Si desea crear un entorno de producción en este tutorial, deje la casilla seleccionada.
6. En Seguridad, seleccione Crear fácilmente para optimizar la configuración de seguridad. De forma predeterminada, todos los datos del motor vectorial se cifran en tránsito y en reposo. El motor vectorial admite permisos de IAM detallados para que pueda definir quién puede crear, actualizar y eliminar cifrados, redes, colecciones e índices.
7. Seleccione Siguiente.
8. Revise la configuración de la colección y seleccione Enviar. Espere unos minutos hasta que el estado de la colección cambie a `Active`.

Paso 3: cargar y buscar datos

Un índice es una colección de documentos con un esquema de datos común que permite almacenar, buscar y recuperar las incrustaciones vectoriales y otros campos. Puedes crear y cargar datos en los índices de una colección OpenSearch sin servidor mediante la consola Dev Tools de OpenSearch Dashboards o una herramienta HTTP como Postman o awscurl. En este tutorial se utilizan herramientas de desarrollo.

Para indexar y buscar datos en la colección de películas

1. Para crear un índice único para su nueva colección, envíe la siguiente solicitud a la consola de Dev Tools. De forma predeterminada, se crea un índice con un motor `nmslib` y una distancia euclidiana.

```
PUT housing-index
{
   "settings": {
      "index.knn": true
   },
   "mappings": {
      "properties": {
         "housing-vector": {
            "type": "knn_vector",
            "dimension": 3
         },
         "title": {
            "type": "text"
         },
         "price": {
            "type": "long"
         },
         "location": {
            "type": "geo_point"
         }
      }
   }
}
```

2. Para indexar un solo documento en housing-index, envíe la siguiente solicitud:

```
POST housing-index/_doc
{
```

```
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Para buscar propiedades similares a las del índice, envíe la siguiente consulta:

```
GET housing-index/_search
{
    "size": 5,
    "query": {
        "knn": {
            "housing-vector": {
                "vector": [
                    10,
                    20,
                    30
                ],
                "k": 5
            }
        }
    }
}
```

Paso 4: eliminar la colección

Dado que la colección de housing es para hacer pruebas, debe eliminarla cuando termine de experimentar.

Para eliminar una colección OpenSearch sin servidor

1. Vuelve a la consola OpenSearch de Amazon Service.
2. Seleccione Colecciones en el panel de navegación izquierdo y elija la colección de propiedades.
3. Para confirmar la eliminación, seleccione Eliminar.

Búsqueda filtrada

Puede usar filtros para mejorar los resultados de búsqueda semántica. Para crear un índice y realizar una búsqueda filtrada en sus documentos, sustituya los datos de carga y búsqueda en el tutorial anterior por las siguientes instrucciones. Los demás pasos siguen siendo los mismos. Para obtener más información acerca de los filtros, consulte búsqueda k-NN con filtros.

Para indexar y buscar datos en la colección de películas

1. Para crear un índice único para tu colección, envía la siguiente solicitud a la consola de Dev Tools:

```
PUT housing-index-filtered
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "housing-vector": {
        "type": "knn_vector",
        "dimension": 3,
        "method": {
          "engine": "faiss",
          "name": "hnsw"
        }
      },
      "title": {
        "type": "text"
      },
      "price": {
        "type": "long"
      },
      "location": {
        "type": "geo_point"
      }
    }
  }
}
```

2. Para indexar un solo documento housing-index-filtered, envía la siguiente solicitud:

```
POST housing-index-filtered/_doc
{
  "housing-vector": [
    10,
    20,
    30
  ],
  "title": "2 bedroom in downtown Seattle",
  "price": "2800",
  "location": "47.71, 122.00"
}
```

3. Para buscar los datos de un apartamento en Seattle por un precio determinado y dentro de una distancia determinada de un punto geográfico, envíe la siguiente solicitud:

```
GET housing-index-filtered/_search
{
  "size": 5,
  "query": {
    "knn": {
      "housing-vector": {
        "vector": [
          0.1,
          0.2,
          0.3
        ],
        "k": 5,
        "filter": {
          "bool": {
            "must": [
              {
                "query_string": {
                  "query": "Find me 2 bedroom apartment in Seattle under $3000 ",
                  "fields": [
                    "title"
                  ]
                }
              },
              {
                "range": {
                  "price": {
                    "lte": 3000
```

```
                }
              }
            },
            {
              "geo_distance": {
                "distance": "100miles",
                "location": {
                  "lat": 48,
                  "lon": 121
                }
              }
            }
          ]
        }
      }
    }
  }
}
```

Cargas de trabajo a escala de mil millones

Las colecciones de búsquedas vectoriales admiten cargas de trabajo con miles de millones de vectores. No necesita reindexar para escalar porque el escalado automático lo hace por usted. Si tienes millones de vectores (o más) con un gran número de dimensiones y necesitas más de 200 OCU, ponte en contacto con AWS Support para aumentar el número máximo de unidades de OpenSearch cómputo (OCU) de tu cuenta.

Limitaciones

Las colecciones de búsqueda vectorial presentan las siguientes limitaciones:

- Las colecciones de búsqueda vectorial no son compatibles con el motor ANN Apache Lucene.
- Las colecciones de búsqueda vectorial solo admiten el algoritmo HNSW con Faiss y no admiten FIV ni IVFQ.
- Las colecciones de búsqueda vectorial no admiten las operaciones de la API de calentamiento, estadística y entrenamiento de modelos.
- Las colecciones de búsqueda vectorial no admiten scripts en línea ni almacenados.

- La información sobre el recuento de índices no está disponible en las colecciones AWS Management Console de búsquedas vectoriales.
- El intervalo de actualización de los índices de las colecciones de búsqueda vectorial es de 60 segundos.

Siguientes pasos

Ahora que sabe cómo crear una colección de búsquedas vectoriales e indexar datos, puede que desee probar algunos de los siguientes ejercicios:

- Utilice el cliente OpenSearch Python para trabajar con colecciones de búsqueda vectorial. Consulte este tutorial en GitHub.
- Utilice el cliente OpenSearch Java para trabajar con colecciones de búsquedas vectoriales. Consulte este tutorial en GitHub.
- Configurado LangChain para usarse OpenSearch como tienda de vectores. LangChain es un marco de código abierto para desarrollar aplicaciones basadas en modelos de lenguaje. Para obtener más información, consulte la LangChain documentación.

Uso de políticas de ciclo de vida de los datos con Amazon OpenSearch sin servidor

Una política del ciclo de vida de los datos para una colección de series temporales de Amazon OpenSearch sin servidor determina la vida útil de los datos de esa colección. OpenSearch sin servidor conserva los datos durante el período de tiempo que usted configure.

Puede configurar una política de ciclo de vida de los datos independiente para cada índice de cada colección de series temporales de su Cuenta de AWS. OpenSearch sin servidor conserva los documentos en índices durante, como mínimo, el período de retención que configure en la política. A continuación, los borra automáticamente según lo mejor que pueda, normalmente en un plazo de 48 horas o en un 10% del período de retención, lo que sea más largo.

Solo las recopilaciones de series temporales admiten las políticas del ciclo de vida de los datos. No son compatibles con las colecciones de búsqueda o búsqueda vectorial.

Temas

- Políticas de ciclo de vida de los datos

- Permisos necesarios
- Prioridad política
- Sintaxis de la política
- Creación de políticas sobre el ciclo de vida de los datos (AWS CLI)
- Consulta de políticas de ciclo de vida de los datos
- Actualización de políticas de ciclo de vida de los datos
- Eliminación de políticas de ciclo de vida de los datos

Políticas de ciclo de vida de los datos

En una política de ciclo de vida de los datos, se especifica una serie de reglas. La política de ciclo de vida de los datos le permite administrar el período de retención de los datos asociados a los índices o colecciones que cumplen estas reglas. Estas reglas definen el período de retención de los datos de un índice o grupo de índices. Cada regla consta de un tipo de recurso (`index`), un período de retención y una lista de recursos (índices) a los que se aplica el período de retención.

El período de retención se define con uno de los siguientes formatos:

- `"MinIndexRetention": "24h"`: OpenSearch sin servidor conserva los datos del índice durante el período especificado en horas o días. Puede configurar este período para que sea de `24h` a `3650d`.
- `"NoMinIndexRetention": true`: OpenSearch sin servidor conserva los datos del índice de forma indefinida.

En el siguiente ejemplo de política, la primera regla especifica un período de retención de 15 días para todos los índices de la colección `marketing`. La segunda regla especifica que todos los nombres de índice que comiencen por `log` en la colección `finance` no tienen un período de retención establecido y se conservarán indefinidamente.

```
{
   "lifeCyclePolicyDetail": {
      "type": "retention",
      "name": "my-policy",
      "policyVersion": "MTY4ODI0NTM2OTk1N18x",
      "policy": {
         "Rules": [
            {
```

```
            "ResourceType":"index",
            "Resource":[
               "index/marketing/*"
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/finance/log*"
            ],
            "NoMinIndexRetention": true
         }
         ]
      },
      "createdDate": 1688245369957,
      "lastModifiedDate": 1688245369957
   }
}
```

En el siguiente ejemplo de regla de política, OpenSearch sin servidor conserva indefinidamente los datos de todos los índices de todas las colecciones de la cuenta.

```
{
   "Rules": [
      {
         "ResourceType": "index",
         "Resource": [
            "index/*/*"
         ]
      }
   ],
   "NoMinIndexRetention": true
}
```

Permisos necesarios

Las políticas de ciclo de vida para OpenSearch sin servidor utilizan los siguientes permisos AWS Identity and Access Management (IAM). Puede especificar condiciones de IAM para restringir a los usuarios a las políticas de ciclo de vida de los datos asociadas con colecciones e índices específicos.

- `aoss:CreateLifecyclePolicy`: cree una política de ciclo de vida de los datos.

- `aoss:ListLifecyclePolicies`: enumere todas las políticas de ciclo de vida de los datos de la cuenta actual.
- `aoss:BatchGetLifecyclePolicy`: consulte una política del ciclo de vida de los datos asociada a un nombre de cuenta o política.
- `aoss:BatchGetEffectiveLifecyclePolicy`: consulte una política del ciclo de vida de los datos para un recurso determinado (`index` es el único recurso compatible).
- `aoss:UpdateLifecyclePolicy`: modifique una política de ciclo de vida de los datos determinada y cambie su configuración o recurso de retención.
- `aoss:DeleteLifecyclePolicy`: elimine una política de ciclo de vida de los datos.

La siguiente política de acceso basada en identidades permite al usuario ver todas las políticas de ciclo de vida de los datos y actualizarlas según el patrón de recursos `collection/application-logs`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateLifecyclePolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListLifecyclePolicies",
                "aoss:BatchGetLifecyclePolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Prioridad política

Puede haber situaciones en las que las reglas de la política de ciclo de vida de los datos se superpongan, dentro de las políticas o entre ellas. Cuando esto sucede, una regla con un nombre o patrón de recurso más específico para un índice anula una regla con un nombre o patrón de recurso más general para cualquier índice que sea común a ambas reglas.

Por ejemplo, en la siguiente política, se aplican dos reglas a un índice `index/sales/logstash`. En esta situación, la segunda regla tiene prioridad porque `index/sales/log*` es la que coincide más tiempo con `index/sales/logstash`. Por lo tanto, OpenSearch sin servidor no establece ningún período de retención para el índice.

```
{
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/*",
            ],
            "MinIndexRetention": "15d"
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/sales/log*",
            ],
            "NoMinIndexRetention": true
         }
      ]
   }
```

Sintaxis de la política

Proporcione una o más reglas. Estas reglas definen la configuración del ciclo de vida de los datos para los índices de OpenSearch sin servidor.

Cada regla contiene los siguientes elementos. Puede proporcionar `MinIndexRetention` o `NoMinIndexRetention` en cada regla, pero no ambas.

Elemento	Descripción
Tipo de recurso	El tipo de recurso al que se aplica la regla. La única opción admitida para las políticas del ciclo de vida de los datos es `index`.
Recurso	Una lista de nombres o patrones de recursos. Los patrones son prefijos seguidos de un comodín (*), que permiten que los permisos asociados se apliquen a varios recursos. Por ejemplo, `index/`*`<collection-name|pattern>`* `/`*`<index-name|pattern>`* .
Retención mínima de índices	El período mínimo, en días (d) u horas (h), para conservar el documento en el índice. El límite inferior es `24h` y el límite superior es `3650d`.
Sin retención mínima de índices	Si `true`, OpenSearch sin servidor conserva los documentos indefinidamente.

A continuación se muestran algunos ejemplos:

```
{
  "Rules": [
    {
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/*"
      ],
      "MinIndexRetention": "20d"
    },
    {
      "ResourceType": "index",
      "Resource": [
        "index/auto*/gear"
      ],
      "MinIndexRetention": "24h"
    },
    {
```

```
      "ResourceType": "index",
      "Resource": [
        "index/autoparts-inventory/tires"
      ],
      "NoMinIndexRetention": true
    }
  ]
}
```

Creación de políticas sobre el ciclo de vida de los datos (AWS CLI)

Para crear una política de ciclo de vida de los datos mediante las operaciones de la API OpenSearch sin servidor, utilice el comando CreateLifeCyclePolicy. Este comando acepta políticas insertadas y archivos .json. Las políticas insertadas deben codificarse como una cadena de escape de JSON.

La siguiente solicitud crea una política de ciclo de vida de los datos:

```
aws opensearchserverless create-lifecycle-policy \
    --name my-policy \
    --type retention \
    --policy "{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":[\"index/autoparts-
inventory/*\"],\"MinIndexRetention\": \"81d\"},{\"ResourceType\":\"index\",\"Resource
\":[\"index/sales/orders*\"],\"NoMinIndexRetention\":true}]}"
```

Para proporcionar la política en un archivo JSON, utilice el formato`--policy file://my-policy.json`

Consulta de políticas de ciclo de vida de los datos

Antes de crear una colección, puede que desee obtener una vista previa de las políticas de ciclo de vida de los datos existentes en la cuenta para ver cuáles tienen un patrón de recursos que coincide con el nombre de su colección. La siguiente solicitud ListLifecyclePolicies enumera todas las políticas de ciclo de vida de los datos a los datos en su cuenta:

```
aws opensearchserverless list-lifecycle-policies --type retention
```

La solicitud devuelve información sobre todas las políticas de ciclo de vida de los datos configuradas. Para ver las reglas de patrón definidas en una política específica, busque la informaciónde la política en el contenido del elemento `lifecyclePolicySummaries` en la respuesta. Tenga en cuenta el `name` y `type` de esta política y utilice estas propiedades en una solicitud BatchGetLifecyclePolicy para recibir una respuesta con los siguientes detalles de la política:

```
{
    "lifecyclePolicySummaries": [
        {
            "type": "retention",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Para limitar los resultados a políticas que contengan colecciones o índices específicos, puede incluir los siguientes filtros:

```
aws opensearchserverless list-lifecycle-policies --type retention --resources
 "index/autoparts-inventory/*"
```

Para ver información detallada sobre una política específica, utilice el comando BatchGetLifecyclePolicy.

Actualización de políticas de ciclo de vida de los datos

Al actualizar una política de ciclo de vida de los datos, todas las colecciones asociadas se ven afectadas. Para actualizar una política de ciclo de vida de los datos en la consola de OpenSearch sin servidor, amplíe las políticas de ciclo de vida de los datos, seleccione la política que desee modificar y seleccione Editar. Realice los cambios y elija Guardar.

Para actualizar una política de ciclo de vida de los datos mediante la API OpenSearch sin servidor, utilice el comando UpdateLifecyclePolicy. Debe incluir un control de versiones de política en la solicitud. Puede recuperar el control de versiones de la política mediante los comandos `ListLifecyclePolicies` o `BatchGetLifecyclePolicy`. Incluir la versión más reciente de la política garantiza que no se anule inadvertidamente un cambio realizado por otra persona.

La siguiente solicitud actualiza una política del ciclo de vida de los datos con un nuevo documento JSON de política:

```
aws opensearchserverless update-lifecycle-policy \
    --name my-policy \
    --type retention \
```

```
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Pueden transcurrir unos minutos de retardo entre el momento en que se actualiza la política y el momento en que se aplican los nuevos periodos de retención.

Eliminación de políticas de ciclo de vida de los datos

Al eliminar una política del ciclo de vida de los datos, deja de aplicarse a los índices coincidentes. Para eliminar una política en la consola de OpenSearch sin servidor, seleccione la política y elija Eliminar.

También puede utilizar el comando DeleteLifecyclePolicy:

```
aws opensearchserverless delete-lifecycle-policy --name my-policy --type retention
```

Uso de AWS SDK para interactuar con Amazon OpenSearch sin servidor

En esta sección, se incluyen ejemplos de cómo utilizar los AWS SDK para interactuar con la API de configuración de Amazon OpenSearch sin servidor. Estos ejemplos de código muestran cómo crear políticas de seguridad y colecciones, y cómo consultar colecciones.

> **Note**
>
> Actualmente estamos creando estos ejemplos de código. Si quieres contribuir con un ejemplo de código (Java, Go, etc.), abra una solicitud de extracción directamente en el Repositorio de GitHub.

Temas

- Python
- JavaScript

Python

El siguiente script de ejemplo utiliza AWS SDK for Python (Boto3), así como también el cliente para Python opensearch-py para crear políticas de acceso a datos, de cifrado y de redes, crear colecciones de coincidencias e indexar algunos datos de ejemplo.

Ejecute los siguientes comandos para asegurarse de que dispone de todas las dependencias necesarias:

```
pip install opensearch-py
pip install boto3
pip install botocore
pip install requests-aws4auth
```

En el script, reemplace `Principal` por el nombre de recurso de Amazon (ARN) del usuario o rol que firma la solicitud. También puede modificar opcionalmente el archivo `region`.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3
import botocore
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

client = boto3.client('opensearchserverless')
service = 'aoss'
region = 'us-east-1'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def createEncryptionPolicy(client):
    """Creates an encryption policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Encryption policy for TV collections',
            name='tv-policy',
            policy="""
                {
                    \"Rules\":[
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ]
```

```
                        }
                    ],
                    \"AWSOwnedKey\":true
                }
                """,
            type='encryption'
        )
        print('\nEncryption policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] The policy name or rules conflict with an existing
 policy.')
        else:
            raise error


def createNetworkPolicy(client):
    """Creates a network policy that matches all collections beginning with tv-"""
    try:
        response = client.create_security_policy(
            description='Network policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Description\":\"Public access for TV collection\",
                    \"Rules\":[
                        {
                            \"ResourceType\":\"dashboard\",
                            \"Resource\":[\"collection\/tv-*\"]
                        },
                        {
                            \"ResourceType\":\"collection\",
                            \"Resource\":[\"collection\/tv-*\"]
                        }
                    ],
                    \"AllowFromPublic\":true
                }]
                """,
            type='network'
        )
        print('\nNetwork policy created:')
        print(response)
```

```
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A network policy with this name already exists.')
        else:
            raise error


def createAccessPolicy(client):
    """Creates a data access policy that matches all collections beginning with tv-"""
    try:
        response = client.create_access_policy(
            description='Data access policy for TV collections',
            name='tv-policy',
            policy="""
                [{
                    \"Rules\":[
                        {
                            \"Resource\":[
                                \"index\/tv-*\/*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateIndex\",
                                \"aoss:DeleteIndex\",
                                \"aoss:UpdateIndex\",
                                \"aoss:DescribeIndex\",
                                \"aoss:ReadDocument\",
                                \"aoss:WriteDocument\"
                            ],
                            \"ResourceType\": \"index\"
                        },
                        {
                            \"Resource\":[
                                \"collection\/tv-*\"
                            ],
                            \"Permission\":[
                                \"aoss:CreateCollectionItems\"
                            ],
                            \"ResourceType\": \"collection\"
                        }
                    ],
                    \"Principal\":[
                        \"arn:aws:iam::123456789012:role\/Admin\"
                    ]
```

```
                }]
                """,
            type='data'
        )
        print('\nAccess policy created:')
        print(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] An access policy with this name already exists.')
        else:
            raise error


def createCollection(client):
    """Creates a collection"""
    try:
        response = client.create_collection(
            name='tv-sitcoms',
            type='SEARCH'
        )
        return(response)
    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ConflictException':
            print(
                '[ConflictException] A collection with this name already exists. Try
 another name.')
        else:
            raise error


def waitForCollectionCreation(client):
    """Waits for the collection to become active"""
    response = client.batch_get_collection(
        names=['tv-sitcoms'])
    # Periodically check collection status
    while (response['collectionDetails'][0]['status']) == 'CREATING':
        print('Creating collection...')
        time.sleep(30)
        response = client.batch_get_collection(
            names=['tv-sitcoms'])
    print('\nCollection successfully created:')
    print(response["collectionDetails"])
    # Extract the collection endpoint from the response
```

```
    host = (response['collectionDetails'][0]['collectionEndpoint'])
    final_host = host.replace("https://", "")
    indexData(final_host)


def indexData(host):
    """Create an index and add some sample data"""
    # Build the OpenSearch client
    client = OpenSearch(
        hosts=[{'host': host, 'port': 443}],
        http_auth=awsauth,
        use_ssl=True,
        verify_certs=True,
        connection_class=RequestsHttpConnection,
        timeout=300
    )
    # It can take up to a minute for data access rules to be enforced
    time.sleep(45)

    # Create index
    response = client.indices.create('sitcoms-eighties')
    print('\nCreating index:')
    print(response)

    # Add a document to the index.
    response = client.index(
        index='sitcoms-eighties',
        body={
            'title': 'Seinfeld',
            'creator': 'Larry David',
            'year': 1989
        },
        id='1',
    )
    print('\nDocument added:')
    print(response)


def main():
    createEncryptionPolicy(client)
    createNetworkPolicy(client)
    createAccessPolicy(client)
    createCollection(client)
    waitForCollectionCreation(client)
```

```
if __name__ == "__main__":
    main()
```

JavaScript

El siguiente script de ejemplo utiliza el SDK para JavaScript en Node.js, así como también el cliente para JavaScript opensearch-js para crear políticas de acceso a datos, de cifrado y de redes, crear colecciones de coincidencias, crear un índice e indexar algunos datos de ejemplo.

Ejecute los siguientes comandos para asegurarse de que dispone de todas las dependencias necesarias:

```
npm i aws-sdk
npm i aws4
npm i @opensearch-project/opensearch
```

En el script, reemplace `Principal` por el nombre de recurso de Amazon (ARN) del usuario o rol que firma la solicitud. También puede modificar opcionalmente el archivo `region`.

```
var AWS = require('aws-sdk');
var aws4 = require('aws4');
var {
    Client,
    Connection
} = require("@opensearch-project/opensearch");
var {
    OpenSearchServerlessClient,
    CreateSecurityPolicyCommand,
    CreateAccessPolicyCommand,
    CreateCollectionCommand,
    BatchGetCollectionCommand
} = require("@aws-sdk/client-opensearchserverless");
var client = new OpenSearchServerlessClient();

async function execute() {
    await createEncryptionPolicy(client)
    await createNetworkPolicy(client)
    await createAccessPolicy(client)
    await createCollection(client)
    await waitForCollectionCreation(client)
```

```
}

async function createEncryptionPolicy(client) {
    // Creates an encryption policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Encryption policy for TV collections',
            name: 'tv-policy',
            type: 'encryption',
            policy: " \
        { \
            \"Rules\":[ \
                { \
                    \"ResourceType\":\"collection\", \
                    \"Resource\":[ \
                        \"collection\/tv-*\" \
                    ] \
                } \
            ], \
            \"AWSOwnedKey\":true \
        }"
        });
        const response = await client.send(command);
        console.log("Encryption policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] The policy name or rules conflict with an
 existing policy.');
        } else
            console.error(error);
    };
}

async function createNetworkPolicy(client) {
    // Creates a network policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateSecurityPolicyCommand({
            description: 'Network policy for TV collections',
            name: 'tv-policy',
            type: 'network',
            policy: " \
            [{ \
                \"Description\":\"Public access for television collection\", \
```

```
                \"Rules\":[ \
                    { \
                        \"ResourceType\":\"dashboard\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    }, \
                    { \
                        \"ResourceType\":\"collection\", \
                        \"Resource\":[\"collection\/tv-*\"] \
                    } \
                ], \
                \"AllowFromPublic\":true \
            }]"
        });
        const response = await client.send(command);
        console.log("Network policy created:");
        console.log(response['securityPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] A network policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createAccessPolicy(client) {
    // Creates a data access policy that matches all collections beginning with 'tv-'
    try {
        var command = new CreateAccessPolicyCommand({
            description: 'Data access policy for TV collections',
            name: 'tv-policy',
            type: 'data',
            policy: " \
            [{ \
                \"Rules\":[ \
                    { \
                        \"Resource\":[ \
                            \"index\/tv-*\/*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateIndex\", \
                            \"aoss:DeleteIndex\", \
                            \"aoss:UpdateIndex\", \
                            \"aoss:DescribeIndex\", \
```

```
                            \"aoss:ReadDocument\", \
                            \"aoss:WriteDocument\" \
                        ], \
                        \"ResourceType\": \"index\" \
                    }, \
                    { \
                        \"Resource\":[ \
                            \"collection\/tv-*\" \
                        ], \
                        \"Permission\":[ \
                            \"aoss:CreateCollectionItems\" \
                        ], \
                        \"ResourceType\": \"collection\" \
                    } \
                ], \
                \"Principal\":[ \
                    \"arn:aws:iam::123456789012:role\/Admin\" \
                ] \
            }]"
        });
        const response = await client.send(command);
        console.log("Access policy created:");
        console.log(response['accessPolicyDetail']);
    } catch (error) {
        if (error.name === 'ConflictException') {
            console.log('[ConflictException] An access policy with that name already
 exists.');
        } else
            console.error(error);
    };
}

async function createCollection(client) {
    // Creates a collection to hold TV sitcoms indexes
    try {
        var command = new CreateCollectionCommand({
            name: 'tv-sitcoms',
            type: 'SEARCH'
        });
        const response = await client.send(command);
        return (response)
    } catch (error) {
        if (error.name === 'ConflictException') {
```

```
            console.log('[ConflictException] A collection with this name already
 exists. Try another name.');
        } else
            console.error(error);
    };
}

async function waitForCollectionCreation(client) {
    // Waits for the collection to become active
    try {
        var command = new BatchGetCollectionCommand({
            names: ['tv-sitcoms']
        });
        var response = await client.send(command);
        while (response.collectionDetails[0]['status'] == 'CREATING') {
            console.log('Creating collection...')
            await sleep(30000) // Wait for 30 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        console.log('Collection successfully created:');
        console.log(response['collectionDetails']);
        // Extract the collection endpoint from the response
        var host = (response.collectionDetails[0]['collectionEndpoint'])
        // Pass collection endpoint to index document request
        indexDocument(host)
    } catch (error) {
        console.error(error);
    };
}

async function indexDocument(host) {

    var client = new Client({
        node: host,
        Connection: class extends Connection {
            buildRequestObject(params) {
                var request = super.buildRequestObject(params)
                request.service = 'aoss';
                request.region = 'us-east-1'; // e.g. us-east-1
```

```
                var body = request.body;
                request.body = undefined;
                delete request.headers['content-length'];
                request.headers['x-amz-content-sha256'] = 'UNSIGNED-PAYLOAD';
                request = aws4.sign(request, AWS.config.credentials);
                request.body = body;

                return request
            }
        }
    });

    // Create an index
    try {
        var index_name = "sitcoms-eighties";

        var response = await client.indices.create({
            index: index_name
        });

        console.log("Creating index:");
        console.log(response.body);

        // Add a document to the index
        var document = "{ \"title\": \"Seinfeld\", \"creator\": \"Larry David\", \"year
\": \"1989\" }\n";

        var response = await client.index({
            index: index_name,
            body: document
        });

        console.log("Adding document:");
        console.log(response.body);
    } catch (error) {
        console.error(error);
    };
}

execute()
```

Uso de AWS CloudFormation para crear colecciones de Amazon OpenSearch sin servidor

Puede utilizar AWS CloudFormation para crear recursos de Amazon OpenSearch sin servidor, como colecciones, políticas de seguridad y puntos de conexión de VPC. Para obtener la referencia completa de CloudFormation para OpenSearch sin servidor, consulte Amazon OpenSearch sin servidor en la Guía del usuario de AWS CloudFormation.

La siguiente plantilla de ejemplo de CloudFormation crea una política de acceso a datos, una política de red y una política de seguridad simples, así como una colección coincidente. Es una buena forma de empezar a utilizar Amazon OpenSearch sin servidor de forma rápida y de aprovisionar los elementos necesarios para crear y utilizar una colección.

> **Important**
>
> En este ejemplo, se utiliza el acceso a la red pública, que no se recomienda para las cargas de trabajo de producción. Recomendamos utilizar el acceso mediante VPC para proteger las colecciones. Para obtener más información, consulte AWS::OpenSearchServerless::VpcEndpoint y the section called “Puntos de conexión de VPC”.

```
AWSTemplateFormatVersion: 2010-09-09
Description: 'Amazon OpenSearch Serverless template to create an IAM user, encryption
 policy, data access policy and collection'
Resources:
  IAMUSer:
    Type: 'AWS::IAM::User'
    Properties:
      UserName:  aossadmin
  DataAccessPolicy:
    Type: 'AWS::OpenSearchServerless::AccessPolicy'
    Properties:
      Name: quickstart-access-policy
      Type: data
      Description: Access policy for quickstart collection
      Policy: !Sub >-
        [{"Description":"Access for cfn user","Rules":
[{"ResourceType":"index","Resource":["index/*/*"],"Permission":["aoss:*"]},
```

```
        {"ResourceType":"collection","Resource":["collection/quickstart"],"Permission":
["aoss:*"]}],
        "Principal":["arn:aws:iam::${AWS::AccountId}:user/aossadmin"]}]
  NetworkPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-network-policy
      Type: network
      Description: Network policy for quickstart collection
      Policy: >-
        [{"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}, {"ResourceType":"dashboard","Resource":["collection/
quickstart"]}],"AllowFromPublic":true}]
  EncryptionPolicy:
    Type: 'AWS::OpenSearchServerless::SecurityPolicy'
    Properties:
      Name: quickstart-security-policy
      Type: encryption
      Description: Encryption policy for quickstart collection
      Policy: >-
        {"Rules":[{"ResourceType":"collection","Resource":["collection/
quickstart"]}],"AWSOwnedKey":true}
  Collection:
    Type: 'AWS::OpenSearchServerless::Collection'
    Properties:
      Name: quickstart
      Type: TIMESERIES
      Description: Collection to holds timeseries data
    DependsOn: EncryptionPolicy
Outputs:
  IAMUser:
    Value: !Ref IAMUSer
  DashboardURL:
    Value: !GetAtt Collection.DashboardEndpoint
  CollectionARN:
    Value: !GetAtt Collection.Arn
```

Administración de los límites de capacidad de Amazon OpenSearch sin servidor

Con Amazon OpenSearch sin servidor, no tiene que administrar la capacidad usted mismo. OpenSearch sin servidor escala automáticamente la capacidad de procesamiento de su cuenta en

función de la carga de trabajo actual. La capacidad de procesamiento sin servidor se mide en las unidades de cómputo (OCU) de OpenSearch. Cada OCU es una combinación de 6 GiB de memoria y la CPU virtual (vCPU) correspondiente, así como la transferencia de datos a Amazon S3. Para obtener más información sobre la arquitectura desacoplada de OpenSearch sin servidor, consulte the section called “Cómo funcionan”.

Al crear su primera colección, OpenSearch sin servidor crea instancias de un total de cuatro OCU (dos para la indexación y dos para la búsqueda). Siempre existen estas OCU, incluso cuando no hay actividad de indexación o búsqueda. Todas las colecciones posteriores pueden compartir estas OCU (excepto las colecciones con claves únicas AWS KMS, que crean una instancia de su propio conjunto de cuatro OCU). Si es necesario, OpenSearch sin servidor escala horizontalmente de manera automática y agrega OCU adicionales a medida que aumenta el uso de indexación y búsqueda. Cuando el tráfico en el punto de conexión de la colección disminuye, la capacidad vuelve a reducirse verticalmente hasta la cantidad mínima de OCU requerida para el tamaño de los datos. Como máximo, se reducirá verticalmente hasta 2 OCU para indexación y 2 OCU para búsqueda.

En el caso de las colecciones de búsqueda y de búsqueda vectorial, todos los datos se almacenan en índices calientes para garantizar tiempos de respuesta rápidos a las consultas. Las colecciones de series temporales utilizan una combinación de almacenamiento en caliente y templado, lo que guarda los datos más recientes en un almacenamiento en caliente para optimizar los tiempos de respuesta a las consultas para los datos a los que se accede con más frecuencia. Para obtener más información, consulte the section called “Elección de un tipo de colección”.

Para administrar la capacidad de las colecciones y controlar los costos, puede especificar la capacidad máxima general de indexación y búsqueda para la cuenta y región actuales, y OpenSearch sin servidor escala horizontalmente los recursos de las colecciones de manera automática en función de estas especificaciones.

Como la capacidad de indexación y búsqueda se escalan por separado, debe especificar los límites a nivel de cuenta para cada una de ellas:

- Capacidad máxima de indexación: OpenSearch sin servidor puede aumentar la capacidad de indexación hasta este número de OCU.
- Capacidad máxima de búsqueda: OpenSearch sin servidor puede aumentar la capacidad de indexación hasta este número de OCU.

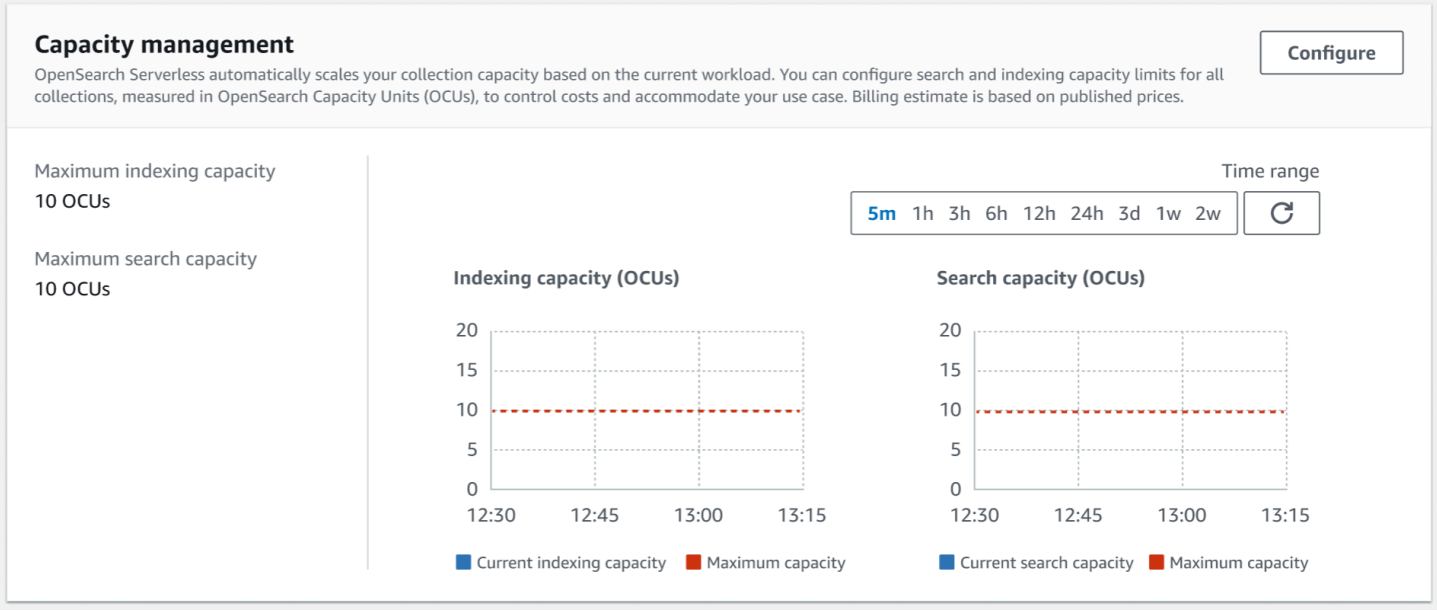
> **Note**
>
> En este momento, la configuración de capacidad solo se aplica según el nivel de cuenta. No puede configurar los límites de capacidad por colección.

El objetivo debe ser garantizar que la capacidad máxima sea lo bastante alta como para asumir los picos de carga de trabajo. Según la configuración, OpenSearch sin servidor escala horizontalmente de manera automática la cantidad de OCU de las colecciones para procesar la carga de trabajo de indexación y búsqueda.

Temas

Como establecer los parámetros de capacidad

Para configurar los ajustes de capacidad en la consola de OpenSearch sin servidor, expanda Sin servidor en el panel de navegación izquierdo y seleccione Panel de control. Especifique la capacidad máxima de indexación y búsqueda en Administración de capacidades:



Para configurar la capacidad mediante la AWS CLI, envíe una solicitud updateAccountSettings:

```
aws opensearchserverless update-account-settings \
    --capacity-limits '{ "maxIndexingCapacityInOCU": 8,"maxSearchCapacityInOCU": 9 }'
```

Límites de la capacidad máxima

Para los tres tipos de colecciones, la capacidad máxima predeterminada es de 10 OCU para la indexación y 10 OCU para la búsqueda. La capacidad mínima permitida para una cuenta es de 2 OCU para la indexación y 2 OCU para la búsqueda. Para las colecciones, la capacidad máxima permitida es de 200 OCU para la indexación y 200 OCU para la búsqueda. Puede configurar el recuento de OCU para que sea cualquier número desde 2 hasta la capacidad máxima permitida, en múltiplos de 2.

Cada OCU incluye suficiente almacenamiento efímero en caliente para 120 GiB de datos de índice. OpenSearch sin servidor admite hasta 1 TiB de datos de índice por colección de búsqueda y búsqueda de vectores, y 10 TiB de datos de índice por colección de series temporales. En el caso de las recopilaciones de series temporales, puede procesar más datos, los cuales pueden almacenarse como datos cálidos en S3.

Para ver una lista de todas las cuotas, consulte cuotas de OpenSearch sin servidor.

Monitoreo del uso de la capacidad

Puede monitorear las métricas de CloudWatch `Search0CU` y `Indexing0CU` a nivel de cuenta para comprender cómo se escalan sus colecciones. Le recomendamos que configure alarmas para que le notifiquen si su cuenta se está acercando a un límite para las métricas relacionadas con la capacidad, de modo que pueda ajustar su configuración de capacidad en consecuencia.

Además, puede utilizar estas métricas para determinar si su configuración de capacidad máxima es adecuada o si necesita ajustarla. Analice estas métricas para centrar sus esfuerzos para optimizar la eficiencia de sus colecciones. Para obtener más información sobre las métricas que OpenSearch sin servidor envía a CloudWatch, consulte the section called “Supervisión sin servidor OpenSearch ”.

Ingerir datos en colecciones de Amazon OpenSearch Serverless

En estas secciones se proporcionan detalles sobre las canalizaciones de ingesta compatibles para la ingesta de datos en las colecciones de Amazon OpenSearch Serverless. También incluyen algunos de los clientes que puede utilizar para interactuar con las operaciones de la API. OpenSearch

Sus clientes deben ser compatibles con la versión OpenSearch 2.x para poder integrarse con OpenSearch Serverless.

Temas

Permisos mínimos necesarios

Para incorporar datos a una colección OpenSearch sin servidor, el director que escribe los datos debe tener los siguientes permisos mínimos asignados en una política de acceso a los datos:

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/target-collection/logs"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:WriteDocument",
               "aoss:UpdateIndex"
            ]
         }
```

```
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Los permisos pueden ser más amplios si planea escribir en índices adicionales. Por ejemplo, en lugar de especificar un único índice de destino, puede conceder permisos a todos los índices (index/*target-collection*/*) o a un subconjunto de índices (index/*target-collection*/*logs**).

Para obtener una referencia de todas las operaciones de OpenSearch API disponibles y sus permisos asociados, consulte. the section called “Operaciones y complementos compatibles”

OpenSearch Ingestión

En lugar de utilizar un cliente de terceros para enviar datos directamente a una colección OpenSearch sin servidor, puede utilizar Amazon OpenSearch Ingestion. Usted configura sus generadores de datos para que envíen datos a OpenSearch Ingestion y esta entrega automáticamente los datos a la colección que usted especifique. También puede configurar OpenSearch Ingestion para transformar los datos antes de entregarlos. Para obtener más información, consulte OpenSearch Ingestión de Amazon.

Una canalización de OpenSearch ingestión necesita permiso para escribir en una colección OpenSearch sin servidor que esté configurada como sumidero. Estos permisos incluyen la capacidad de describir la colección y enviarle solicitudes HTTP.

En primer lugar, cree un rol de IAM que tenga los permisos `aoss:BatchGetCollection` y `aoss:APIAccessAll` para todos los recursos (`*`). A continuación, incluya este rol en una política de acceso a los datos y asígnele permisos para crear índices, actualizar índices, describir índices y escribir documentos dentro de la colección. Por último, especifique el ARN del rol como el valor de la opción sts_role_arn en la configuración de la canalización.

Para obtener instrucciones para completar cada uno de estos pasos, consulte the section called “Otorgar a las canalizaciones acceso a las colecciones”.

Para empezar a usar OpenSearch Ingestion, consulte. the section called “Tutorial: incorporar datos en una colección”

Fluent Bit

Puede utilizar la imagenAWS de Fluent Bit y el complemento OpenSearch de salida para introducir datos en colecciones OpenSearch sin servidor.

> **Note**
>
> Debe tener la versión 2.30.0 o posterior de la imagen de Fluent Bit AWS para poder integrarla con Serverless. OpenSearch

Ejemplo de configuración:

Este ejemplo de sección de resultados del archivo de configuración muestra cómo utilizar una colección OpenSearch Serverless como destino. La adición importante es el parámetro `AWS_Service_Name`, que es `aoss`. `Host` es el punto de conexión de la colección.

```
[OUTPUT]
    Name  opensearch
    Match *
    Host  collection-endpoint.us-west-2.aoss.amazonaws.com
    Port  443
    Index  my_index
    Trace_Error On
    Trace_Output On
    AWS_Auth On
    AWS_Region <region>
    AWS_Service_Name aoss
    tls     On
    Suppress_Type_Name On
```

Amazon Data Firehose

Firehose admite OpenSearch Serverless como destino de entrega. Para obtener instrucciones sobre cómo enviar datos a OpenSearch Serverless, consulte Crear una transmisión de entrega de Kinesis Data Firehose y OpenSearch elegir Serverless para su destino en la Guía para desarrolladores de Amazon Data Firehose.

La función de IAM que le proporciones a Firehose para su entrega debe especificarse en una política de acceso a datos con `aoss:WriteDocument` el permiso mínimo para la recopilación de destino, y

debes tener un índice preexistente al que enviar los datos. Para obtener más información, consulte the section called “Permisos mínimos necesarios”.

Antes de enviar datos a OpenSearch Serverless, es posible que tengas que realizar transformaciones en los datos. Para obtener más información acerca de cómo utilizar las funciones de Lambda para realizar esta tarea, consulte Amazon Kinesis Data Firehose Data Transformation en la misma guía.

Fluentd

Puede usar el OpenSearch complemento Fluentd para recopilar datos de su infraestructura, contenedores y dispositivos de red y enviarlos a OpenSearch colecciones sin servidor. Calyptia mantiene una distribución de Fluentd que contiene todas las dependencias posteriores de Ruby y SSL.

Para usar Fluentd para enviar datos a Serverless OpenSearch

1. Descargue la versión 1.4.2 o posterior de Calyptia Fluentd desde https://www.fluentd.org/download. Esta versión incluye el OpenSearch complemento por defecto, que es compatible con Serverless. OpenSearch
2. Instale el paquete. Siga las instrucciones en la documentación de Fluentd según su sistema operativo:
   - Red Hat Enterprise Linux / CentOS / Amazon Linux
   - Debian / Ubuntu
   - Windows
   - MacOSX
3. Agregue una configuración que envíe datos a OpenSearch Serverless. Esta configuración de ejemplo envía el mensaje “test” a una sola colección. Asegúrese de hacer lo siguiente:
   - Para `host`, especifique el punto final de su colección OpenSearch Serverless.
   - En `aws_service_name`, especifique `aoss`.

```
<source>
@type sample
tag test
```

```
test {"hello":"world"}
</source>

<match test>
@type opensearch
host https://collection-endpoint.us-east-1.aoss.amazonaws.com
port 443
index_name fluentd
aws_service_name aoss
</match>
```

4. Ejecute Calyptia Fluentd para empezar a enviar datos a la colección. Por ejemplo, puede ejecutar el siguiente comando en Mac:

```
sudo launchctl load /Library/LaunchDaemons/calyptia-fluentd.plist
```

Go

El siguiente código de ejemplo utiliza el cliente opensearch-go para Go a fin de establecer una conexión segura con la colección OpenSearch Serverless especificada y crear un índice único. Debe proporcionar valores para `region` y `host`.

```
package main

import (
  "context"
  "log"
  "strings"
  "github.com/aws/aws-sdk-go-v2/aws"
  "github.com/aws/aws-sdk-go-v2/config"
  opensearch "github.com/opensearch-project/opensearch-go/v2"
  opensearchapi "github.com/opensearch-project/opensearch-go/v2/opensearchapi"
  requestsigner "github.com/opensearch-project/opensearch-go/v2/signer/awsv2"
)

const endpoint = "" // serverless collection endpoint

func main() {
 ctx := context.Background()

 awsCfg, err := config.LoadDefaultConfig(ctx,
```

```
 config.WithRegion("<AWS_REGION>"),
 config.WithCredentialsProvider(
  getCredentialProvider("<AWS_ACCESS_KEY>", "<AWS_SECRET_ACCESS_KEY>",
"<AWS_SESSION_TOKEN>"),
 ),
)
if err != nil {
 log.Fatal(err) // don't log.fatal in a production-ready app
}

// create an AWS request Signer and load AWS configuration using default config folder
or env vars.
signer, err := requestsigner.NewSignerWithService(awsCfg, "aoss") // "aoss" for Amazon
OpenSearch Serverless
if err != nil {
 log.Fatal(err) // don't log.fatal in a production-ready app
}

// create an opensearch client and use the request-signer
client, err := opensearch.NewClient(opensearch.Config{
 Addresses: []string{endpoint},
 Signer:    signer,
})
if err != nil {
 log.Fatal("client creation err", err)
}

indexName := "go-test-index"

 // define index mapping
mapping := strings.NewReader(`{
 "settings": {
   "index": {
        "number_of_shards": 4
        }
      }
 }`)

// create an index
createIndex := opensearchapi.IndicesCreateRequest{
 Index: indexName,
   Body: mapping,
}
createIndexResponse, err := createIndex.Do(context.Background(), client)
```

```
 if err != nil {
  log.Println("Error ", err.Error())
  log.Println("failed to create index ", err)
  log.Fatal("create response body read err", err)
 }
 log.Println(createIndexResponse)

 // delete the index
 deleteIndex := opensearchapi.IndicesDeleteRequest{
  Index: []string{indexName},
 }

 deleteIndexResponse, err := deleteIndex.Do(context.Background(), client)
 if err != nil {
  log.Println("failed to delete index ", err)
  log.Fatal("delete index response body read err", err)
 }
 log.Println("deleting index", deleteIndexResponse)
}

func getCredentialProvider(accessKey, secretAccessKey, token string)
 aws.CredentialsProviderFunc {
 return func(ctx context.Context) (aws.Credentials, error) {
  c := &aws.Credentials{
   AccessKeyID:     accessKey,
   SecretAccessKey: secretAccessKey,
   SessionToken:    token,
  }
  return *c, nil
 }
}
```

Java

El siguiente código de ejemplo utiliza el cliente opensearch-java para Java para establecer una conexión segura con la colección OpenSearch Serverless especificada y crear un índice único. Debe proporcionar valores para `region` y `host`.

La diferencia importante en comparación con los dominios de OpenSearch servicio es el nombre del servicio (`aoss`en lugar de). `es`

```
// import OpenSearchClient to establish connection to OpenSearch Serverless collection
import org.opensearch.client.opensearch.OpenSearchClient;
```

```
SdkHttpClient httpClient = ApacheHttpClient.builder().build();

// create an opensearch client and use the request-signer
OpenSearchClient client = new OpenSearchClient(
    new AwsSdk2Transport(
        httpClient,
        "...us-west-2.aoss.amazonaws.com", // serverless collection endpoint
        "aoss" // signing service name
        Region.US_WEST_2, // signing service region
        AwsSdk2TransportOptions.builder().build()
    )
);

String index = "sample-index";

// create an index
CreateIndexRequest createIndexRequest = new
 CreateIndexRequest.Builder().index(index).build();
CreateIndexResponse createIndexResponse = client.indices().create(createIndexRequest);
System.out.println("Create index reponse: " + createIndexResponse);

// delete the index
DeleteIndexRequest deleteIndexRequest = new
 DeleteIndexRequest.Builder().index(index).build();
DeleteIndexResponse deleteIndexResponse = client.indices().delete(deleteIndexRequest);
System.out.println("Delete index reponse: " + deleteIndexResponse);

httpClient.close();
```

JavaScript

El siguiente código de ejemplo utiliza el cliente opensearch-js JavaScript para establecer una conexión segura con la colección OpenSearch Serverless especificada, crear un índice único, agregar un documento y eliminar el índice. Debe proporcionar valores para `node` y `region`.

La diferencia importante en comparación con los dominios de OpenSearch servicio es el nombre del servicio (`aoss`en lugar de). `es`

Version 3

En este ejemplo, se utiliza la versión 3 del SDK para JavaScript Node.js.

```
const { defaultProvider } = require('@aws-sdk/credential-provider-node');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () => {
                const credentialsProvider = defaultProvider();
                return credentialsProvider();
            },
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({ index })).body);
    }

    // add a document to the index
    const document = { foo: 'bar' };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);

    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Version 2

En este ejemplo, se usa la versión 2 del SDK para JavaScript Node.js.

```
const AWS = require('aws-sdk');
const { Client } = require('@opensearch-project/opensearch');
const { AwsSigv4Signer } = require('@opensearch-project/opensearch/aws');

async function main() {
    // create an opensearch client and use the request-signer
    const client = new Client({
        ...AwsSigv4Signer({
            region: 'us-west-2',
            service: 'aoss',
            getCredentials: () =>
                new Promise((resolve, reject) => {
                    AWS.config.getCredentials((err, credentials) => {
                        if (err) {
                            reject(err);
                        } else {
                            resolve(credentials);
                        }
                    });
                }),
        }),
        node: '' # // serverless collection endpoint
    });

    const index = 'movies';

    // create index if it doesn't already exist
    if (!(await client.indices.exists({ index })).body) {
        console.log((await client.indices.create({
            index
        })).body);
    }

    // add a document to the index
    const document = {
        foo: 'bar'
    };
    const response = await client.index({
        id: '1',
        index: index,
        body: document,
    });
    console.log(response.body);
```

```
    // delete the index
    console.log((await client.indices.delete({ index })).body);
}

main();
```

Logstash

Puede usar el OpenSearch complemento Logstash para publicar registros en colecciones OpenSearch sin servidor.

Para usar Logstash para enviar datos a Serverless OpenSearch

1. Instale la versión 2.0.0 o posterior del logstash-output-opensearchcomplemento mediante Docker o Linux.

   Docker

   Docker aloja el software Logstash OSS con el complemento de OpenSearch salida preinstalado: opensearchproject/ -output-plugin. logstash-oss-with-opensearch Puede extraer la imagen como cualquier otra:

   ```
   docker pull opensearchproject/logstash-oss-with-opensearch-output-plugin:latest
   ```

   Linux

   En primer lugar, instale la última versión de Logstash si aún no lo hizo. A continuación, instale la versión 2.0.0 del complemento de salida:

   ```
   cd logstash-8.5.0/
   bin/logstash-plugin install --version 2.0.0 logstash-output-opensearch
   ```

   Si el complemento ya está instalado, actualícelo a la versión más reciente:

   ```
   bin/logstash-plugin update logstash-output-opensearch
   ```

A partir de la versión 2.0.0 del complemento, el SDK usa la versión 3. AWS Si utilizas una versión de Logstash anterior a la 8.4.0, debes eliminar todos los AWS complementos preinstalados e instalar el complemento: `logstash-integration-aws`

```
/usr/share/logstash/bin/logstash-plugin remove logstash-input-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-input-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-s3
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sns
/usr/share/logstash/bin/logstash-plugin remove logstash-output-sqs
/usr/share/logstash/bin/logstash-plugin remove logstash-output-cloudwatch

/usr/share/logstash/bin/logstash-plugin install --version 0.1.0.pre logstash-
integration-aws
```

2. Para que el complemento de OpenSearch salida funcione con OpenSearch Serverless, debes realizar las siguientes modificaciones en la sección de salida de logstash.conf: `opensearch`

   - Especifique `aoss` como el `service_name` en `auth_type`.
   - Especifique el punto de conexión de la colección para `hosts`.
   - Agregue los parámetros `default_server_major_version` y `legacy_template`. Estos parámetros son necesarios para que el complemento funcione con Serverless. OpenSearch

```
output {
  opensearch {
    hosts => "collection-endpoint:443"
    auth_type => {
      ...
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

Este ejemplo de archivo de configuración toma las entradas de los archivos de un bucket de S3 y las envía a una colección OpenSearch Serverless:

```
input {
  s3  {
```

```
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    ecs_compatibility => disabled
    hosts => "https://my-collection-endpoint.us-east-1.aoss.amazonaws.com:443"
    index => my-index
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      service_name => 'aoss'
    }
    default_server_major_version => 2
    legacy_template => false
  }
}
```

3. A continuación, ejecute Logstash con la nueva configuración para probar el complemento:

```
bin/logstash -f config/test-plugin.conf
```

Python

El siguiente código de ejemplo usa el cliente opensearch-py para Python para establecer una conexión segura con la colección OpenSearch Serverless especificada, crear un índice único y buscar en ese índice. Debe proporcionar valores para `region` y `host`.

La diferencia importante en comparación con los dominios de OpenSearch servicio es el nombre del servicio (`aoss`en lugar de). `es`

```
from opensearchpy import OpenSearch, RequestsHttpConnection, AWSV4SignerAuth
import boto3

host = ''  # serverless collection endpoint, without https://
region = ''  # e.g. us-east-1

service = 'aoss'
```

```
credentials = boto3.Session().get_credentials()
auth = AWSV4SignerAuth(credentials, region, service)

# create an opensearch client and use the request-signer
client = OpenSearch(
    hosts=[{'host': host, 'port': 443}],
    http_auth=auth,
    use_ssl=True,
    verify_certs=True,
    connection_class=RequestsHttpConnection,
    pool_maxsize=20,
)

# create an index
index_name = "books-index"
create_response = client.indices.create(
    index_name
)

print('\nCreating index:')
print(create_response)

# index a document
document = {
  'title': 'The Green Mile,
  'director': 'Stephen King',
  'year': '1996'
}

response = client.index(
    index = 'books-index',
    body = document,
    id = '1'
)


# delete the index
delete_response = client.indices.delete(
    index_name
)

print('\nDeleting index:')
print(delete_response)
```

Ruby

La `opensearch-aws-sigv4` gema proporciona acceso a OpenSearch Serverless, junto con OpenSearch Service, de forma inmediata. Dispone de todas las funciones del cliente opensearch-ruby, ya que es una dependencia de esta gema.

Cuando cree una instancia del firmante de Sigv4, especifique `aoss` como nombre del servicio:

```
require 'opensearch-aws-sigv4'
require 'aws-sigv4'

signer = Aws::Sigv4::Signer.new(service: 'aoss',
                                region: 'us-west-2',
                                access_key_id: 'key_id',
                                secret_access_key: 'secret')

# create an opensearch client and use the request-signer
client = OpenSearch::Aws::Sigv4Client.new(
  { host: 'https://your.amz-opensearch-serverless.endpoint',
    log: true },
  signer)

# create an index
index = 'prime'
client.indices.create(index: index)

# insert data
client.index(index: index, id: '1', body: { name: 'Amazon Echo',
                                            msrp: '5999',
                                            year: 2011 })

# query the index
client.search(body: { query: { match: { name: 'Echo' } } })

# delete index entry
client.delete(index: index, id: '1')

# delete the index
client.indices.delete(index: index)
```

Firma de solicitudes HTTP con otros clientes

Los siguientes requisitos se aplican al firmar solicitudes en colecciones OpenSearch sin servidor cuando se crean solicitudes HTTP con otros clientes.

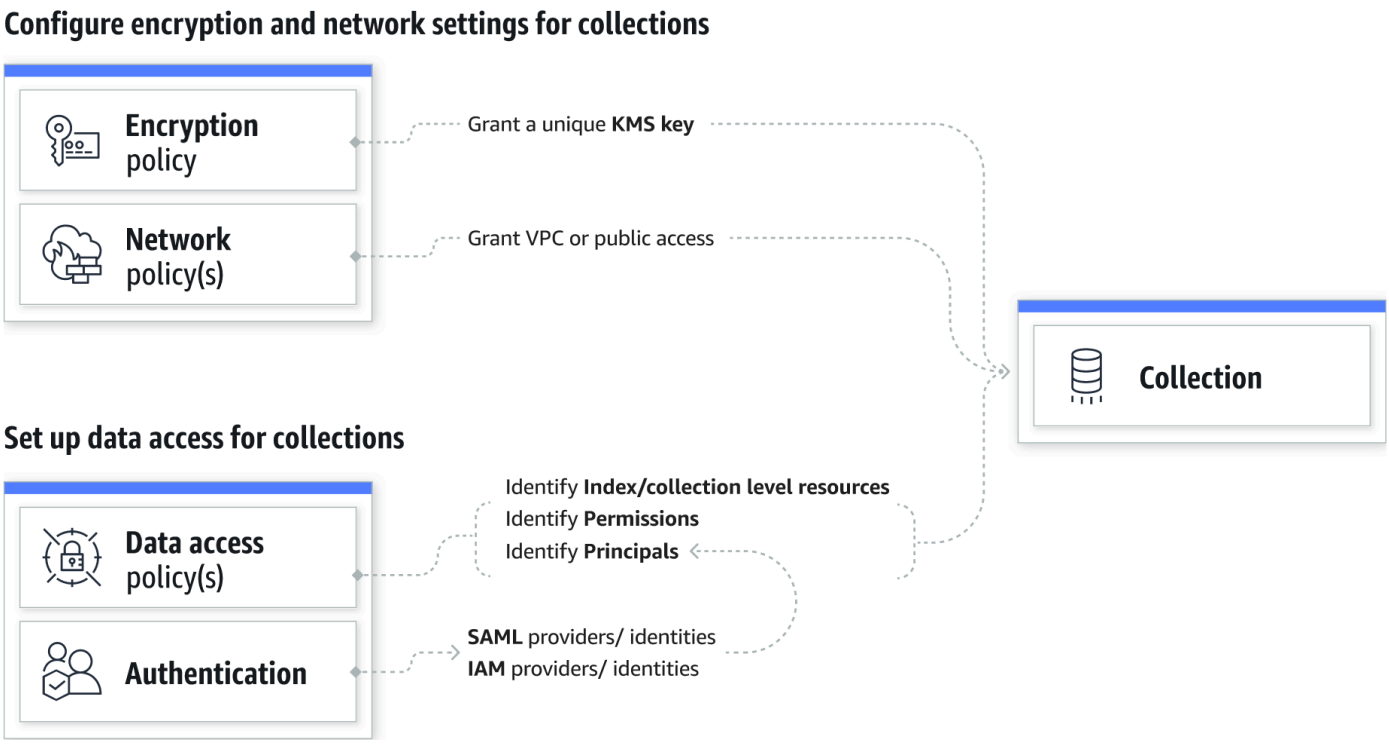
- Debe especificar el nombre del servicio como `aoss`.
- El encabezado `x-amz-content-sha256` es obligatorio para todas las solicitudes de Signature Version 4 de AWS . Proporciona un hash de la carga de solicitud. Si hay una carga de solicitud, establezca el valor en su hash criptográfico del algoritmo de hash seguro (SHA) (SHA256). Si no hay ninguna carga de solicitud, establezca el valor en `e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855`, que es el hash de una cadena vacía.

Descripción general de la seguridad en Amazon OpenSearch Serverless

La seguridad de Amazon OpenSearch Serverless se diferencia fundamentalmente de la seguridad de Amazon OpenSearch Service en los siguientes aspectos:

Característica	OpenSearch Servicio	OpenSearch Sin servidor
Control de acceso a los datos	El acceso a los datos está determinado por las políticas de IAM y el control de acceso detallado.	El acceso a los datos está determinado por las políticas de acceso a los datos.
Cifrado en reposo	El cifrado en reposo es opcional para los dominios.	El cifrado en reposo es obligator io para las colecciones.
Configuración y administración de seguridad	Debe configurar la red, el cifrado y el acceso a los datos de forma individual para cada dominio.	Puede usar políticas de seguridad para administrar la configuración de seguridad de varias colecciones a escala.

El siguiente diagrama ejemplifica los componentes de seguridad que componen una colección funcional. A una colección se le debe asignar una clave de cifrado, una configuración de acceso a la red y una política de acceso a los datos coincidente que otorgue permisos a sus recursos.



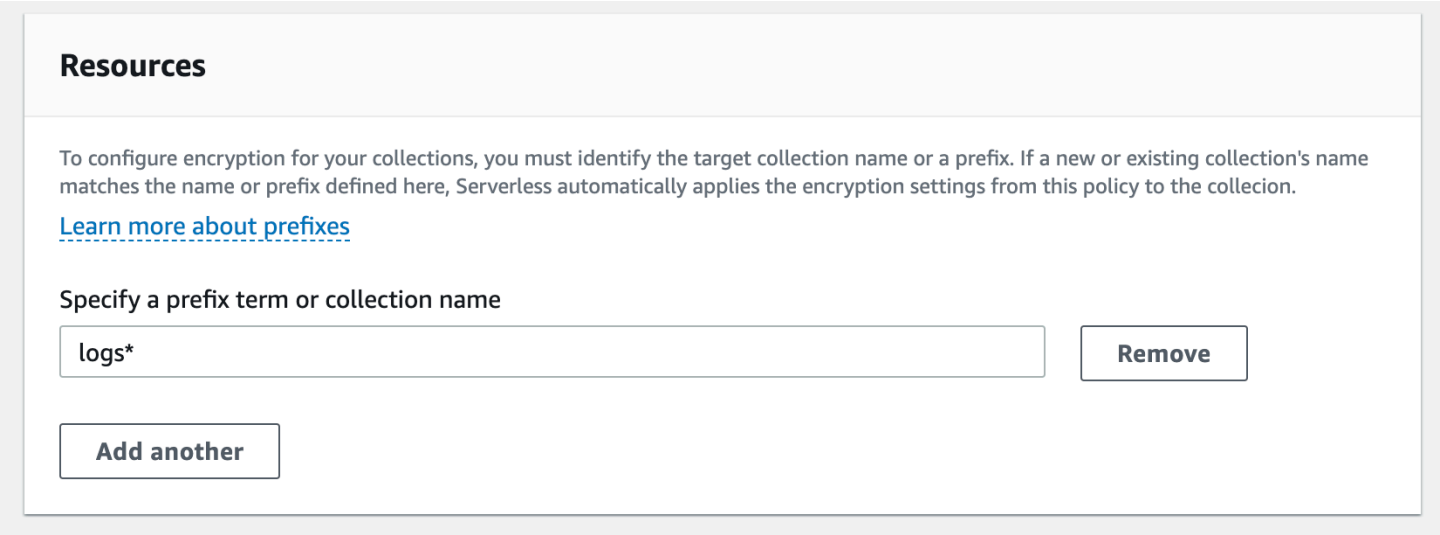
Temas

- Políticas de cifrado
- Políticas de red
- Políticas de acceso a datos
- Autenticación SAML e IAM
- Seguridad de la infraestructura
- Introducción a la seguridad en Amazon OpenSearch Serverless
- Identity and Access Management en Amazon OpenSearch sin servidor
- Cifrado en Amazon OpenSearch sin servidor
- Acceso a la red para Amazon OpenSearch Serverless
- Control de acceso a los datos para Amazon OpenSearch sin servidor
- Acceda a Amazon OpenSearch Serverless mediante un punto final de interfaz () AWS PrivateLink
- Autenticación SAML para Amazon Serverless OpenSearch
- Validación de conformidad para Amazon OpenSearch sin servidor

Políticas de cifrado

Las políticas de cifrado definen si sus colecciones se cifran con una clave gestionada por el cliente Clave propiedad de AWS o con una clave gestionada por el cliente. Las políticas de cifrado constan de dos componentes: un patrón de recursos y una clave de cifrado. El patrón de recursos define a qué colección o colecciones se aplica la política. La clave de cifrado determina cómo se protegerán las colecciones asociadas.

Para aplicar una política a varias colecciones debe incluir un comodín (*) en la regla de política. Por ejemplo, la siguiente política se aplica a todas las colecciones cuyos nombres comiencen por “logs” (registros).

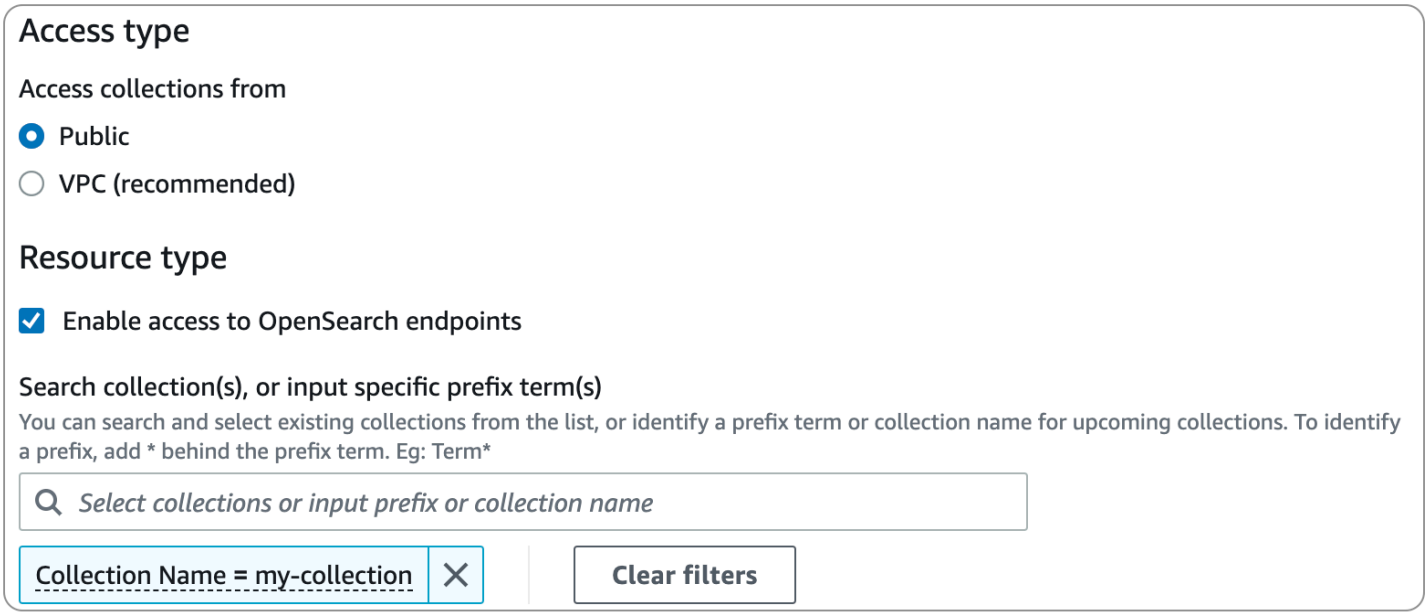


Las políticas de cifrado agilizan el proceso de creación y administración de colecciones, especialmente cuando se hace mediante programación. Puede crear una colección simplemente especificando un nombre y, al crearla, se le asigna de forma automática una clave de cifrado.

Políticas de red

Las políticas de red definen si se puede acceder a sus colecciones de forma privada o a través de Internet desde redes públicas. Se puede acceder a las colecciones privadas a través de puntos de enlace de VPC OpenSearch gestionados sin servidor o mediante dispositivos específicos, Servicios de AWS como Amazon Bedrock, mediante acceso privado.Servicio de AWS Al igual que las políticas de cifrado, las políticas de red se pueden aplicar a varias colecciones, lo que le permite administrar el acceso a la red para muchas colecciones a gran escala.

Las políticas de red constan de dos componentes: un tipo de acceso y un tipo de recurso. El tipo de acceso puede ser público o privado. El tipo de recurso determina si el acceso que elija se aplica al punto final de la recopilación, al punto final de los OpenSearch paneles o a ambos.



Si planea configurar el acceso a la VPC dentro de una política de red, primero debe crear uno o más puntos de enlace de VPC OpenSearch administrados sin servidor. Estos puntos de enlace le permiten acceder a OpenSearch Serverless como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect

El acceso privado a solo Servicios de AWS se puede aplicar al punto final de la colección, no al OpenSearch punto final de Dashboards. OpenSearch Servicios de AWS no se le puede conceder acceso a los OpenSearch paneles de control.

Políticas de acceso a datos

Las políticas de acceso a datos definen la forma en que los usuarios acceden a los datos de sus colecciones. Las políticas de acceso a datos le ayudan a administrar las colecciones a escala mediante la asignación automática de permisos de acceso a las colecciones e índices que coinciden con un patrón específico. Se pueden aplicar varias políticas a un solo recurso.

Las políticas de acceso a datos constan de un conjunto de reglas, cada una con tres componentes: un tipo de recurso, los recursos concedidos y un conjunto de permisos. El tipo de recurso puede ser una colección o un índice. Los recursos concedidos pueden ser nombres o patrones de colecciones o índices con un comodín (*). La lista de permisos especifica a qué operaciones de OpenSearch API concede acceso la política. Además, la política contiene una lista de entidades principales,

que especifican los roles, los usuarios y las identidades SAML de IAM a los que se debe conceder acceso.

Para obtener más información sobre el formato de una política de acceso a datos, consulte la sintaxis de la política.

Antes de crear una política de acceso a datos, debe tener uno o más roles o usuarios de IAM, o identidades SAML, a los que proporcionar acceso en la política. Para más información, consulte la siguiente sección.

Autenticación SAML e IAM

La entidad principal de IAM y las identidades de SAML son uno de los componentes básicos de una política de acceso a los datos. En la instrucción `principal` de una política de acceso puede incluir roles, usuarios e identidades SAML de IAM. A estas entidades principales se le conceden los permisos que usted especifique en las reglas de política asociadas.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/marketing/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
```

```
            "arn:aws:iam::123456789012:user/Dale",
            "arn:aws:iam::123456789012:role/RegulatoryCompliance",
            "saml/123456789012/myprovider/user/Annie"
        ]
    }
]
```

La autenticación SAML se configura directamente en OpenSearch Serverless. Para obtener más información, consulte the section called “Autenticación SAML”.

Seguridad de la infraestructura

Amazon OpenSearch Serverless está protegido por la seguridad de AWS la red global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Las llamadas a la API AWS publicadas se utilizan para acceder a Amazon OpenSearch Serverless a través de la red. Los clientes deben admitir Transport Layer Security (TLS). Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3. Para obtener una lista de los cifrados compatibles con TLS 1.3, consulta los protocolos y cifrados TLS en la documentación de Elastic Load Balancing.

Además, debe firmar las solicitudes con un identificador de clave de acceso y una clave de acceso secreta que estén asociadas a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Introducción a la seguridad en Amazon OpenSearch Serverless

Los siguientes tutoriales le ayudan a empezar a utilizar Amazon OpenSearch Serverless. Ambos tutoriales siguen los mismos pasos básicos, pero uno usa la consola mientras que el otro usa la AWS CLI.

Tenga en cuenta que los casos de uso de estos tutoriales están simplificados. Las políticas de red y seguridad son bastante abiertas. En las cargas de trabajo de producción, se recomienda configurar funciones de seguridad más sólidas, como la autenticación SAML, el acceso a la VPC y las políticas de acceso restrictivo a los datos.

Temas

- Tutorial: Introducción a la seguridad en Amazon OpenSearch Serverless (consola)
- Tutorial: Introducción a la seguridad en Amazon OpenSearch Serverless (CLI)

Tutorial: Introducción a la seguridad en Amazon OpenSearch Serverless (consola)

En este tutorial, se explican los pasos básicos para crear y gestionar políticas de seguridad mediante la consola Amazon OpenSearch Serverless.

En este tutorial, debe completar los siguientes pasos:

1. Configurar permisos
2. Crear una política de cifrado
3. Crear una política de red
4. Configurar la política de acceso a datos
5. Crear una colección
6. Cargar y buscar datos

Este tutorial le mostrará cómo configurar una colección con AWS Management Console. Para conocer los mismos pasos que se siguen al utilizar AWS CLI, consulte the section called “Tutorial: Introducción a la seguridad (CLI)”.

Paso 1: Configurar los permisos

> **Note**
>
> Puedes omitir este paso si ya utilizas una política más amplia basada en la identidad, como `Action":"aoss:*"` o `Action":"*"`. Sin embargo, en entornos de producción, le recomendamos que siga la entidad principal del privilegio mínimo y solo asigne los permisos mínimos necesarios para completar una tarea.

Para completar este tutorial, debe tener los permisos de IAM correctos. Su usuario o rol debe tener adjunta una política basada en la identidad con los siguientes permisos mínimos:

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

```
    {
      "Action": [
        "aoss:ListCollections",
        "aoss:BatchGetCollection",
        "aoss:CreateCollection",
        "aoss:CreateSecurityPolicy",
        "aoss:GetSecurityPolicy",
        "aoss:ListSecurityPolicies",
        "aoss:CreateAccessPolicy",
        "aoss:GetAccessPolicy",
        "aoss:ListAccessPolicies"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Para obtener una lista completa de los permisos OpenSearch sin servidor, consulte. the section called “Identity and Access Management”

Paso 2: Crear una política de cifrado

Las políticas de cifrado especifican la AWS KMS clave que OpenSearch Serverless utilizará para cifrar la colección. Puede cifrar colecciones con una clave Clave administrada de AWS o una clave diferente. Para simplificar este tutorial, cifraremos nuestra colección con un Clave administrada de AWS.

Para crear una política de cifrado en

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Expanda Sin servidor en el panel de navegación de la izquierda y seleccione Políticas de red.
3. Seleccione Crear política de cifrado.
4. Asigne el nombre de esta política a los libros de políticas. Para la descripción, introduzca Política de cifrado para la colección de libros.
5. En Recursos, introduzca libros, que es el nombre con el que llamará su colección. Si desea que este sea más extenso, puede incluir un asterisco (`books*`) para que la política se aplique a todas las colecciones que comiencen por la palabra “libros”.
6. En Cifrado, mantenga seleccionado Utilizar clave propia de AWS.
7. Seleccione Crear.

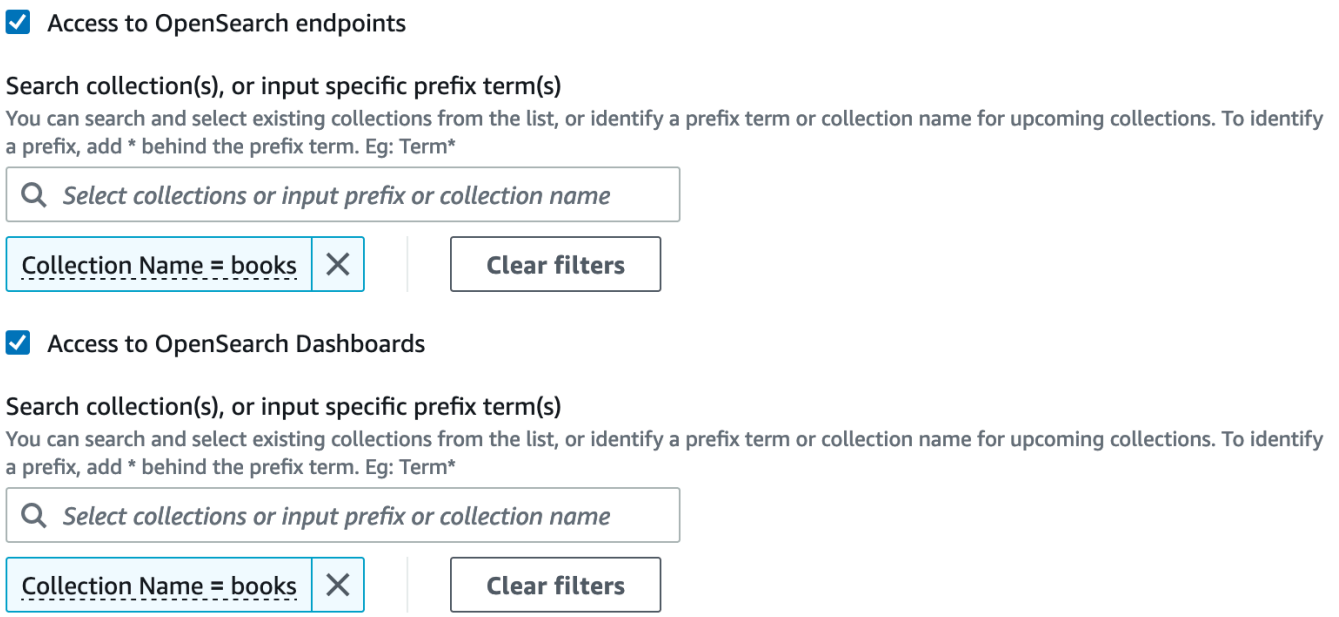
Paso 3: Crear una política de red

Las políticas de red determinan si se puede acceder a la colección a través de Internet desde redes públicas o si se debe acceder a ella a través de puntos de conexión de VPC OpenSearch gestionados sin servidor. En este tutorial, configuraremos el acceso público.

Crear una política de red

1. Seleccione Políticas en el panel de navegación de la izquierda y, a continuación, Crear política.
2. Asigne el nombre de esta política a los libros de políticas. Para la descripción, introduzca Política de redes para la colección de libros.
3. En la Regla 1, asígnele un nombre a la regla Acceso público a la colección de libros.
4. Para simplificar este tutorial, configuraremos el acceso público para la colección de libros. Para el tipo de acceso, seleccione Público.
5. Vamos a acceder a la colección desde los paneles de control. OpenSearch Para ello, debe configurar el acceso a la red para los paneles y el OpenSearch punto final; de lo contrario, los paneles no funcionarán.

   Para el tipo de recurso, habilite el acceso a los OpenSearch puntos finales y el acceso a los paneles. OpenSearch
6. En ambos cuadros de entrada, introduzca Nombre de la colección = libros. Esta configuración reduce el alcance de la política para que solo se aplique a una única colección (`books`). La regla debe tener un aspecto similar al siguiente:



7. Seleccione Crear.

Paso 4: Crear una política de acceso a datos

No podrá acceder a los datos de su colección hasta que configure el acceso a los datos. Las políticas de acceso a los datos son independientes de la política basada en identidades de IAM que configuró en el paso 1. Permiten a los usuarios acceder a los datos reales de una colección.

En este tutorial, le brindamos a un solo usuario los permisos necesarios para indexar datos en la colección de libros.

Para crear una política de acceso a datos

1. En el panel de navegación de la izquierda, seleccione Políticas de acceso a datos y Crear política de acceso.
2. Asigne el nombre de esta política a los libros de políticas. Para la descripción, introduzca Política de acceso de datos para la colección de libros.
3. Seleccione JSON para el método de definición de políticas y pegue la siguiente política en el editor de JSON.

   Sustituya el ARN principal por el ARN de la cuenta que usará para iniciar sesión en los OpenSearch paneles e indexar datos.

```
[
   {
      "Rules":[
         {
            "ResourceType":"index",
            "Resource":[
               "index/books/*"
            ],
            "Permission":[
               "aoss:CreateIndex",
               "aoss:DescribeIndex",
               "aoss:ReadDocument",
               "aoss:WriteDocument",
               "aoss:UpdateIndex",
               "aoss:DeleteIndex"
            ]
         }
      ],
```

```
      "Principal":[
         "arn:aws:iam::123456789012:user/my-user"
      ]
   }
]
```

Esta política proporciona a un solo usuario los permisos mínimos necesarios para crear un índice en la colección de libros, indexar algunos datos y buscarlos.

4. Seleccione Crear.

Paso 5: Crear una colección

Como ya configuró las políticas de cifrado y red, puede crear una colección coincidente y la configuración de seguridad se le aplicará automáticamente.

Para crear una colección sin servidor OpenSearch

1. Seleccione Colecciones en el panel de navegación de la izquierda y elija Crear colección.
2. Nombre los libros de la colección.
3. Para el tipo de colección, seleccione Buscar.
4. En Cifrado, OpenSearch Serverless le informa de que el nombre de la colección coincide con la política de `books-policy` cifrado.
5. En la configuración de acceso a la red, OpenSearch Serverless le informa de que el nombre de la colección coincide con la política de `books-policy` red.
6. Elija Siguiente.
7. En las opciones de la política de acceso a los datos, OpenSearch Serverless le informa de que el nombre de la colección coincide con la política de acceso a los `books-policy` datos.
8. Elija Siguiente.
9. Revise la configuración de la colección y seleccione Enviar. Las colecciones suelen tardar menos de un minuto en inicializarse.

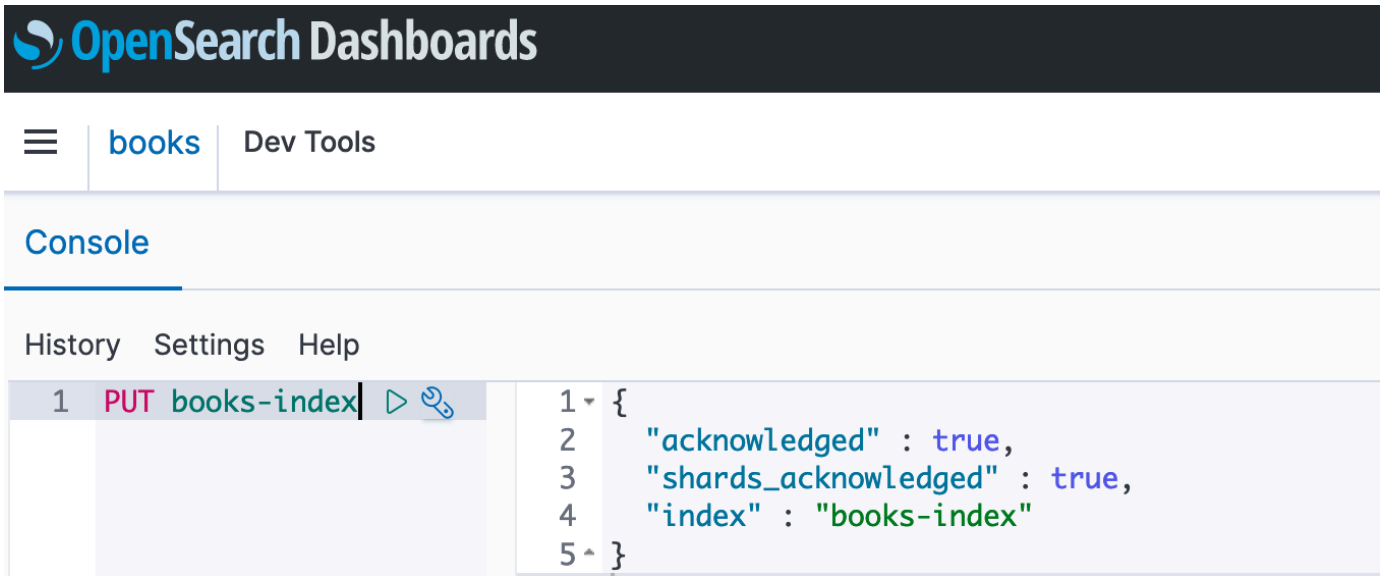
Paso 6: Cargar y buscar datos

Puede cargar datos a una colección OpenSearch sin servidor mediante Postman o curl. Para abreviar, en estos ejemplos se utilizan las herramientas de desarrollo de la consola de Dashboards. OpenSearch

Para indexar y buscar datos en la colección

1. Seleccione Colecciones en el panel de navegación de la izquierda y elija la colección de libros para abrir su página de detalles.
2. Elija la URL de los OpenSearch paneles de control para la colección. La URL toma el formato `https://collection-id.us-east-1.aoss.amazonaws.com/_dashboards`.
3. Inicie sesión en OpenSearch Dashboards con las claves de AWS acceso y secreta del director que especificó en su política de acceso a los datos.
4. En OpenSearch Dashboards, abre el menú de navegación de la izquierda y selecciona Herramientas de desarrollo.
5. Para crear un índice único denominado books-index, ejecute el siguiente comando:

```
PUT books-index
```



6. Para indexar un solo documento en books-index, ejecute el siguiente comando:

```
PUT books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

7. Para buscar datos en los OpenSearch paneles de control, debe configurar al menos un patrón de índice. OpenSearch utiliza estos patrones para identificar los índices que desea analizar.

Abra el menú principal de Dashboards, elija Gestión de pilas, luego elija Patrones de índice y, a continuación, elija Crear patrón de índice. Para este tutorial, introduzca books-index.

8. Elija Siguiente paso y, a continuación, elija Crear patrón de índice. Una vez creado el patrón, puede ver los diversos campos de documento, como `author` y `title`.
9. Para comenzar a buscar los datos, vuelva a abrir el menú principal y elija Explorar o utilice la API de búsqueda.

Tutorial: Introducción a la seguridad en Amazon OpenSearch Serverless (CLI)

En este tutorial se explican los pasos descritos en el tutorial de introducción a la consola en materia de seguridad, pero se utiliza la consola de servicio AWS CLI en lugar de la consola de OpenSearch servicio.

En este tutorial, deberá completar los siguientes pasos:

1. Crear una política de permisos de IAM
2. Adjuntar la política de IAM a un rol de IAM
3. Crear una política de cifrado
4. Crear una política de red
5. Crear una recopilación
6. Configurar la política de acceso a datos
7. Recuperar el punto de conexión de la colección
8. Cargar los datos a su conexión
9. Buscar datos en su colección

El objetivo de este tutorial es configurar una única colección OpenSearch sin servidor con una configuración bastante sencilla de cifrado, red y acceso a los datos. Por ejemplo, configuraremos el acceso a la red pública, el cifrado Clave administrada de AWS y una política de acceso a datos simplificada que otorgue permisos mínimos a un solo usuario.

En un escenario de producción, considere implementar una configuración más robusta, incluyendo autenticación SAML, una clave de cifrado personalizada y acceso VPC.

Para empezar con las políticas de seguridad en Serverless OpenSearch

1.

> **Note**
>
> Puedes omitir este paso si ya utilizas una política más amplia basada en la identidad, como `Action":"aoss:*"` o `Action":"*"`. Sin embargo, en entornos de producción, le recomendamos que siga la entidad principal del privilegio mínimo y solo asigne los permisos mínimos necesarios para completar una tarea.

Para empezar, cree una política AWS Identity and Access Management con los permisos mínimos necesarios para realizar los pasos de este tutorial. Le pondremos a la política el siguiente nombre `TutorialPolicy`:

```
aws iam create-policy \
  --policy-name TutorialPolicy \
  --policy-document "{\"Version\": \"2012-10-17\",\"Statement\":
 [{\"Action\": [\"aoss:ListCollections\",\"aoss:BatchGetCollection\",
\"aoss:CreateCollection\",\"aoss:CreateSecurityPolicy\",\"aoss:GetSecurityPolicy\",
\"aoss:ListSecurityPolicies\",\"aoss:CreateAccessPolicy\",\"aoss:GetAccessPolicy\",
\"aoss:ListAccessPolicies\"],\"Effect\": \"Allow\",\"Resource\": \"*\"}]}"
```

Respuesta de ejemplo

```
{
    "Policy": {
        "PolicyName": "TutorialPolicy",
        "PolicyId": "ANPAW6WRAECKG6QJWUV7U",
        "Arn": "arn:aws:iam::123456789012:policy/TutorialPolicy",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 0,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "CreateDate": "2022-10-16T20:57:18+00:00",
        "UpdateDate": "2022-10-16T20:57:18+00:00"
    }
}
```

2. Asocie `TutorialPolicy` al rol de IAM que indexará y buscará datos en la colección. Le pondremos al usuario el siguiente nombre `TutorialRole`:

```
aws iam attach-role-policy \
  --role-name TutorialRole \
  --policy-arn arn:aws:iam::123456789012:policy/TutorialPolicy
```

3. Antes de crear una colección, debe crear una política de cifrado que asigne una Clave propiedad de AWS a la colección de libros que creará en un paso posterior.

   Envíe la siguiente solicitud para crear una política de cifrado para la colección de libros:

```
aws opensearchserverless create-security-policy \
  --name books-policy \
  --type encryption --policy "{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection\/books\"]}],\"AWSOwnedKey\":true}"
```

   Respuesta de ejemplo

```
{
    "securityPolicyDetail": {
        "type": "encryption",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDAwNTk5MF8x",
        "policy": {
            "Rules": [
                {
                    "Resource": [
                        "collection/books"
                    ],
                    "ResourceType": "collection"
                }
            ],
            "AWSOwnedKey": true
        },
        "createdDate": 1669240005990,
        "lastModifiedDate": 1669240005990
    }
}
```

4. Cree una política de red que proporcione acceso público a la colección de libros:

```
aws opensearchserverless create-security-policy --name books-policy --type network
 \
  --policy "[{\"Description\":\"Public access for books collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/books\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/books\"]}],
\"AllowFromPublic\":true}]"
```

Respuesta de ejemplo

```
{
    "securityPolicyDetail": {
        "type": "network",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDI1Njk1NV8x",
        "policy": [
            {
                "Rules": [
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "dashboard"
                    },
                    {
                        "Resource": [
                            "collection/books"
                        ],
                        "ResourceType": "collection"
                    }
                ],
                "AllowFromPublic": true,
                "Description": "Public access for books collection"
            }
        ],
        "createdDate": 1669240256955,
        "lastModifiedDate": 1669240256955
    }
}
```

5. Crea la colección de libros:

```
aws opensearchserverless create-collection --name books --type SEARCH
```

Respuesta de ejemplo

```
{
    "createCollectionDetail": {
        "id": "8kw362bpwg4gx9b2f6e0",
        "name": "books",
        "status": "CREATING",
        "type": "SEARCH",
        "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
        "kmsKeyArn": "auto",
        "createdDate": 1669240325037,
        "lastModifiedDate": 1669240325037
    }
}
```

6. Cree una política de acceso a datos que proporcione los permisos mínimos para indexar y buscar datos en la colección de libros. Reemplace entidad principal de ARN por el ARN de `TutorialRole` del paso 1:

```
aws opensearchserverless create-access-policy \
  --name books-policy \
  --type data \
  --policy "[{\"Rules\":[{\"ResourceType\":\"index\",\"Resource\":
[\"index\/books\/books-index\"],\"Permission\":[\"aoss:CreateIndex
\",\"aoss:DescribeIndex\",\"aoss:ReadDocument\",\"aoss:WriteDocument
\",\"aoss:UpdateIndex\",\"aoss:DeleteIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:role\/TutorialRole\"]}]"
```

Respuesta de ejemplo

```
{
    "accessPolicyDetail": {
        "type": "data",
        "name": "books-policy",
        "policyVersion": "MTY2OTI0MDM5NDY1M18x",
        "policy": [
            {
```

```
                "Rules": [
                    {
                        "Resource": [
                            "index/books/books-index"
                        ],
                        "Permission": [
                            "aoss:CreateIndex",
                            "aoss:DescribeIndex",
                            "aoss:ReadDocument",
                            "aoss:WriteDocument",
                            "aoss:UpdateDocument",
                            "aoss:DeleteDocument"
                        ],
                        "ResourceType": "index"
                    }
                ],
                "Principal": [
                    "arn:aws:iam::123456789012:role/TutorialRole"
                ]
            }
        ],
        "createdDate": 1669240394653,
        "lastModifiedDate": 1669240394653
    }
}
```

`TutorialRole` ahora debería poder indexar y buscar documentos en la colección de libros.

7. Para realizar llamadas a la OpenSearch API, necesita el punto final de recopilación. Envíe la siguiente solicitud para recuperar el parámetro `collectionEndpoint`:

```
aws opensearchserverless batch-get-collection --names books
```

Respuesta de ejemplo

```
{
    "collectionDetails": [
        {
            "id": "8kw362bpwg4gx9b2f6e0",
            "name": "books",
            "status": "ACTIVE",
            "type": "SEARCH",
            "description": "",
```

```
            "arn": "arn:aws:aoss:us-
east-1:123456789012:collection/8kw362bpwg4gx9b2f6e0",
            "createdDate": 1665765327107,
            "collectionEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com",
            "dashboardEndpoint": "https://8kw362bpwg4gx9b2f6e0.us-
east-1.aoss.amazonaws.com/_dashboards"
        }
    ],
    "collectionErrorDetails": []
}
```

> **Note**
>
> No podrá ver el punto de conexión de la colección hasta que el estado de la colección cambie a `ACTIVE`. Puede que tenga que hacer varias llamadas para comprobar el estado hasta que la colección se haya creado de forma correcta.

8. Utilice una herramienta HTTP como Postman o curl para indexar los datos de la colección de libros. Crearemos un índice llamado books-index y agregaremos un solo documento.

   Envíe la siguiente solicitud al punto de conexión de la colección que recuperó en el paso anterior, con las credenciales `TutorialRole`.

```
PUT https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_doc/1
{
  "title": "The Shining",
  "author": "Stephen King",
  "year": 1977
}
```

   Respuesta de ejemplo

```
{
  "_index" : "books-index",
  "_id" : "1",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 0,
    "successful" : 0,
```

```
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 0
}
```

9. Para empezar a buscar datos en tu colección, utilice la API de búsqueda. La siguiente consulta representa una búsqueda básica:

```
GET https://8kw362bpwg4gx9b2f6e0.us-east-1.aoss.amazonaws.com/books-index/_search
```

Respuesta de ejemplo

```
{
    "took": 405,
    "timed_out": false,
    "_shards": {
        "total": 6,
        "successful": 6,
        "skipped": 0,
        "failed": 0
    },
    "hits": {
        "total": {
            "value": 2,
            "relation": "eq"
        },
        "max_score": 1.0,
        "hits": [
            {
                "_index": "books-index:0::3xJq14MBUaOS0wL26UU9:0",
                "_id": "F_bt4oMBLle5pYmm5q4T",
                "_score": 1.0,
                "_source": {
                    "title": "The Shining",
                    "author": "Stephen King",
                    "year": 1977
                }
            }
        ]
    }
}
```

Identity and Access Management en Amazon OpenSearch sin servidor

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y autorizar (tener permisos) para utilizar los recursos de OpenSearch sin servidor. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Temas

Políticas basadas en identidades de OpenSearch sin servidor

Compatibilidad con las políticas basadas en identidad	Sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Con las políticas basadas en identidad de IAM, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para obtener más información sobre los elementos que puede

utilizar en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades para OpenSearch sin servidor

Para ver ejemplos de políticas basadas en identidad de OpenSearch sin servidor, consulte the section called “Ejemplos de políticas basadas en identidades”.

Acciones de política de OpenSearch sin servidor

Admite acciones de política	Sí

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Las acciones de políticas de OpenSearch sin servidor utilizan el siguiente prefijo antes de la acción:

```
aoss
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      "aoss:action1",
      "aoss:action2"
         ]
```

Puede especificar varias acciones utilizando caracteres comodín (*). Por ejemplo, para especificar todas las acciones que comiencen con la palabra `Describe`, incluya la siguiente acción:

```
"Action": "aoss:List*"
```

Para ver ejemplos de políticas basadas en identidad de OpenSearch sin servidor, consulte Ejemplos de políticas basadas en identidades para OpenSearch sin servidor.

Recursos de políticas para OpenSearch sin servidor

Admite recursos de políticas	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Claves de condición de política para Amazon OpenSearch sin servidor

Admite claves de condición de políticas específicas del servicio	Sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puede crear expresiones condicionales que utilicen operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

Además del control de acceso basado en atributos (ABAC), OpenSearch sin servidor admite las siguientes claves de condición:

- `aoss:collection`
- `aoss:CollectionId`
- `aoss:index`

Puede utilizar estas claves de condición incluso al proporcionar políticas de acceso y de seguridad. Por ejemplo:

```
[
   {
      "Effect":"Allow",
      "Action":[
         "aoss:CreateAccessPolicy",
         "aoss:CreateSecurityPolicy"
      ],
      "Resource":"*",
      "Condition":{
         "StringLike":{
            "aoss:collection":"log"
         }
      }
   }
]
```

En este ejemplo, la condición se aplica a las políticas que contienen reglas que coinciden tanto con el nombre como con el patrón de una colección. Las condiciones funcionan de la el siguiente manera:

- `StringEquals`: se aplica a políticas con reglas que contienen la cadena de exacta de recursos “log” (es decir,`collection/log`).

- `StringLike`: se aplica a políticas con reglas que contienen la cadena de recursos que incluye la cadena "log" (es decir, `collection/log` pero también `collection/logs-application` o `collection/applogs123`).

> **Note**
>
> Las claves de condiciones de colección no se aplican a nivel de índice. Por ejemplo, en la política anterior, la condición no se aplicaría a una política de acceso o seguridad que contenga la cadena de recursos`index/logs-application/*`.

Para obtener una lista de las claves de condición de OpenSearch sin servidor, consulte Claves de condición de Amazon OpenSearch sin servidor en la Referencia de autorizaciones de servicio. Para obtener más información sobre las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por Amazon OpenSearch sin servidor.

ABAC con OpenSearch sin servidor

Admite ABAC (etiquetas en las políticas)	Sí

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puede adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte ¿Qué es ABAC? en la Guía del Usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulte Uso del control de acceso basado en atributos (ABAC) en la Guía del Usuario de IAM.

Para obtener más información sobre el etiquetado de recursos OpenSearch sin servidor, consulte the section called “Etiquetado de colecciones”.

Uso de credenciales temporales con OpenSearch sin servidor

Admite el uso de credenciales temporales	Sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utilice credenciales temporales si inicia sesión en la AWS Management Console con cualquier método excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para obtener más información sobre el cambio de roles, consulte Cambio a un rol (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puede usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulte Credenciales de seguridad temporales en IAM.

Uso de roles vinculados a servicios para OpenSearch sin servidor

Admite roles vinculados a servicios	Sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en su Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para obtener más información sobre cómo crear o administrar roles vinculados a servicios de OpenSearch sin servidor, consulte the section called “Rol de creación de colecciones”.

Ejemplos de políticas basadas en identidades para OpenSearch sin servidor

De forma predeterminada, los usuarios y roles no tienen permiso para crear, ver ni modificar recursos de OpenSearch sin servidor. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles, y los usuarios pueden asumirlos.

Para obtener información sobre cómo crear una política basada en identidad de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por Amazon OpenSearch sin servidor, incluido el formato de los ARN para cada uno de los tipos de recursos, consulte Acciones, recursos y claves de condición para Amazon OpenSearch sin servidor en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de OpenSearch sin servidor en la consola
- Administración de colecciones de OpenSearch sin servidor
- Visualización de colecciones de OpenSearch sin servidor
- Operaciones de la API de OpenSearch

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidad son muy eficaces. Determinan si alguien puede crear, acceder o eliminar los recursos de OpenSearch sin servidor de su cuenta. Estas acciones pueden generar costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar recursos de OpenSearch sin servidor de la cuenta. Estas acciones pueden generar costes adicionales para

su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte la Política de validación del analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Uso de OpenSearch sin servidor en la consola

Para acceder a OpenSearch sin servidor en la consola de OpenSearch Service, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de OpenSearch sin servidor en su cuenta de AWS. Si se crea una política basada en identidades que es más restrictiva que los permisos necesarios mínimos, la consola no funcionará del modo esperado para las entidades (tales como roles de IAM) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intenta realizar.

La siguiente política permite al usuario acceder a OpenSearch sin servidor desde la consola de OpenSearch Service:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "*",
            "Effect": "Allow",
            "Action": [
                "aoss:ListCollections",
                "aoss:BatchGetCollection",
                "aoss:ListAccessPolicies",
                "aoss:ListSecurityConfigs",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:ListVpcEndpoints",
                "aoss:GetAccessPolicy",
                "aoss:GetAccountSettings",
                "aoss:GetSecurityConfig",
                "aoss:GetSecurityPolicy"
            ]
        }
    ]
}
```

Administración de colecciones de OpenSearch sin servidor

Esta política es un ejemplo de la política de “administración de colecciones” que permite al usuario gestionar y administrar las colecciones de Amazon OpenSearch sin servidor. El usuario puede crear, ver y eliminar colecciones.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Resource": "arn:aws:aoss:region:123456789012:collection/*",
            "Action": [
                "aoss:CreateCollection",
                "aoss:DeleteCollection",
                "aoss:UpdateCollection"
            ],
            "Effect": "Allow"
        },
        {
            "Resource": "*",
            "Action": [
                "aoss:BatchGetCollection",
                "aoss:ListCollections",
                "aoss:CreateAccessPolicy",
                "aoss:CreateSecurityPolicy"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Visualización de colecciones de OpenSearch sin servidor

Este ejemplo de política permite a un usuario ver los detalles de todas las colecciones de Amazon OpenSearch sin servidor de su cuenta. El usuario no puede modificar las colecciones ni las políticas de seguridad asociadas.

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

```
                "aoss:ListAccessPolicies",
                "aoss:ListCollections",
                "aoss:ListSecurityPolicies",
                "aoss:ListTagsForResource",
                "aoss:BatchGetCollection"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Operaciones de la API de OpenSearch

Las operaciones de la API del plano de datos consisten en las funciones que se utilizan en OpenSearch sin servidor para obtener el valor del servicio en tiempo real. Las operaciones de la API del plano de control consisten en las funciones que se utilizan para configurar el entorno.

Para acceder a las API del plano de datos de Amazon OpenSearch sin servidor y a OpenSearch Dashboards desde el navegador, debe añadir dos permisos de IAM para los recursos de recopilación. Estos permisos son `aoss:APIAccessAll` y `aoss:DashboardsAccessAll`.

> **Note**
>
> A partir del 10 de mayo de 2023, OpenSearch sin servidor requerirá estos dos nuevos permisos de IAM para los recursos de recopilación. El permiso `aoss:APIAccessAll` concede el acceso al plano de datos y el permiso `aoss:DashboardsAccessAll` permite abrir OpenSearch Dashboards desde el navegador. Si no se añaden los dos nuevos permisos de IAM, se produce un error 403.

Este ejemplo de política permite a un usuario acceder a las API del plano de datos para una colección específica de su cuenta y acceder a OpenSearch Dashboards para todas las colecciones de su cuenta.

```
{
    "Version": "2012-10-17",
    "Statement": [
         {
            "Effect": "Allow",
            "Action": "aoss:APIAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:collection/collection-id"
```

```
        },
        {
            "Effect": "Allow",
            "Action": "aoss:DashboardsAccessAll",
            "Resource": "arn:aws:aoss:region:account-id:dashboards/default"
        }
    ]
}
```

Tanto `aoss:APIAccessAll` como `aoss:DashboardsAccessAll` otorgan el permiso completo de IAM a los recursos de la colección, mientras que el permiso de los paneles también permite el acceso a OpenSearch Dashboards. Cada permiso funciona de forma independiente, por lo que una denegación explícita de `aoss:APIAccessAll` no bloquea el acceso `aoss:DashboardsAccessAll` a los recursos, incluidas las herramientas para desarrolladores. Lo mismo sucede con una negación en `aoss:DashboardsAccessAll`.

OpenSearch sin servidor solo admite la dirección IP de origen en las condiciones establecidas en la política de IAM de la entidad principal para las llamadas al plano de datos:

```
"Condition": {
    "IpAddress": {
         "aws:SourceIp": "52.95.4.14"
    }
}
```

Cifrado en Amazon OpenSearch sin servidor

Cifrado en reposo

Cada colección de Amazon OpenSearch sin servidor que se crea está protegida con cifrado de datos en reposo, una característica de seguridad que ayuda a prevenir el acceso no autorizado a los datos. El cifrado en reposo utiliza AWS Key Management Service (AWS KMS) para almacenar y administrar las claves de cifrado. Utiliza el algoritmo estándar de cifrado avanzado con claves de 256 bits (AES-256) para realizar el cifrado.

Temas

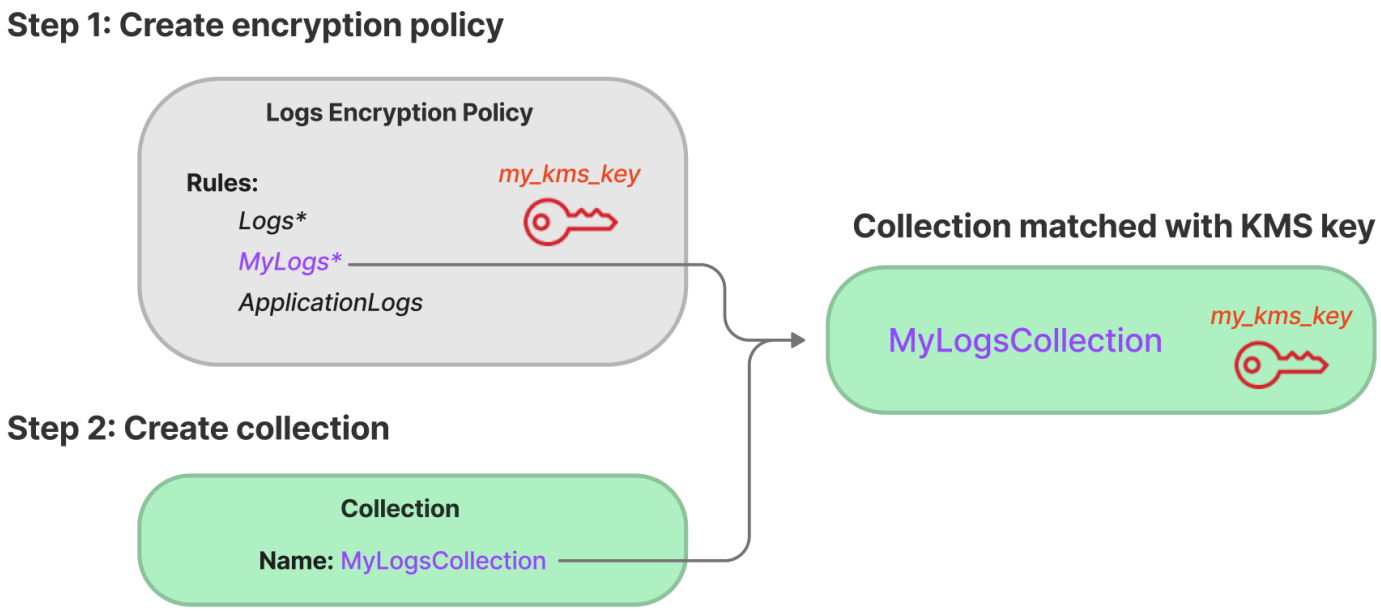
- Políticas de cifrado
- Consideraciones
- Permisos necesarios

- Política de claves para una clave administrada por el cliente
- Cómo OpenSearch sin servidor utiliza las concesiones en AWS KMS
- Creación de políticas de cifrado (consola)
- Creación de políticas de cifrado (AWS CLI)
- Visualización de políticas de cifrado
- Actualización de políticas de cifrado
- Eliminación de políticas de cifrado

Políticas de cifrado

Con las políticas de cifrado, puede administrar numerosas colecciones a escala mediante la asignación automática de una clave de cifrado a las colecciones más recientes que coincidan con un nombre o un patrón específicos.

Al crear una política de cifrado, puede especificar un prefijo, que es una regla de coincidencia basada en caracteres comodín, como `MyCollection*`, o escribir un nombre de colección único. Después, cuando se cree una colección que coincida con ese patrón de nombre o prefijo, se le asignarán de forma automática la política y la clave de KMS correspondientes.



Las políticas de cifrado contienen los siguientes elementos:

- `Rules`: una o más reglas de coincidencia de colecciones, cada una con los siguientes subelementos:

  - `ResourceType`: en la actualidad, la única opción es “colección”. Las políticas de cifrado solo se aplican a los recursos de colecciones.
  - `Resource`: uno o más nombres o patrones de colección a los que se aplicará la política, en el formato `collection/<collection name|pattern>`.
- `AWSOwnedKey`: si se utiliza una Clave propiedad de AWS o no.
- `KmsARN`: si configura el valor `AWSOwnedKey` en falso, especifique el nombre de recurso de Amazon (ARN) de la clave KMS con la que se va a cifrar las colecciones asociadas. Si incluye este parámetro, OpenSearch sin servidor ignora el parámetro `AWSOwnedKey`.

El siguiente ejemplo de política asignará una clave administrada por el cliente a cualquier colección futura denominada `autopartsinventory`, así como a las colecciones que comiencen por el término “ventas”:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Incluso si una política coincide con el nombre de una colección, puede optar por anular esta asignación automática durante la creación de la colección si el patrón de recursos contiene un comodín (*). Si decide anular la asignación automática de claves, OpenSearch sin servidor crea una política de cifrado denominada auto-**<collection-name>** y la adjunta a la colección. En un principio, la política solo se aplica a una única colección, pero se puede modificar para que incluya colecciones adicionales.

Si modifica las reglas de políticas para que dejen de coincidir con una colección, la clave KMS asociada continuará asignada a esa colección. La colección siempre permanece cifrada con su

clave de cifrado inicial. Si desea cambiar la clave de cifrado de una colección, debe volver a crear la colección.

Si las reglas de varias políticas coinciden con una colección, se utiliza la regla más específica. Por ejemplo, si una política contiene una regla para `collection/log*` y otra para `collection/logSpecial`, se utiliza la clave de cifrado de la segunda política porque es más específica.

No puede usar un nombre o un prefijo en una política si ya existe en otra política. OpenSearch sin servidor muestra un error si intenta configurar patrones de recursos idénticos en diferentes políticas de cifrado.

Consideraciones

Cuando configure el cifrado de las colecciones, tenga en cuenta lo siguiente:

- El cifrado en reposo es obligatorio para todas las colecciones sin servidor.
- Puede elegir entre utilizar una clave administrada por el cliente o una Clave propiedad de AWS. Si elige una clave administrada por el cliente, le recomendamos habilitar la rotación automática de claves.
- No se puede cambiar la clave de cifrado de una colección después de su creación. Elija cuidadosamente qué AWS KMS usará la primera vez que configure una colección.
- Una colección solo puede coincidir con una única política de cifrado.
- Las colecciones con claves KMS únicas no pueden compartir las unidades de cómputo de OpenSearch (OCU) con otras colecciones. Cada colección con una clave única requiere 4 OCU propias.
- Si actualiza la clave KMS de una política de cifrado, el cambio no afectará a las colecciones coincidentes existentes con claves KMS ya asignadas.
- OpenSearch sin servidor no comprueba de forma explícita los permisos de usuario en las claves administradas por el cliente. Si un usuario tiene permisos para acceder a una colección mediante una política de acceso a los datos, podrá incorporar y consultar los datos cifrados con la clave asociada.

Permisos necesarios

El cifrado en reposo para OpenSearch sin servidor utiliza los siguientes permisos de AWS Identity and Access Management (IAM). Puede especificar las condiciones de IAM para restringir a los usuarios a colecciones específicas.

- `aoss:CreateSecurityPolicy`: cree una política de cifrado.
- `aoss:ListSecurityPolicies` enumere todas las políticas y colecciones de cifrado a las que están adjuntas.
- `aoss:GetSecurityPolicy`: consulte los detalles de una política de cifrado específica.
- `aoss:UpdateSecurityPolicy`: modifique una política de cifrado.
- `aoss:DeleteSecurityPolicy`: elimine una política de cifrado.

El siguiente ejemplo de política de acceso basada en la identidad proporciona los permisos mínimos necesarios para que un usuario administre las políticas de cifrado con el patrón de recursos `collection/application-logs`.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "aoss:CreateSecurityPolicy",
            "aoss:UpdateSecurityPolicy",
            "aoss:DeleteSecurityPolicy",
            "aoss:GetSecurityPolicy"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aoss:collection":"application-logs"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "aoss:ListSecurityPolicies"
         ],
         "Resource":"*"
      }
   ]
}
```

Política de claves para una clave administrada por el cliente

Si selecciona una clave administrada por el cliente para proteger una colección, OpenSearch sin servidor obtiene permiso para utilizar la clave KMS en nombre de la entidad principal que realiza la selección. Esa entidad principal, un usuario o un rol, debe tener los permisos en la clave KMS que OpenSearch sin servidor necesita. Puede proporcionar estos permisos en una política de claves o en una política de IAM.

Como mínimo, OpenSearch sin servidor necesita los siguientes permisos en una clave administrada por el cliente:

- kms:DescribeKey
- kms:CreateGrant
- kms:ListKeys

Por ejemplo:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:ListKeys"
      ],
      "Resource": "*"
    },
{
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:CreateGrant"
      ],
      "Resource": "{kms-key-arn}"
    }
  ]
}
```

OpenSearch sin servidor crea una concesión con los permisos kms:GenerateDataKey y kms:Decrypt.

Si desea conservar la clave exclusiva para OpenSearch sin servidor, puede agregar la condición kms:ViaService a esa política de claves:

```
"Condition": {
  "StringEquals": {
    "kms:ViaService": "aoss.us-east-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Para más información, consulte Uso de políticas de claves en AWS KMS en la Guía del desarrollador de AWS Key Management Service.

Cómo OpenSearch sin servidor utiliza las concesiones en AWS KMS

OpenSearch sin servidor requiere una concesión para poder utilizar una clave administrada por el cliente.

Cuando crea una política de cifrado en su cuenta con una clave nueva, OpenSearch sin servidor crea una concesión en su nombre mediante el envío de la solicitud CreateGrant a AWS KMS. Las concesiones en AWS KMS se utilizan para otorgar a OpenSearch sin servidor acceso a una clave KMS en una cuenta de cliente.

OpenSearch sin servidor necesita la concesión para utilizar la clave administrada por el cliente para las siguientes operaciones internas:

- Enviar solicitudes de DescribeKey a AWS KMS para comprobar que el ID de la clave simétrica administrada por el cliente proporcionado es válido.
- Enviar solicitudes de GenerateDataKey a la clave KMS para crear claves de datos para cifrar objetos.
- Enviar solicitudes de Decrypt a AWS KMS para descifrar las claves de datos cifradas para que puedan usarse para cifrar sus datos.

Puede revocar el acceso a la concesión o eliminar el acceso del servicio a la clave administrada por el cliente en cualquier momento. Si lo hace, OpenSearch sin servidor no podrá acceder a ninguno de los datos cifrados por la clave administrada por el cliente, lo que afectará a todas las operaciones

que dependen de esos datos y provocará errores y fallos de `AccessDeniedException` en los flujos de trabajo asíncronos.

OpenSearch sin servidor retira las concesiones en un flujo de trabajo asíncrono cuando una determinada clave administrada por el cliente no está asociada a ninguna política o colección de seguridad.

Creación de políticas de cifrado (consola)

En una política de cifrado, se especifica una clave KMS y una serie de patrones de colección a los que se aplicará la política. A cualquier colección nueva que coincida con uno de los patrones definidos en la política se le asignará la clave KMS correspondiente al crear la colección. Recomendamos que cree las políticas de cifrado antes de empezar a crear las colecciones.

Para crear una política de cifrado de OpenSearch sin servidor

1. Abra la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación izquierdo, amplíe Sin servidor y seleccione Políticas de cifrado.
3. Seleccione Crear política de cifrado.
4. Escriba un nombre y una descripción para la política.
5. En Recursos, ingrese uno o más patrones de recursos para esta política de cifrado. Todas las colecciones recién creadas en la región y Cuenta de AWS actuales que coincidan con uno de los patrones se asignan de forma automática a esta política. Por ejemplo, si introduce `ApplicationLogs` (sin comodín) y luego crea una colección con ese nombre, la política y la clave KMS correspondientes se asignarán a esa colección.

   También puede proporcionar un prefijo como `Logs*`, que asigna la política a cualquier colección nueva cuyo nombre comience por `Logs`. Mediante el uso de comodines, puede administrar la configuración de cifrado de varias colecciones a escala.
6. En Cifrado, elija la clave KMS que se debe utilizar.
7. Seleccione Crear.

Siguiente paso: crear colecciones

Después de configurar una o más políticas de cifrado, puede empezar a crear colecciones que coincidan con las reglas definidas en esas políticas. Para obtener instrucciones, consulte the section called “Creación de colecciones”.

En el paso de Cifrado de la creación de la colección, OpenSearch sin servidor le informa que el nombre que ingresó coincide con el patrón definido en una política de cifrado y asigna de forma automática la clave KMS correspondiente a esa colección. Si el patrón de recursos contiene un comodín (*), puede anular la coincidencia y seleccionar su propia clave.

Creación de políticas de cifrado (AWS CLI)

Para crear una política de cifrado mediante las operaciones de la API de OpenSearch sin servidor, especifique los patrones de recursos y una clave de cifrado en formato JSON. La solicitud CreateSecurityPolicy acepta políticas insertadas y archivos .json.

Las políticas de cifrado tienen el siguiente formato. El archivo de muestra `my-policy.json` coincidirá con cualquier colección futura con el nombre `autopartsinventory`, así como con cualquier colección cuyo nombre comience con `sales`.

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
   ],
   "AWSOwnedKey":false,
   "KmsARN":"arn:aws:encryption:us-east-1:123456789012:key/93fd6da4-a317-4c17-
bfe9-382b5d988b36"
}
```

Para usar una clave propiedad del servicio, configure la `AWSOwnedKey` como `true`:

```
{
   "Rules":[
      {
         "ResourceType":"collection",
         "Resource":[
            "collection/autopartsinventory",
            "collection/sales*"
         ]
      }
```

```
   ],
   "AWSOwnedKey":true
}
```

La siguiente solicitud crea la política de cifrado:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy file://my-policy.json
```

A continuación, utilice la operación de la API CreateCollection para crear una o más colecciones que coincidan con uno de los patrones de recursos.

Visualización de políticas de cifrado

Antes de crear una colección, puede que desee obtener una vista previa de las políticas de cifrado existentes en su cuenta para ver cuál tiene un patrón de recursos que coincide con el nombre de su colección. La siguiente solicitud ListSecurityPolicies enumera todas las políticas de cifrado de su cuenta:

```
aws opensearchserverless list-security-policies --type encryption
```

La solicitud devuelve información sobre todas las políticas de cifrado configuradas. Utilice el contenido del elemento `policy` para ver las reglas de patrón que se definen en la política:

```
{
   "securityPolicyDetails": [
      {
         "createdDate": 1663693217826,
         "description": "Sample encryption policy",
         "lastModifiedDate": 1663693217826,
         "name": "my-policy",
         "policy": "{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"]}],\"AWSOwnedKey\":true}",
         "policyVersion": "MTY2MzY5MzIxNzgyNl8x",
         "type": "encryption"
      }
   ]
}
```

Para ver información detallada sobre una política específica, incluida la clave KMS, utilice el comando GetSecurityPolicy.

Actualización de políticas de cifrado

Si actualiza la clave KMS en una política de cifrado, el cambio solo se aplica a las colecciones recién creadas que coincidan con el nombre o patrón configurado. No afecta a las colecciones existentes que ya tienen claves KMS asignadas.

Lo mismo sucede con las reglas de coincidencia de las políticas. Si agrega, modifica o elimina una regla, el cambio solo se aplica a las colecciones recién creadas. Las colecciones existentes no pierden la clave KMS asignada si modifica las reglas de una política para que ya no coincida con el nombre de una colección.

Para actualizar una política de cifrado en la consola de OpenSearch sin servidor, elija Políticas de cifrado, seleccione la política que desee modificar y elija Editar. Realice los cambios y elija Guardar.

Para actualizar una política de cifrado mediante la API de OpenSearch sin servidor, utilice la operación UpdateSecurityPolicy. La siguiente solicitud actualiza una política de cifrado con un nuevo documento JSON de política:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type encryption \
    --policy-version 2 \
    --policy file://my-new-policy.json
```

Eliminación de políticas de cifrado

Cuando se elimina una política de cifrado, las colecciones que estén utilizando en ese momento la clave KMS definida en la política no se ven afectadas. Para eliminar una política en la consola de OpenSearch sin servidor, seleccione la política y elija Eliminar.

También puede utilizar la operación DeleteSecurityPolicy:

```
aws opensearchserverless delete-security-policy --name my-policy --type encryption
```

Cifrado en tránsito

En OpenSearch sin servidor, todas las rutas de una colección se cifran en tránsito mediante Transport Layer Security 1.2 (TLS) y un cifrado AES-256 estándar del sector. El acceso a todas

las API y paneles de Opensearch también se realiza a través de TLS 1.2. TLS es un conjunto de protocolos criptográficos estándares del sector que se utilizan para cifrar la información que se intercambia a través de la red.

Acceso a la red para Amazon OpenSearch Serverless

La configuración de red de una colección de Amazon OpenSearch Serverless determina si se puede acceder a la colección a través de Internet desde redes públicas o si se debe acceder a ella de forma privada.

El acceso privado se puede aplicar a uno de los siguientes sitios o a ambos:

- OpenSearch Terminales de VPC gestionados sin servidor
- Compatible Servicios de AWS , como Amazon Bedrock

Puede configurar el acceso a la red por separado para el OpenSearchpunto final de una colección y el punto final de OpenSearch Dashboards correspondiente.

El acceso a la red es el mecanismo de aislamiento que permite el acceso desde diferentes redes de origen. Por ejemplo, si el punto final de los OpenSearch paneles de una colección es de acceso público, pero el punto final de la OpenSearch API no, el usuario solo podrá acceder a los datos de la recopilación a través de los paneles cuando se conecte desde una red pública. Si intentan llamar a las OpenSearch API directamente desde una red pública, se bloquearán. La configuración de red se puede utilizar para estas permutaciones de origen a tipo de recurso.

Temas

Políticas de red

Las políticas de red le permiten administrar muchas colecciones a gran escala al asignar de forma automática la configuración de acceso a la red a las colecciones que cumplen con las reglas definidas en la política.

En una política de red, se especifican una serie de reglas. Estas reglas definen los permisos de acceso a los puntos finales de la recopilación y a los puntos finales de los OpenSearch paneles de control. Cada regla consta de un tipo de acceso (público o privado) y un tipo de recurso (punto final de colección o OpenSearch panel de control). Para cada tipo de recurso (`collection` y `dashboard`), especifique una serie de reglas que definen a qué colecciones se aplicará la política.

En este ejemplo de política, la primera regla especifica el acceso al punto final de la VPC tanto al punto final de la recopilación como al punto final de Dashboards para todas las colecciones que comiencen por el término. `marketing*` También especifica el acceso a Amazon Bedrock.

> **Note**
>
> El acceso privado a Servicios de AWS Amazon Bedrock solo se aplica al punto final de la colección, no al OpenSearch punto final de OpenSearch Dashboards. Incluso si es así`dashboard`, Servicios de AWS no `ResourceType` se le puede conceder acceso a OpenSearch los paneles de control.

La segunda regla especifica el acceso público a la colección `finance`, pero solo para el punto de conexión de la colección (sin acceso a los paneles).

```
[
   {
      "Description":"Marketing access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/marketing*"
            ]
         },
         {
            "ResourceType":"dashboard",
            "Resource":[
```

```
                "collection/marketing*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   },
   {
      "Description":"Sales access",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Esta política solo proporciona acceso público a los OpenSearch paneles de control para las colecciones que comiencen por «finanzas». Cualquier intento de acceder directamente a la OpenSearch API fallará.

```
[
  {
    "Description": "Dashboards access",
    "Rules": [
      {
        "ResourceType": "dashboard",
        "Resource": [
          "collection/finance*"
        ]
      }
    ],
    "AllowFromPublic": true
  }
```

```
]
```

Las políticas de red pueden aplicarse a las colecciones existentes, así como a las colecciones futuras. Por ejemplo, puede crear una colección y, a continuación, crear una política de red con una regla que coincida con el nombre de la colección. No es necesario crear políticas de red para crear colecciones.

Consideraciones

Al configurar el acceso a la red para sus colecciones, tenga en cuenta lo siguiente:

- Si planea configurar el acceso al punto de enlace de VPC para una colección, primero debe crear al OpenSearch menos un punto de enlace de VPC administrado sin servidor.
- El acceso privado Servicios de AWS solo se aplica al punto final de la colección, no al OpenSearch punto final de Dashboards. OpenSearch Incluso si es así`dashboard`, Servicios de AWS no `ResourceType` se le puede conceder acceso a los OpenSearch paneles de control.
- Si se puede acceder a una colección desde redes públicas, también se puede acceder a ella desde todos los puntos finales de VPC OpenSearch gestionados sin servidor y desde todos ellos. Servicios de AWS
- Se pueden aplicar varias políticas de red a una sola colección. Para más información, consulte the section called “Prioridad política”.

Permisos necesarios

El acceso a la red para OpenSearch Serverless utiliza los siguientes permisos (IAM). AWS Identity and Access Management Puede especificar condiciones de IAM para restringir a los usuarios a las políticas de red asociadas con colecciones específicas.

- `aoss:CreateSecurityPolicy`: cree una política de acceso a la red.
- `aoss:ListSecurityPolicies`: enumere todas las políticas de red de la cuenta actual.
- `aoss:GetSecurityPolicy`: vea una especificación de la política de acceso a la red.
- `aoss:UpdateSecurityPolicy`: modifique una política de acceso a la red determinada y cambiar el ID de VPC o la designación de acceso público.
- `aoss:DeleteSecurityPolicy`: elimine una política de acceso a la red (después de separarla de todas las colecciones).

La siguiente política de acceso basada en identidades permite al usuario ver todas las políticas de red y actualizarlas según el patrón de recursos`collection/application-logs`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "aoss:UpdateSecurityPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": "application-logs"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:ListSecurityPolicies",
                "aoss:GetSecurityPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Prioridad política

Puede haber situaciones en las que las reglas de la política de red se superpongan, dentro de las políticas o entre ellas. Cuando esto sucede, una regla que especifica el acceso público anula una regla que especifica el acceso privado para cualquier colección que sea común a ambas reglas.

Por ejemplo, en la siguiente política, ambas reglas asignan acceso a la red de la colección `finance`, pero una regla especifica el acceso a la VPC y la otra especifica el acceso público. En esta situación, el acceso público anula el acceso a la VPC únicamente para la recaudación de fondos (porque existe en ambas reglas), por lo que se podrá acceder a la colección de fondos desde las redes públicas. La colección de ventas tendrá acceso a VPC desde el punto de conexión especificado.

```
[
```

```
   {
      "Description":"Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/sales",
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ]
   },
   {
      "Description":"Rule 2",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

Si se aplican varios puntos de conexión de VPC de diferentes reglas a una colección, las reglas son aditivas y se podrá acceder a la colección desde todos los puntos de conexión especificados. Si lo configura `AllowFromPublic` `true` pero también proporciona uno `SourceVPCEs` o más`SourceServices`, OpenSearch Serverless ignora los puntos finales de la VPC y los identificadores de servicio, y las colecciones asociadas tendrán acceso público.

Creación de políticas de (consola)

Las políticas de red se pueden aplicar tanto a las políticas existentes como a las políticas future. Se recomienda crear políticas de red antes de empezar a crear colecciones.

Para crear una política de red sin servidor OpenSearch

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación de la izquierda, expanda Sin servidor y seleccione Políticas de red.
3. Seleccione Crear políticas de red.
4. Escriba un nombre y una descripción para la política.
5. Proporcione una o más reglas. Estas reglas definen los permisos de acceso para sus colecciones OpenSearch sin servidor y sus puntos finales de OpenSearch Dashboards.

   Cada regla contiene los siguientes elementos:

Elemento	Descripción
Nombre de la regla	Nombre que describa el contenido de la regla. Por ejemplo, “Acceso a VPC para el equipo de marketing”.
Tipo de acceso	Elija el acceso público o privado. A continuación, selecciona una o ambas de las siguientes opciones: • Puntos de enlace de VPC para el acceso: especifique uno o más puntos de enlace de VPC administrados sin servidor (puntos de enlace de VPC administrados)Open Search . • Servicio de AWS acceso privado: seleccione uno o Servicios de AWS más compatibles.
Tipo de recurso	Seleccione si desea proporcionar acceso a los OpenSearch puntos finales (lo que permite realizar llamadas a la OpenSearch API), a los OpenSearch paneles (lo que permite el acceso a las visualizaciones y a la interfaz de usuario de los OpenSearch complementos) o a ambos.

Elemento	Descripción
	Note Servicio de AWS El acceso privado solo se aplica al punto final de la colección, no al OpenSearch punto final de Dashboards. OpenSearch Incluso si selecciona los OpenSearch paneles, solo Servicios de AWS se le puede conceder el acceso al punto final.

Para cada tipo de recurso que seleccione, puede elegir las colecciones existentes a las que aplicar la configuración de la política o crear uno o más patrones de recursos. Los patrones de recursos constan de un prefijo y un comodín (*) y definen a qué colecciones se aplicará la configuración de la política.

Por ejemplo, si incluye un patrón denominado `Marketing*`, a cualquier colección nueva o existente cuyo nombre comience por “Marketing” se le aplicará automáticamente la configuración de red de esta política. Un único comodín (`*`) aplica la política a todas las colecciones actuales y future.

Además, puede especificar el nombre de una colección futura sin caracteres comodín, como`Finance`. OpenSearch Serverless aplicará la configuración de la política a cualquier colección recién creada con ese nombre exacto.

6. Cuando esté satisfecho, seleccione Crear.

Creación de políticas de (AWS CLI)

Para crear una política de red mediante las operaciones de la API OpenSearch sin servidor, debe especificar las reglas en formato JSON. La CreateSecurityPolicysolicitud acepta políticas en línea y archivos.json. Todas las colecciones y patrones deben tomar la forma `collection/<collection name|pattern>`.

> **Note**
>
> El tipo de recurso `dashboards` solo permite el acceso a los OpenSearch paneles, pero para que los OpenSearch paneles funcionen, también debes permitir el acceso a la colección desde las mismas fuentes. Consulte la segunda política a continuación para ver un ejemplo.

Para especificar el acceso privado, incluya uno o ambos de los siguientes elementos:

- `SourceVPCEs`— Especifique uno o más puntos finales de VPC OpenSearch gestionados sin servidor.
- `SourceServices`— Especifique el identificador de uno o más de los compatibles. Servicios de AWS Actualmente, se admiten los siguientes identificadores de servicio:
  - `bedrock.amazonaws.com`— Amazon Bedrock

El siguiente ejemplo de política de red proporciona acceso privado, a un punto final de VPC y a Amazon Bedrock, a los puntos de enlace de recopilación solo para las colecciones que comiencen con el prefijo. `log*` Los usuarios autenticados no pueden iniciar sesión en los OpenSearch paneles; solo pueden acceder al punto final de la recopilación mediante programación.

```
[
   {
      "Description":"Private access for log collections",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/log*"
            ]
         }
      ],
      "AllowFromPublic":false,
      "SourceVPCEs":[
         "vpce-050f79086ee71ac05"
      ],
      "SourceServices":[
         "bedrock.amazonaws.com"
      ],
   }
```

```
]
```

La siguiente política proporciona acceso público al OpenSearch punto final y a los OpenSearch paneles de control de una sola colección denominada. `finance` Si la colección no existe, la configuración de red se aplicará a la colección siempre y cuando se cree.

```
[
   {
      "Description":"Public access for finance collection",
      "Rules":[
         {
            "ResourceType":"dashboard",
            "Resource":[
               "collection/finance"
            ]
         },
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/finance"
            ]
         }
      ],
      "AllowFromPublic":true
   }
]
```

La siguiente solicitud crea la política de red anterior:

```
aws opensearchserverless create-security-policy \
    --name sales-inventory \
    --type network \
    --policy "[{\"Description\":\"Public access for finance collection\",\"Rules
\":[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection\/finance\"]},
{\"ResourceType\":\"collection\",\"Resource\":[\"collection\/finance\"]}],
\"AllowFromPublic\":true}]"
```

Para proporcionar la política en un archivo JSON, utilice el formato`--policy file://my-policy.json`

Visualización de políticas de red

Antes de crear una colección, puede que desee obtener una vista previa de las políticas de red existentes en su cuenta para ver cuáles tienen un patrón de recursos que coincide con el nombre de su colección. La siguiente ListSecurityPoliciessolicitud muestra todas las políticas de red de su cuenta:

```
aws opensearchserverless list-security-policies --type network
```

La solicitud devuelve información sobre todas las políticas de red configuradas. Para ver las reglas de patrón definidas en una política específica, busque la información de la política en el contenido del elemento `securityPolicySummaries` en la respuesta. Tenga en cuenta el `name` `type` final de esta política y utilice estas propiedades en una GetSecurityPolicysolicitud para recibir una respuesta con los siguientes detalles de la política:

```
{
    "securityPolicyDetail": [
        {
            "type": "network",
            "name": "my-policy",
            "policyVersion": "MTY2MzY5MTY1MDA3Ml8x",
            "policy": "[{\"Description\":\"My network policy rule\",\"Rules\":
[{\"ResourceType\":\"dashboard\",\"Resource\":[\"collection/*\"]}],\"AllowFromPublic
\":true}]",
            "createdDate": 1663691650072,
            "lastModifiedDate": 1663691650072
        }
    ]
}
```

Para ver información detallada sobre una política específica, utilice el GetSecurityPolicycomando.

Actualización de las políticas de red

Al modificar los puntos de conexión de VPC o la designación de acceso público de una red, todas las colecciones asociadas se ven afectadas. Para actualizar una política de red en la consola OpenSearch sin servidor, expanda Políticas de red, seleccione la política que desee modificar y elija Editar. Realice los cambios y elija Guardar.

Para actualizar una política de red mediante la API OpenSearch sin servidor, utilice el UpdateSecurityPolicycomando. Debe incluir un control de versiones de política en la solicitud. Puede

recuperar el control de versiones de la política mediante los comandos `ListSecurityPolicies` o `GetSecurityPolicy`. Incluir la versión más reciente de la política garantiza que no se anule inadvertidamente un cambio realizado por otra persona.

La siguiente solicitud actualiza una política de red con un nuevo documento JSON de política:

```
aws opensearchserverless update-security-policy \
    --name sales-inventory \
    --type network \
    --policy-version MTY2MzY5MTY1MDA3Ml8x \
    --policy file://my-new-policy.json
```

Eliminar las políticas de red

Para poder eliminar una política de red, debe desconectarla de todas las colecciones. Para eliminar una política en la consola OpenSearch sin servidor, selecciónela y elija Eliminar.

También puede usar el DeleteSecurityPolicycomando:

```
aws opensearchserverless delete-security-policy --name my-policy --type network
```

Control de acceso a los datos para Amazon OpenSearch sin servidor

Con el control de acceso a los datos de Amazon OpenSearch sin servidor, puede permitir que los usuarios accedan a las colecciones e índices, sin importar su origen de red o mecanismo de acceso. Puede proporcionar acceso a roles de IAM e identidades SAML.

Los permisos de acceso se administran mediante las políticas de acceso a los datos, que se aplican a las colecciones y a los recursos de índice. Las políticas de acceso a datos le ayudan a administrar las colecciones a escala mediante la asignación automática de permisos de acceso a las colecciones e índices que coinciden con un patrón específico. Se pueden aplicar varias políticas de acceso a los datos a un solo recurso. Tenga en cuenta que debe tener una política de acceso a los datos para su colección a fin de acceder a la URL de OpenSearch Dashboards.

Temas

- Políticas de acceso a datos frente a políticas de IAM
- Permisos de IAM necesarios
- Sintaxis de la política

- Permisos de política compatibles
- Ejemplos de conjuntos de datos en OpenSearch Dashboards
- Creación de políticas de acceso a los datos (consola)
- Creación de políticas de acceso a los datos (AWS CLI)
- Visualización de políticas de acceso a los datos
- Actualización de las políticas de acceso a los datos
- Eliminación de políticas de acceso a los datos

Políticas de acceso a datos frente a políticas de IAM

Las políticas de acceso a los datos están separadas de forma lógica de las políticas AWS Identity and Access Management (IAM). Los permisos de IAM controlan el acceso a las operaciones de la API sin servidor, como `CreateCollection` y `ListAccessPolicies`. Las políticas de acceso a los datos controlan el acceso a las operaciones de OpenSearch que admite OpenSearch sin servidor, como `PUT <index>` o `GET _cat/indices`.

Los permisos de IAM que controlan el acceso a las operaciones de la API de la política de acceso a los datos, como `aoss:CreateAccessPolicy` y `aoss:GetAccessPolicy` (que se describen en la siguiente sección), no afectan al permiso especificado en una política de acceso a los datos.

Por ejemplo, supongamos que una política de IAM niega a un usuario crear políticas de acceso a los datos para `collection-a`, pero le permite crear políticas de acceso a datos para todas las colecciones (`*`):

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aoss:collection": "collection-a"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "aoss:CreateAccessPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Si el usuario crea una política de acceso a los datos que permite ciertos permisos a todas las colecciones (`collection/*` o `index/*/*`), la política se aplicará a todas las colecciones, incluida la colección A.

> **Important**
>
> Contar con permisos dentro de una política de acceso a datos no es suficiente para acceder a los datos de la colección de OpenSearch sin servidor. A una entidad principal también se le debe conceder acceso a los permisos `aoss:APIAccessAll` y `aoss:DashboardAccessAll` de IAM. Ambos permiten acceso completo a los recursos de la colección, mientras que el permiso de los paneles también permite el acceso a los paneles de OpenSearch. Si una entidad principal no tiene estos dos permisos de IAM, recibirá 403 errores cuando intente enviar solicitudes a la colección. Para obtener más información, consulte the section called “Operaciones de la API de OpenSearch”.

Permisos de IAM necesarios

El control de acceso a los datos para OpenSearch sin servidor utiliza los siguientes permisos de IAM. Puede especificar las condiciones de IAM para restringir a los usuarios a nombres de políticas de acceso específicos.

- `aoss:CreateAccessPolicy`: cree una política de acceso.
- `aoss:ListAccessPolicies`: enumere todas las políticas de acceso.
- `aoss:GetAccessPolicy`: consulte los detalles sobre una política de acceso específica.
- `aoss:UpdateAccessPolicy`: modifique una política de acceso.
- `aoss:DeleteAccessPolicy`: elimine una política de acceso.

La siguiente política de acceso basada en la identidad permite al usuario ver todas las políticas de acceso y actualizar las políticas que contienen el patrón de recursos `collection/logs`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:ListAccessPolicies",
                "aoss:GetAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Action": [
                "aoss:UpdateAccessPolicy"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aoss:collection": [
                        "logs"
                    ]
                }
            }
        }
    ]
}
```

Sintaxis de la política

Una política de acceso a datos incluye un conjunto de reglas, cada una con los siguientes elementos:

Elemento	Descripción
`ResourceType`	El tipo de recurso (colección o índice) al que se le aplican los permisos. Los permisos de alias y plantillas se encuentran en el nivel de la colección , mientras que los permisos para crear, modificar y buscar datos están en

Elemento	Descripción
	el nivel del índice. Para más información, consulte Permisos de políticas compatibles.
`Resource`	Una lista de nombres o patrones de recursos. Los patrones son prefijos seguidos de un comodín (*), que permiten que los permisos asociados se apliquen a varios recursos. • Las colecciones adoptan el formato `collection/ <name|pattern>` . • Los índices toman el formato `index/<collection-name|pattern> /<index-name|pattern/>` .
`Permission`	Una lista de permisos a otorgar para los recursos especificados. Para obtener una lista completa de las operaciones de la API y de los permisos que permiten, consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.
`Principal`	Una lista de una o más entidades principales a las que conceder acceso. Las entidades principales pueden ser ARN de roles de IAM o identidades SAML. Estas entidades principales deben estar dentro de la Cuenta de AWS actual. No se admite el acceso entre cuentas.

La siguiente política de ejemplo otorga permisos de alias y plantillas a la colección llamada `autopartsinventory`, así como a cualquier colección que comience por el prefijo `sales*`. También otorga permisos de lectura y escritura a todos los índices dentro de la colección `autopartsinventory` y a todos los índices de la colección `salesorders` que comiencen por el prefijo `orders*`.

```
[
   {
      "Description": "Rule 1",
      "Rules":[
         {
            "ResourceType":"collection",
            "Resource":[
               "collection/autopartsinventory",
               "collection/sales*"
            ],
```

```
            "Permission":[
               "aoss:CreateCollectionItems",
               "aoss:UpdateCollectionItems",
               "aoss:DescribeCollectionItems"
            ]
         },
         {
            "ResourceType":"index",
            "Resource":[
               "index/autopartsinventory/*",
               "index/salesorders/orders*"
            ],
            "Permission":[
               "aoss:*"
            ]
         }
      ],
      "Principal":[
         "arn:aws:iam::123456789012:user/Dale",
         "arn:aws:iam::123456789012:role/RegulatoryCompliance",
         "saml/123456789012/myprovider/user/Annie",
         "saml/123456789012/anotherprovider/group/Accounting"
      ]
   }
]
```

No se puede denegar el acceso de forma explícita dentro de una política. Por lo tanto, todos los permisos de la política son aditivos. Por ejemplo, si una política concede el permiso `aoss:ReadDocument` a un usuario y otra `aoss:WriteDocument`, el usuario tendrá ambos permisos. Si una tercera política concede al mismo usuario el permiso `aoss:*`, el usuario puede realizar todas las acciones del índice asociado; los permisos más restrictivos no anulan los menos restrictivos.

Permisos de política compatibles

Las políticas de acceso a los datos admiten los siguientes permisos. Para conocer las operaciones de la API de OpenSearch que permite cada permiso, consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.

Permisos de colección

- `aoss:CreateCollectionItems`

- aoss:DeleteCollectionItems
- aoss:UpdateCollectionItems
- aoss:DescribeCollectionItems
- aoss:*

Permisos de índice

- aoss:ReadDocument
- aoss:WriteDocument
- aoss:CreateIndex
- aoss:DeleteIndex
- aoss:UpdateIndex
- aoss:DescribeIndex
- aoss:*

Ejemplos de conjuntos de datos en OpenSearch Dashboards

OpenSearch Dashboards proporcionan conjuntos de datos de ejemplo que incluyen visualizaciones, paneles y otras herramientas para ayudarlo a explorar Dashboards antes de agregar sus propios datos. Para crear índices a partir de estos datos de ejemplo, necesita una política de acceso a los datos que otorgue permisos al conjunto de datos con el que desee trabajar. La siguiente política usa un comodín (*) para proporcionar permisos a los tres conjuntos de datos de ejemplo.

```
[
  {
    "Rules": [
      {
        "Resource": [
          "index/<collection-name>/opensearch_dashboards_sample_data_*"
        ],
        "Permission": [
          "aoss:CreateIndex",
          "aoss:DescribeIndex",
          "aoss:ReadDocument"
        ],
        "ResourceType": "index"
```

```
      }
    ],
    "Principal": [
      "arn:aws:iam::<account-id>:user/<user>"
    ]
  }
]
```

Creación de políticas de acceso a los datos (consola)

Puede crear una política de acceso a los datos con el editor visual o en el formato JSON. A cualquier colección nueva que coincida con uno de los patrones definidos en la política se le asignarán los permisos correspondientes al crear la colección.

Para crear una política de acceso a los datos de OpenSearch sin servidor

1. Abra la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación izquierdo, expanda Sin servidor y seleccione Control de acceso a los datos.
3. Elija Crear política de acceso.
4. Escriba un nombre y una descripción para la política.
5. Proporcione un nombre para la primera regla de la política. Por ejemplo, “Acceso a la colección de registros”.
6. Seleccione Agregar entidades principales, y luego uno o varios roles de IAM o usuarios y grupos de SAML para proporcionarles acceso a los datos.

   > **Note**
   >
   > Para seleccionar las entidades principales desde los menús desplegables, debe tener los permisos `iam:ListUsers` y `iam:ListRoles` (para las entidades principales de IAM) y el permiso `aoss:ListSecurityConfigs` (para las identidades de SAML).

7. Elija Otorgar y seleccione los permisos de alias, plantillas e índices que desea conceder a las entidades principales asociadas. Para obtener una lista completa de los permisos y el acceso que permiten, consulte the section called “Operaciones y permisos de OpenSearch API compatibles”.
8. (Opcional) Configure reglas adicionales para la política.

9. Seleccione Crear. Puede transcurrir alrededor de un minuto de retardo entre el momento en que se crea la política y el momento en el que se aplican los permisos. Si tarda más de 5 minutos, póngase en contacto con AWS Support.

> **Important**
>
> Si la política solo incluye permisos de índices (y no permisos de colecciones), es posible que siga apareciendo un mensaje sobre las colecciones coincidentes que indique lo siguiente: `Collection cannot be accessed yet. Configure data access policies so that users can access the data within this collection`. Puede omitir esta advertencia. Las entidades principales autorizadas pueden seguir realizando las operaciones relacionadas con índices que tengan asignadas en la colección.

Creación de políticas de acceso a los datos (AWS CLI)

Para crear una política de acceso a los datos mediante la API de OpenSearch sin servidor, utilice el comando `CreateAccessPolicy`. El comando acepta políticas insertadas y archivos .json. Las políticas insertadas deben codificarse como una cadena de escape de JSON.

La siguiente solicitud crea una política de acceso a los datos:

```
aws opensearchserverless create-access-policy \
    --name marketing \
    --type data \
    --policy "[{\"Rules\":[{\"ResourceType\":\"collection\",\"Resource\":
[\"collection/autopartsinventory\",\"collection/sales*\"],\"Permission\":
[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",\"Resource\":
[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],\"Permission
\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]"
```

Para proporcionar la política dentro de un archivo .json, utilice el formato `--policy file://my-policy.json`.

Las entidades principales incluidas en la política ahora pueden usar las operaciones de OpenSearch a las que se les concedió acceso.

Visualización de políticas de acceso a los datos

Antes de crear una colección, puede que desee obtener una vista previa de las políticas de acceso a los datos existentes en la cuenta para ver cuáles tienen un patrón de recursos que coincide con el nombre de su colección. La siguiente solicitud de ListAccessPolicies enumera todas las políticas de acceso a los datos en su cuenta:

```
aws opensearchserverless list-access-policies --type data
```

La solicitud devuelve información sobre todas las políticas de acceso a los datos configuradas. Para ver las reglas de patrón definidas en una política específica, busque la información de la política en el contenido del elemento `accessPolicySummaries` en la respuesta. Anote el `name` y `type` de esta política y utilice estas propiedades en una solicitud de GetAccessPolicy para recibir una respuesta con los siguientes detalles de la política:

```
{
    "accessPolicyDetails": [
        {
            "type": "data",
            "name": "my-policy",
            "policyVersion": "MTY2NDA1NDE4MDg1OF8x",
            "description": "My policy",
            "policy": "[{\"Rules\":[{\"ResourceType\":\"collection\",
\"Resource\":[\"collection/autopartsinventory\",\"collection/sales*\"],
\"Permission\":[\"aoss:UpdateCollectionItems\"]},{\"ResourceType\":\"index\",
\"Resource\":[\"index/autopartsinventory/*\",\"index/salesorders/orders*\"],
\"Permission\":[\"aoss:ReadDocument\",\"aoss:DescribeIndex\"]}],\"Principal\":
[\"arn:aws:iam::123456789012:user/Shaheen\"]}]",
            "createdDate": 1664054180858,
            "lastModifiedDate": 1664054180858
        }
    ]
}
```

Puede incluir filtros de recursos para limitar los resultados a políticas que contengan colecciones o índices específicos:

```
aws opensearchserverless list-access-policies --type data --resource
 "index/autopartsinventory/*"
```

Para ver los detalles de una política específica, utilice el comando GetAccessPolicy.

Actualización de las políticas de acceso a los datos

Al actualizar una política de acceso a los datos, todas las colecciones asociadas se ven afectadas. Para actualizar una política de acceso a datos en la consola de OpenSearch sin servidor, elija Control de acceso a los datos, seleccione la política que desee modificar y elija Editar. Realice los cambios y elija Guardar.

Para actualizar una política de acceso a los datos mediante la API de OpenSearch sin servidor, envíe la solicitud `UpdateAccessPolicy`. Debe incluir una versión de la política, que puede recuperar mediante los comandos `ListAccessPolicies` or `GetAccessPolicy`. Incluir la versión más reciente de la política garantiza que no se anule inadvertidamente un cambio realizado por otra persona.

La siguiente solicitud de UpdateAccessPolicy actualiza una política de acceso a los datos con un nuevo documento de política JSON:

```
aws opensearchserverless update-access-policy \
    --name sales-inventory \
    --type data \
    --policy-version MTY2NDA1NDE4MDg1OF8x \
    --policy file://my-new-policy.json
```

Pueden transcurrir unos minutos de retardo entre el momento en que se actualiza la política y el momento en que se aplican los nuevos permisos.

Eliminación de políticas de acceso a los datos

Al eliminar una política de acceso a los datos, todas las colecciones asociadas pierden el acceso definido en la política. Asegúrese de que sus usuarios de IAM y SAML tengan el acceso adecuado a la colección antes de eliminar una política. Para eliminar una política en la consola de OpenSearch sin servidor, seleccione la política y elija Eliminar.

También puede utilizar el comando DeleteAccessPolicy:

```
aws opensearchserverless delete-access-policy --name my-policy --type data
```

Acceda a Amazon OpenSearch Serverless mediante un punto final de interfaz () AWS PrivateLink

Puede usarlo AWS PrivateLink para crear una conexión privada entre su VPC y Amazon OpenSearch Serverless. Puede acceder a OpenSearch Serverless como si estuviera en su VPC, sin el uso de una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect Las instancias de su VPC no necesitan direcciones IP públicas para acceder OpenSearch a Serverless.

Esta conexión privada se establece mediante la creación de un punto de conexión de interfaz alimentado por AWS PrivateLink . Creamos una interfaz de red de punto de conexión en cada subred especificada para el punto de conexión de interfaz. Se trata de interfaces de red administradas por el solicitante que sirven como punto de entrada para el tráfico destinado a Serverless. OpenSearch

Para obtener más información, consulte Acceso a Servicios de AWS a través de AWS PrivateLink en la Guía de AWS PrivateLink.

Temas

Resolución de DNS de los puntos de conexión de colección

Al crear un punto de conexión de VPC, el servicio crea una nueva zona alojada privada Amazon Route 53 y la adjunta a la VPC. Esta zona alojada privada consta de un registro para convertir el registro DNS comodín de las colecciones OpenSearch sin servidor (`*.aoss.us-east-1.amazonaws.com`) en las direcciones de interfaz utilizadas para el punto final. Solo necesita un punto final de VPC OpenSearch sin servidor en una VPC para acceder a todas y cada una de las colecciones y paneles de control de cada una de ellas. Región de AWS Cada VPC con un punto final para OpenSearch Serverless tiene su propia zona alojada privada adjunta.

OpenSearch Serverless también crea un registro DNS comodín público de Route 53 para todas las colecciones de la región. El nombre DNS se resuelve en las direcciones IP públicas de OpenSearch Serverless. Los clientes de las VPC que no tienen un punto final de OpenSearch VPC sin servidor o los clientes de las redes públicas pueden usar la resolución pública de Route 53 y acceder a las colecciones y los paneles con esas direcciones IP.

La dirección de resolver de DNS de una VPC determinada es la segunda dirección IP del CIDR de la VPC. Todos los clientes de la VPC deben usar ese resolver para obtener la dirección de punto de conexión de VPC para cualquier colección. La resolución utiliza una zona alojada privada creada por Serverless. OpenSearch Basta con usar ese resolverr para todas las colecciones de cualquier cuenta. También es posible utilizar el resolver de VPC para algunos puntos de conexión de colección y el resolver público para otros, aunque normalmente no es necesario.

VPC y políticas de acceso a la red

Para conceder permisos de red a OpenSearch las API y los paneles de control de sus colecciones, puede utilizar las políticas de acceso a la red OpenSearch sin servidor. Puede controlar este acceso a la red desde sus puntos de conexión de VPC o desde la Internet pública. Como su política de red solo controla los permisos de tráfico, también debe configurar una política de acceso a los datos que especifique los permisos para operar con los datos de una colección y sus índices. Piense en un punto final de VPC OpenSearch sin servidor como un punto de acceso al servicio, una política de acceso a la red como el punto de acceso a nivel de red a las colecciones y los paneles de control, y una política de acceso a los datos como el punto de acceso para un control de acceso detallado para cualquier operación con los datos de la recopilación.

Como puede especificar varios ID de punto de conexión de VPC en una política de red, le recomendamos que cree un punto de conexión de VPC para cada VPC que necesite acceder a una colección. Estas VPC pueden pertenecer a AWS cuentas distintas de la cuenta propietaria de la política de recopilación y red sin servidor. OpenSearch No recomendamos crear una solución de emparejamiento de VPC a VPC ni ninguna otra solución de proxy entre dos cuentas para que la VPC de una cuenta pueda utilizar el punto de conexión de VPC de otra cuenta. Esto es menos seguro y rentable que cada VPC que tenga su propio punto de conexión. El administrador de la otra VPC, que ha configurado el acceso al punto de conexión de esa VPC en la política de red, no podrá ver fácilmente la primera VPC.

Políticas de punto de conexión y VPC

Amazon OpenSearch Serverless admite políticas de puntos de conexión para VPC. Una política de punto de conexión es una política basada en recursos de IAM que se puede asociar a un punto

de conexión de VPC para controlar qué entidades principales de AWS pueden utilizar el punto de conexión para acceder a su servicio de AWS. Para obtener más información, consulte Controlar el acceso a puntos de conexión de VPC con políticas de punto de conexión.

Para usar una política de punto de conexión, primero debe crear un punto de conexión de interfaz. Puede crear un punto final de interfaz mediante la consola OpenSearch Serverless o la OpenSearch API Serverless. Después de crear el punto de conexión de interfaz, tendrá que añadir la política del punto de conexión al punto de conexión. Para obtener más información, consulte Acceder a Amazon OpenSearch Serverless mediante un punto final de interfaz (AWS PrivateLink).

> **Note**
>
> No puede definir una política de puntos finales directamente en la consola de OpenSearch servicio.

Una política de punto de conexión no anula ni reemplaza otras políticas basadas en identidades, políticas basadas en recursos, políticas de red o políticas de acceso a datos que haya configurado. Para obtener información sobre cómo actualizar la política de puntos de conexión, consulte Controlar el acceso a puntos de conexión de VPC con políticas de punto de conexión.

De forma predeterminada, una política de punto de conexión concede acceso completo al punto de conexión de VPC.

```
{
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Si bien la política de puntos de conexión de VPC predeterminada concede acceso total a los puntos de conexión, puede configurar una política de puntos de conexión de VPC para permitir el acceso a roles y usuarios específicos. Para eso, vea el siguiente ejemplo:

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012",
                    "987654321098"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Puede especificar una colección OpenSearch sin servidor para incluirla como elemento condicional en su política de puntos de conexión de VPC. Para eso, vea el siguiente ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CollectionName": [
                        "coll-abc"
                    ]
                }
            }
        }
    ]
}
```

Puede usar las identidades de SAML en la política de puntos de conexión de VPC para determinar el acceso a esos puntos. Debe usar un comodín (*) en la sección de la entidad principal de la política de puntos de conexión de VPC. Para eso, vea el siguiente ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        }
    ]
}
```

Además, puede configurar su política de puntos de conexión para que incluya una política de entidad principal de SAML específica. Para eso, vea lo siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SamlPrincipal": [
                        "saml/123456789012/idp123/user/user1234"]
                    }
                }
            }
        ]
    }
```

Para obtener más información sobre el uso de la autenticación SAML con Amazon OpenSearch Serverless, consulte Autenticación SAML para Amazon Serverless. OpenSearch

También puede incluir usuarios de IAM y SAML en la misma política de puntos de conexión de VPC. Para eso, vea el siguiente ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:SamlGroups": [
                        "saml/123456789012/idp123/group/football",
                        "saml/123456789012/idp123/group/soccer",
                        "saml/123456789012/idp123/group/cricket"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "123456789012"
                ]
            },
            "Action": "*",
            "Resource": "*"
        }
    ]
}
```

Consideraciones

Antes de configurar un punto final de interfaz para OpenSearch Serverless, tenga en cuenta lo siguiente:

- OpenSearch Serverless permite realizar llamadas a todas las operaciones de OpenSearch API compatibles (no a las operaciones de API de configuración) a través del punto final de la interfaz.
- Después de crear un punto final de interfaz para OpenSearch Serverless, aún debe incluirlo en las políticas de acceso a la red para que pueda acceder a las colecciones sin servidor.
- De forma predeterminada, se permite el acceso total a OpenSearch Serverless a través del punto final de la interfaz. Puede asociar un grupo de seguridad a las interfaces de red de los puntos finales para controlar el tráfico a OpenSearch Serverless a través del punto final de la interfaz.
- Una sola unidad Cuenta de AWS puede tener un máximo de 50 puntos finales de VPC OpenSearch sin servidor.
- Si habilita el acceso público a Internet a la API o los paneles de control de su colección en una política de red, cualquier VPC y la Internet pública pueden acceder a su colección.
- Si está en las instalaciones y fuera de la VPC, no puede usar directamente una resolución de DNS para la resolución del punto final de la VPC OpenSearch sin servidor. Si necesita acceso a una VPN, la VPC necesita un resolver de proxy de DNS para que lo usen los clientes externos. Route 53 ofrece una opción de punto de conexión de entrada que puede usar para resolver consultas de DNS a su VPC desde su red en las instalaciones u otra VPC.
- Para otras consideraciones, consulte Consideraciones en la Guía de AWS PrivateLink.

Permisos necesarios

El acceso a la VPC para OpenSearch Serverless utiliza los siguientes permisos AWS Identity and Access Management (IAM). Puede especificar las condiciones de IAM para restringir a los usuarios a colecciones específicas.

- `aoss:CreateVpcEndpoint`: cree un punto de conexión de VPC.
- `aoss:ListVpcEndpoints`: enumere todos los puntos de conexión de VPC.
- `aoss:BatchGetVpcEndpoint`: consulte los detalles sobre un subconjunto de puntos de conexión de VPC.
- `aoss:UpdateVpcEndpoint`: modifique un punto de conexión de VPC.
- `aoss:DeleteVpcEndpoint`: elimine un punto de conexión de VPC.

Además, necesita los siguientes permisos de Amazon EC2 y Route 53 para crear un punto de conexión de VPC.

- `ec2:CreateTags`

- `ec2:CreateVpcEndpoint`
- `ec2:DeleteVpcEndPoints`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:ModifyVpcEndPoint`
- `route53:AssociateVPCWithHostedZone`
- `route53:ChangeResourceRecordSets`
- `route53:CreateHostedZone`
- `route53:DeleteHostedZone`
- `route53:GetChange`
- `route53:GetHostedZone`
- `route53:ListHostedZonesByName`
- `route53:ListHostedZonesByVPC`
- `route53:ListResourceRecordSets`

Cree un punto final de interfaz para Serverless OpenSearch

Puede crear un punto final de interfaz para OpenSearch Serverless mediante la consola o la API OpenSearch Serverless.

Para crear un punto final de interfaz para una colección sin servidor OpenSearch

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación de la izquierda, expanda Sin servidor y seleccione Puntos de conexión de VPC.
3. Seleccione Crear punto de conexión de VPC.
4. Proporcione un nombre para el punto de conexión.
5. En el caso de la VPC, selecciona la VPC desde la que accederás a Serverless. OpenSearch
6. En el caso de las subredes, selecciona una subred desde la que accederás a Serverless. OpenSearch

7. En Grupos de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red del punto de conexión. Este es un paso fundamental en el que limita los puertos, protocolos y orígenes para el tráfico entrante que autoriza para el punto de conexión. Asegúrese de que las reglas del grupo de seguridad permitan que los recursos que utilizarán el punto final de la VPC se comuniquen con OpenSearch Serverless para comunicarse con la interfaz de red del punto final.
8. Seleccione Crear punto de conexión.

Para crear un punto final de VPC mediante la API OpenSearch sin servidor, utilice el comando. `CreateVpcEndpoint`

> **Note**
>
> Después de crear un punto de conexión, registre su ID (por ejemplo, `vpce-050f79086ee71ac05`. Para proporcionar el acceso del punto de conexión a sus colecciones, debe incluir este ID en una o más políticas de acceso a la red.

Próximo paso: Otorgar al punto de conexión acceso a la colección

Tras crear un punto de conexión de interfaz, debe proporcionarles acceso a las colecciones mediante políticas de acceso a la red. Para obtener más información, consulte the section called “Acceso a la red”.

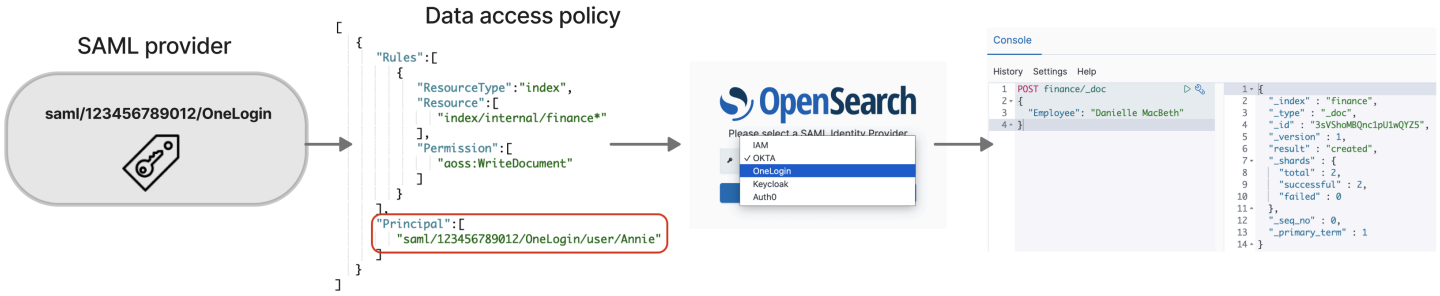
Autenticación SAML para Amazon Serverless OpenSearch

Con la autenticación SAML para Amazon OpenSearch Serverless, puede usar su proveedor de identidad actual para ofrecer el inicio de sesión único (SSO) para los puntos de enlace de los OpenSearch paneles de control de las colecciones sin servidor.

La autenticación SAML le permite utilizar proveedores de identidad externos para iniciar sesión en Dashboards con el fin de indexar y buscar datos. OpenSearch OpenSearch Serverless es compatible con los proveedores que utilizan el estándar SAML 2.0, como IAM Identity Center, Okta, Keycloak, Active Directory Federation Services (AD FS) y Auth0. Puede configurar IAM Identity Center para sincronizar usuarios y grupos de otras fuentes de identidad, como Okta OneLogin y Microsoft Entra ID. Para obtener una lista de las fuentes de identidad compatibles con el IAM Identity Center y los pasos para configurarlas, consulte los tutoriales de introducción en la Guía del usuario del IAM Identity Center.

> **Note**
>
> La autenticación SAML solo sirve para acceder a los OpenSearch paneles de control a través de un navegador web. Los usuarios autenticados solo pueden realizar solicitudes a las operaciones de la OpenSearch API a través de las herramientas de desarrollo de los paneles de control. OpenSearch Sus credenciales de SAML no le permiten realizar solicitudes HTTP directas a las operaciones de la OpenSearch API.

Para configurar la autenticación SAML, primero debe configurar un proveedor de identidades (IdP) SAML. A continuación, se incluyen uno o más usuarios de ese IdP en una política de acceso a datos. Esta política le otorga ciertos permisos para las colecciones o los índices. A continuación, un usuario puede iniciar sesión en los OpenSearch paneles y realizar las acciones que se permiten en la política de acceso a los datos.



Temas

- Consideraciones
- Permisos necesarios
- Crear proveedores SAML de (consola)
- Acceder a los paneles OpenSearch
- Concesión de acceso a las identidades de SAML a los datos de la colección
- Creación de proveedores SAML (AWS CLI)
- Ver proveedores SAML
- Actualización de proveedores SAML
- Eliminar proveedores SAML

Consideraciones

A la hora de configurar la autenticación SAML, tenga en cuenta lo siguiente:

- No se admiten las solicitudes firmadas y cifradas.
- No se admiten las aserciones cifradas.
- No se admite la autenticación ni el cierre de sesión iniciada por el IDP.

Permisos necesarios

La autenticación SAML para OpenSearch Serverless utiliza los siguientes permisos AWS Identity and Access Management (IAM):

- `aoss:CreateSecurityConfig`: cree un proveedor SAML.
- `aoss:ListSecurityConfig`: enumere todos los proveedores de SAML en la cuenta actual.
- `aoss:GetSecurityConfig`: vea la información del proveedor de SAML.
- `aoss:UpdateSecurityConfig`: modifique la configuración de proveedor de SAML determinada, incluidos los metadatos XML.
- `aoss:DeleteSecurityConfig`: elimine un proveedor SAML.

La siguiente política de acceso basada en la identidad permite al usuario administrar todas las configuraciones de IdP:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "aoss:CreateSecurityConfig",
                "aoss:DeleteSecurityConfig",
                "aoss:GetSecurityConfig",
                "aoss:UpdateSecurityConfig",
                "aoss:ListSecurityConfigs"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
```

```
}
```

Tenga en cuenta que el elemento `Resource` debe ser un comodín.

Crear proveedores SAML de (consola)

En estos pasos se explica cómo crear proveedores de SAML. Esto permite la autenticación SAML con la autenticación iniciada por el proveedor de servicios (SP) para los paneles. OpenSearch No se admite la autenticación IdP.

Para habilitar la autenticación SAML en los paneles OpenSearch

1. Inicia sesión en la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación de la izquierda, expanda Sin servidor y seleccione Autenticación SAML.
3. Seleccione Agregar proveedor SAML.
4. Escriba un nombre y una descripción para el proveedor.

   > **Note**
   >
   > El nombre que especifique es de acceso público y aparecerá en un menú desplegable cuando los usuarios inicien sesión en los OpenSearch paneles. Asegúrese de que el nombre sea fácilmente reconocible y no revele información confidencial sobre su proveedor de identidad.

5. En Configurar IdP, copie la URL del servicio al consumidor de aserciones (ACS).
6. Utilice la URL de ACS que acaba de copiar para configurar su proveedor de identidades. La terminología y los pasos varían según el proveedor. Consulte la documentación de su proveedor.

   En Okta, por ejemplo, se crea una “aplicación web SAML 2.0” y se especifica la URL de ACS como URL de inicio de sesión única, URL de destinatario y URL de destino. Para Auth0, debe especificarlo en las URL de devolución de llamadas permitidas.
7. Indique la restricción de audiencia si su IdP tiene un campo para ello. La restricción de audiencia es un valor dentro de la aserción SAML que especifica a quién va dirigida esta. Para OpenSearch Serverless, especifique. `aws:opensearch:<aws account id>` Por ejemplo, `aws:opensearch:123456789012`.

El nombre del campo de restricción de audiencia varía según el proveedor. Para Okta, es Audiencia URI (ID de entidad del SP). En el caso de IAM Identity Center, es la audiencia de Application SAML.

8. Si utiliza IAM Identity Center, también debe especificar el siguiente asignación de atributos: `Subject=${user:name}`, con un formato de `unspecified`.
9. Después de configurar el proveedor de identidades, genera un archivo de metadatos de IdP. Este archivo XML contiene información sobre el proveedor, como un certificado TLS, puntos de conexión de inicio de sesión único y el ID de entidad del proveedor de identidad.

   Copie el texto del archivo de metadatos del IdP y péguelo en Proporcionar metadatos desde el campo de IdP. Alternativamente, seleccione Importar desde archivo XML y cargue el archivo. El archivo de metadatos debe tener un aspecto similar al siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>s
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

10. Mantenga vacío el campo Atributo ID de usuario personalizado para utilizar el elemento `NameID` de la aserción SAML para el nombre de usuario. Si su aserción no utiliza este elemento estándar y, en su lugar, incluye el nombre de usuario como un atributo personalizado, especifique ese

atributo aquí. Los atributos distinguen entre mayúsculas y minúsculas. Solo se admite un único atributo de usuario.

El siguiente ejemplo muestra un atributo de anulación para `NameID` en la aserción SAML:

```
<saml2:Attribute Name="UserId" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:type="xs:string">annie</saml2:AttributeValue>
</saml2:Attribute>
```

11. (Opcional) Especifique un atributo personalizado en el campo Atributos del grupo, como `role` o `group`. Solo se admite un único atributo de grupo. No hay ningún atributo de grupo predeterminado. Si no especifica ninguna, sus políticas de acceso a datos solo pueden contener entidades principales de usuario.

    El siguiente ejemplo muestra un atributo de grupo en la aserción SAML:

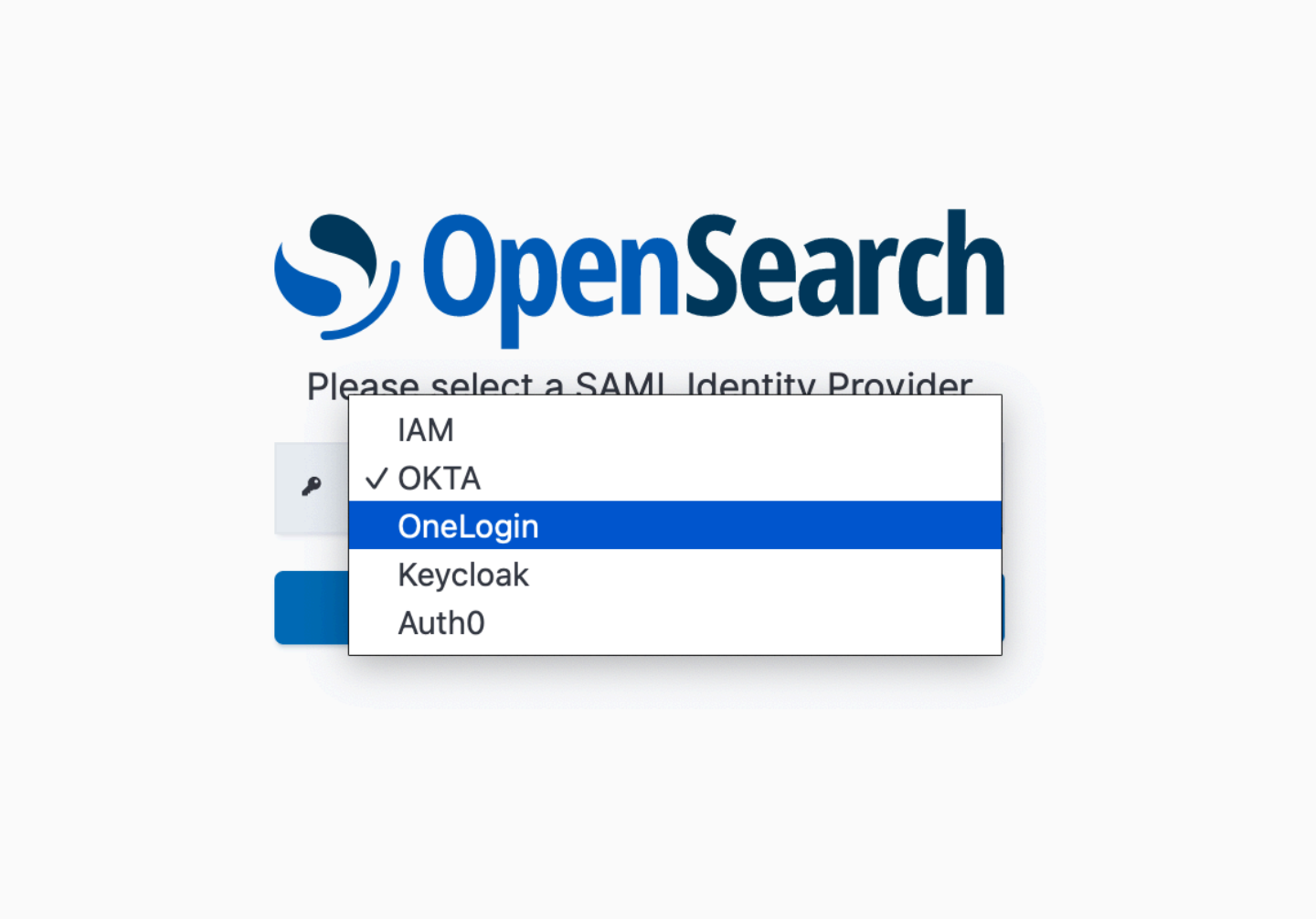
    ```
    <saml2:Attribute Name="department"
     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">finance</saml2:AttributeValue>
    </saml2:Attribute>
    ```

12. De forma predeterminada, OpenSearch Dashboards cierra la sesión de los usuarios después de 24 horas. Puede configurar este valor en cualquier número entre 1 y 12 horas (15 y 720 minutos) especificando el tiempo de espera de los OpenSearch paneles. Si intenta establecer el tiempo de espera igual o inferior a 15 minutos, la sesión se restablecerá a una hora.
13. Seleccione Crear proveedor.

Acceder a los paneles OpenSearch

Tras configurar un proveedor de SAML, todos los usuarios y grupos asociados a ese proveedor pueden navegar hasta el punto de conexión de los OpenSearch paneles. La URL de Dashboards tiene el formato *collection-endpoint*`/_dashboards/` para todas las colecciones.

Si tienes SAML activado, al seleccionar el enlace que aparece en la AWS Management Console página de selección de IdP, donde puedes iniciar sesión con tus credenciales de SAML. Primero, use el menú desplegable para seleccionar un proveedor de identidades:



Inicie sesión con sus credenciales de usuario de IdP.

Si no tienes el SAML activado, al seleccionar el enlace que aparece en él podrás AWS Management Console iniciar sesión como usuario o rol de IAM, sin opción de usar SAML.

Concesión de acceso a las identidades de SAML a los datos de la colección

Después de crear un proveedor de SAML, aún tendrá que concederles acceso a los datos de sus colecciones a los usuarios y grupos subyacentes. Para concederles el acceso deberá hacerlo a través de políticas de acceso a datos. Hasta que no les proporcione acceso a los usuarios, estos no podrán leer, escribir ni eliminar ningún dato de sus colecciones.

Para conceder el acceso, cree una política de acceso a los datos y especifique sus ID de usuario o grupo de SAML en la declaración de `Principal`:

```
[
   {
      "Rules":[
       ...
      ],
      "Principal":[
         "saml/987654321098/myprovider/user/Shaheen",
         "saml/987654321098/myprovider/group/finance"
      ]
   }
]
```

Puede concederles acceso a colecciones, índices o ambos. Si desea que diferentes usuarios tengan permisos diferentes, cree varias reglas. Para obtener una lista de los permisos disponibles, consulte Permisos de políticas compatibles. Para obtener información sobre cómo dar formato a una política de acceso, consulte Sintaxis de políticas.

Creación de proveedores SAML (AWS CLI)

Para crear un proveedor de SAML mediante la API OpenSearch sin servidor, envía una solicitud: CreateSecurityConfig

```
aws opensearchserverless create-security-config \
    --name myprovider \
    --type saml \
    --saml-options file://saml-auth0.json
```

Especifique `saml-options`, incluido el XML de los metadatos, como un mapa clave-valor dentro de un archivo .json. El XML de los metadatos debe estar codificado como una cadena de escape JSON.

```
{
   "sessionTimeout": 70,
   "groupAttribute": "department",
   "userAttribute": "userid",
   "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>"
}
```

Ver proveedores SAML

La siguiente ListSecurityConfigssolicitud muestra una lista de todos los proveedores de SAML de tu cuenta:

```
aws opensearchserverless list-security-configs --type saml
```

La solicitud devuelve información sobre todos los proveedores de SAML existentes, incluidos los metadatos completos del IdP que genera su proveedor de identidades:

```
{
   "securityConfigDetails": [
      {
         "configVersion": "MTY2NDA1MjY4NDQ5M18x",
         "createdDate": 1664054180858,
         "description": "Example SAML provider",
         "id": "saml/123456789012/myprovider",
         "lastModifiedDate": 1664054180858,
         "samlOptions": {
            "groupAttribute": "department",
            "metadata": "<EntityDescriptor xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata
\" ... ... ... IDPSSODescriptor>\r\n<\/EntityDescriptor>",
            "sessionTimeout": 120,
            "userAttribute": "userid"
         }
      }
   ]
}
```

Para ver los detalles de un proveedor específico, incluida la `configVersion` para actualizaciones futuras, envíe una solicitud `GetSecurityConfig`.

Actualización de proveedores SAML

Para actualizar un proveedor de SAML mediante la consola OpenSearch sin servidor, elige la autenticación SAML, selecciona tu proveedor de identidad y selecciona Editar. Puede modificar todos los campos, incluidos los metadatos y los atributos personalizados.

Para actualizar un proveedor a través de la API OpenSearch sin servidor, envía una UpdateSecurityConfigsolicitud e incluye el identificador de la política que se va a actualizar. También debe incluir una versión de configuración, que puede recuperar mediante los comandos

`ListSecurityConfigs` o `GetSecurityConfig`. Incluir la versión más reciente garantiza que no se anule inadvertidamente un cambio realizado por otra persona.

La siguiente solicitud actualiza las opciones de SAML de un proveedor:

```
aws opensearchserverless update-security-config \
    --id saml/123456789012/myprovider \
    --type saml \
    --saml-options file://saml-auth0.json \
    --config-version MTY2NDA1MjY4NDQ5M18x
```

Especifique las opciones de configuración de SAML como un mapa clave-valor dentro de un archivo .json.

> **Important**
>
> Las actualizaciones de las opciones de SAML no son graduales. Si al realizar una actualización no especifica el valor para un parámetro en el objeto `SAMLOptions`, los valores existentes se sustituirán por valores vacíos. Por ejemplo, si la configuración actual contiene un valor para `userAttribute` y luego hace una actualización y no incluye este valor, el valor se elimina de la configuración. Asegúrese de saber cuáles son los valores existentes antes de realizar una actualización llamando a la operación `GetSecurityConfig`.

Eliminar proveedores SAML

Al eliminar un proveedor de SAML, las referencias de los usuarios y grupos asociados en las políticas de acceso a datos dejan de funcionar. Para evitar confusiones, le recomendamos que elimine todas las referencias al punto de conexión en sus políticas de acceso antes de eliminar el punto de conexión.

Para eliminar un proveedor de SAML mediante la consola OpenSearch sin servidor, elija Autenticación, seleccione el proveedor y elija Eliminar.

Para eliminar un proveedor a través de la API OpenSearch sin servidor, envía una solicitud: DeleteSecurityConfig

```
aws opensearchserverless delete-security-config --id saml/123456789012/myprovider
```

Validación de conformidad para Amazon OpenSearch sin servidor

Auditores externos evalúan la seguridad y la conformidad de Amazon OpenSearch sin servidor como parte de varios programas de conformidad de AWS. Entre estos, se incluyen SOC, PCI e HIPAA.

Para saber si un servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y escoja el programa de conformidad que le interese. 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 servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Guías de inicio rápido de seguridad y conformidad: estas guías de implementación tratan consideraciones sobre arquitectura y ofrecen pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Arquitectura para la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico, se describe cómo las empresas pueden utilizar AWS para crear aplicaciones aptas para HIPAA.

  > **Note**
  >
  > No todos los Servicios de AWS son aptos para HIPAA. Para obtener más información, consulte la Referencia de servicios aptos para HIPAA.

- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).

- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Etiquetado de colecciones de Amazon OpenSearch sin servidor

Las etiquetas permiten asignar información arbitraria a un dominio de Amazon OpenSearch sin servidor para poder categorizar y filtrar esa información. Una etiqueta es un elemento de metadatos que usted o AWS asigna a un recurso de AWS.

Cada etiqueta consta de una key (clave) y un value (valor). En el caso de etiquetas que usted asigna, debe definir la clave y el valor. Por ejemplo, puede definir la clave como `stage` y el valor de un recurso como `test`.

Con una etiqueta, puede hacer lo siguiente:

- Identificar y organizar sus recursos de AWS. Muchos servicios de AWS admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, podría asignarle la misma etiqueta a una colección de OpenSearch sin servidor que se le concede a un dominio de Amazon OpenSearch Service.
- Realizar un seguimiento de los costos de AWS. Estas etiquetas se activan en el panel de AWS Billing and Cost Management. AWS usa las etiquetas para clasificar los costos y enviar un informe mensual de asignación de costos. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la Guía del usuario de AWS Billing.

En OpenSearch sin servidor, el recurso principal es una colección. Puede utilizar la consola de OpenSearch Service, la AWS CLI, las operaciones de la API de OpenSearch sin servidor o los AWS SDK para agregar, administrar y eliminar etiquetas de una colección.

Permisos necesarios

OpenSearch sin servidor utiliza los siguientes permisos AWS Identity and Access Management Access Analyzer (IAM) para etiquetar colecciones:

- `aoss:TagResource`
- `aoss:ListTagsForResource`
- `aoss:UntagResource`

Uso de etiquetas (consola)

La consola es la forma más sencilla para etiquetar un dominio.

Para crear una etiqueta (consola)

1. Inicie sesión en la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. Expanda Serverless (Sin servidor) en el panel de navegación de la izquierda y seleccione Collections (Colecciones).
3. Seleccione la colección a la que desee agregar etiquetas y vaya a la pestaña Tags (Etiquetas).
4. Elija Administrar y Add new tag (Agregar nueva etiqueta).
5. Introduzca una clave de etiqueta y un valor opcional.
6. Seleccione Save.

Para eliminar una etiqueta, siga los mismos pasos y elija Remove (Quitar) en la página Manage tags (Administrar etiquetas).

Para obtener más información sobre cómo utilizar la consola para trabajar con etiquetas, consulte Tag Editor en la Guía de introducción a la consola de administración de AWS.

Uso de etiquetas (AWS CLI)

Para etiquetar una colección mediante la AWS CLI, envíe una solicitud de TagResource:

```
aws opensearchserverless tag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

```
  --tags Key=service,Value=aoss Key=source,Value=logs
```

Consulte las etiquetas existentes para una colección con el comando ListTagsForResource:

```
aws opensearchserverless list-tags-for-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
```

Elimine las etiquetas de una colección mediante el comando UntagResource:

```
aws opensearchserverless untag-resource
  --resource-arn arn:aws:aoss:us-east-1:123456789012:collection/my-collection
  --tag-keys service
```

Operaciones y complementos compatibles en Amazon OpenSearch Serverless

Amazon OpenSearch Serverless admite diversos OpenSearch complementos, así como un subconjunto de las operaciones de la API de indexación, búsqueda y metadatos disponibles en. OpenSearch Puede incluir los permisos en la columna izquierda de la tabla dentro de las políticas de acceso a datos para limitar el acceso a determinadas operaciones.

Temas

- Operaciones y permisos de OpenSearch API compatibles
- OpenSearch Plugins compatibles

Operaciones y permisos de OpenSearch API compatibles

En la siguiente tabla, se enumeran las operaciones de API que admite OpenSearch Serverless, junto con sus permisos de IAM correspondientes:

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:CreateIndex`	PUT <index>	Crea índices. Para obtener más información, consulte la sección Crear un índice.

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
		Note Este permiso también se aplica a la creación de índices con los datos de muestra en OpenSearch los paneles.
`aoss:DescribeIndex`	• GET <index> • GET <index>/_mapping • GET <index>/_mappings • GET <index>/_setting • GET <index>/_setting/ <setting> • GET <index>/_settings • GET <index>/_settings/ <setting> • GET _cat/indices • GET _mapping • GET _mappings • GET _resolve/index/ <index>	Describe los índices. Para obtener más información, consulte los siguientes recursos: • Obtener índice • Obtener un mapeo • Obtener la configuración • Índices CAT (la respuesta no incluye `health` ningún `status` campo).

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:WriteDocument`	• ELIMINAR <index>/_doc/ <id> • POST <index>/_bulk • POST <index>/_doc/ <id> (solo para tipos de colecciones de búsquedas) • POST <index>/_doc • POST <index>/_update/<id> • POST _bulk • PUT <index>/_create/<id> (solo para tipos de colecciones de búsquedas) • PUT <index>/_doc/<id> (solo para tipos de colecciones de búsquedas)	Redacta y actualiza documentos. Para obtener más información, consulte los recursos de siguientes: • Bulk • Índice de datos **Note** Algunas operaciones solo están permitidas para colecciones de tipos `SEARCH`. Para obtener más información, consulte the section called “Elección de un tipo de colección”.

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:ReadDocument`	• GET <index>/_analyze • GET <index>/_doc/ <id> • GET <index>/_explain/ <id> • GET <index>/_mget • GET <index>/_source/ <id> • GET <index>/_count • GET <index>/_field_caps • GET <index>/_msearch • GET <index>/_rank_eval • GET <index>/_search • GET <index>/_validate/ <query> • GET _analyze • GET _field_caps • GET _mget • GET _search • HEAD <index>/_doc/ <id> • HEAD <index>/_source/ <id> • POST <index>/_analyze • POST <index>/_explain/ <id> • POST <index>/_count • POST <index>/_field_caps • POST <index>/_rank_eval • POST <index>/_search • POST _analyze • POST _field_caps • POST _search	Lee los documentos. Para obtener más información, consulte los siguientes recursos: • Realice el análisis de texto • Obtener el documento • Recuento • Consulte DSL • Evaluación de clasificación • Analice la API • Explique

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:DeleteIndex`	DELETE <target>	Elimina índices. Para obtener más información, consulte Eliminar índices.
`aoss:UpdateIndex`	• POST _mapping • POST <index>/_mapping/ • POST <index>/_mappings/ • POST <index>/_setting • POST <index>/_setting • POST _setting • POST _settings • PUT _mapping • PUT <index>/_mapping • PUT <index>/_mapping • PUT <index>/_setting • PUT <index>/_settings • PUT _setting • PUT _settings	Actualiza las configuraciones del índice. Para obtener más información, consulte los siguientes recursos: • Mapeo • Actualizar las configuraciones
`aoss:CreateCollectionItems`	POST _aliases	Crea alias de índice. Para obtener más información, consulte Crear alias.

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:DescribeCollectionItems`	• GET <index>/_alias/ <alias> • GET _alias • GET _alias/ <alias> • GET _cat/alias • GET _cat/templates • GET _cat/templates/ <template_name> • GET _component_template • GET _component_template/ <component-template> • GET _index_template • GET _index_template/ <index-template> • HEAD _alias/ <alias> • HEAD _component_template/ <component-template> • HEAD _index_template/ <name> • HEAD <index>/_alias/ <alias>	Describe los alias y las plantillas del índice. Para obtener más información, consulte los siguientes recursos: • Administrar alias • Plantillas del índice

Permiso de política de acceso a datos	OpenSearch Operaciones de API	Descripción y advertencias
`aoss:UpdateCollectionItems`	• POST <index>/_alias/ <alias> • POST <index>/_aliases/ <alias> • POST _component_template/ <component-template> • POST _index_template/ <index-template> • PUT <index>/_alias/ <alias> • PUT <index>/_aliases/ <alias> • PUT _component_template/ <component-template> • PUT _index_template/ <index-template>	Actualiza los alias y las plantillas del índice. Para obtener más información, consulte los siguientes recursos: • Alias de índice • Plantillas del índice
`aoss:DeleteCollectionItems`	• DELETE <index>/_alias/ <alias> • DELETE _component_template/ <component-template> • DELETE _index_template/ <index-template> • DELETE <index>/_aliases/ <alias>	Elimina los alias y las plantillas del índice. Para obtener más información, consulte los siguientes recursos: • Eliminar alias • Elimina una plantilla

OpenSearch Plugins compatibles

OpenSearch Las colecciones sin servidor vienen preempaquetadas con los siguientes complementos de la OpenSearch comunidad. La ejecución sin servidor implementa y administra automáticamente los complementos.

Complementos de análisis

- ICU Analysis
- Japanese (kuromoji) Analysis

- Análisis coreano (Nori)
- Phonetic Analysis
- Smart Chinese Analysis
- Stempel Polish Analysis
- Ukrainian Analysis

Complementos de Mapper

- Mapper Size
- Mapper Murmur3
- Texto anotado de Mapper

Complementos de la creación de scripts

- Painless
- Expression
- Mustache

Además, OpenSearch Serverless incluye todos los complementos que se envían como módulos.

Supervisión de Amazon OpenSearch Serverless

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon OpenSearch Serverless y sus demás AWS soluciones. AWS proporciona las siguientes herramientas de monitoreo para monitorear OpenSearch Serverless, informar cuando algo anda mal y tomar medidas automáticas cuando sea apropiado:

- Amazon CloudWatch monitorea tus AWS recursos y las aplicaciones en las que AWS ejecutas en tiempo real. Puede recopilar métricas y realizar un seguimiento de las métricas, crear paneles personalizados y definir alarmas que le advierten o que toman medidas cuando una métrica determinada alcanza el umbral que se especifique.

  Por ejemplo, puede CloudWatch hacer un seguimiento del uso de la CPU u otras métricas de sus instancias de Amazon EC2 y lanzar automáticamente nuevas instancias cuando sea necesario. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

- AWS CloudTrail captura las llamadas a la API y los eventos relacionados realizados por su cuenta de Cuenta de AWSo en su nombre. Entrega los archivos de registro al bucket de Amazon S3 que se especifique. Puede identificar qué usuarios y cuentas llamaron AWS, la dirección IP de origen desde la que se realizaron las llamadas y cuándo se produjeron las llamadas. Para más información, consulte la Guía del usuario deAWS CloudTrail.
- Amazon EventBridge ofrece una transmisión casi en tiempo real de los eventos del sistema que describen los cambios en sus dominios OpenSearch de servicio. Puede crear reglas que vigilen ciertos eventos y activar acciones automatizadas en otros Servicios de AWS cuando se produzcan estos eventos. Para obtener más información, consulta la Guía del EventBridge usuario de Amazon.

Supervisión OpenSearch sin servidor con Amazon CloudWatch

Puede supervisar Amazon OpenSearch Serverless mediante Amazon Serverless CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, de forma que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio.

También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

OpenSearch Serverless informa de las siguientes métricas en el `AWS/AOSS` espacio de nombres.

Métrica	Descripción
`ActiveCollection`	Indica si una colección está activa. Un valor de 1 significa que la colección está en estado `ACTIVE`. Este valor se emite al crear correctamente una colección y permanece como 1 hasta que esta se elimine. La métrica no puede tener un valor de 0. Estadísticas pertinentes: máximo Dimensiones: `ClientId`, `CollectionId` , `CollectionName`

Métrica	Descripción
	Frecuencia: 60 segundos
`DeletedDocuments`	El número total de documentos eliminados. Estadísticas pertinentes: promedio, suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frecuencia: 60 segundos
`IndexingOCU`	El número de unidades de OpenSearch cómputo (OCU) utilizadas para ingerir los datos recopilados. Esta métrica se aplica según el nivel de la cuenta. Estadísticas pertinentes: suma Dimensiones: `ClientId` Frecuencia: 60 segundos
`IngestionDataRate`	La velocidad de indexación en GiB por segundo de una colección o índice. Esta métrica se aplica únicamente a las solicitudes de indexación masiva. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frecuencia: 60 segundos

Métrica	Descripción
`IngestionDocumentErrors`	Número total de errores del documento durante el procesamiento de una colección o índice. Tras una solicitud de indexación masiva satisfactoria, los redactore s procesan la solicitud y emiten errores para todos los documentos fallidos incluidos en la solicitud. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `Collectio nName` , `IndexId`, `IndexName` Frecuencia: 60 segundos
`IngestionDocumentRate`	La velocidad por segundo a la que se incorporan los documentos a una colección o índice. Esta métrica se aplica únicamente a las solicitudes de indexación masiva. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `Collectio nName` , `IndexId`, `IndexName` Frecuencia: 60 segundos
`IngestionRequestErrors`	El número total de errores de solicitud de indexación masiva en una colección. OpenSearch Serverless emite esta métrica cuando una solicitud de indexación masiva falla por cualquier motivo, como un problema de autentica ción o disponibilidad. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `Collectio nName` Frecuencia: 60 segundos

Métrica	Descripción
`IngestionRequestLatency`	La latencia, en segundos, de las operaciones de escritura masiva en una colección. Estadísticas pertinentes: mínimo, máximo, promedio Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos
`IngestionRequestRate`	El número total de operaciones de escritura masiva recibidas por una colección. Estadísticas pertinentes: mínimo, máximo, promedio Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos
`IngestionRequestSuccess`	El número de operaciones de indexación de datos de una colección. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos
`SearchableDocuments`	Número total de documentos susceptibles de búsqueda en una colección o índice. Estadísticas pertinentes: Suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frecuencia: 60 segundos

Métrica	Descripción
`SearchRequestErrors`	El número total de errores de consulta por minuto de una colección. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos
`SearchRequestLatency`	El tiempo promedio, en milisegundos, que se tarda en completar una operación de búsqueda en una colección. Estadísticas pertinentes: mínimo, máximo, promedio Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos
`SearchOCU`	El número de unidades de OpenSearch cómputo (OCU) utilizadas para buscar los datos de la recopilación. Esta métrica se aplica según el nivel de la cuenta. Estadísticas pertinentes: suma Dimensiones: `ClientId` Frecuencia: 60 segundos
`SearchRequestRate`	El número total de solicitudes de búsqueda por minuto para una colección. Estadísticas pertinentes: promedio, máximo, suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos

Métrica	Descripción
`StorageUsedInS3`	La cantidad, en bytes, de almacenamiento de Amazon S3 utilizada. OpenSearch La tecnología Serverless almacena los datos indexados en Amazon S3. Debe seleccionar el periodo en un minuto para obtener un valor preciso. Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` , `IndexId`, `IndexName` Frecuencia: 60 segundos
`2xx, 3xx, 4xx, 5xx`	El número de solicitudes para la colección que produjeron el código de respuesta HTTP especificado (2xx, 3xx, 4xx, 5xx). Estadísticas pertinentes: suma Dimensiones: `ClientId`, `CollectionId` , `CollectionName` Frecuencia: 60 segundos

Registrar las llamadas a la OpenSearch API sin servidor mediante AWS CloudTrail

Amazon OpenSearch Serverless está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en Serverless.

CloudTrail captura todas las llamadas a la API de OpenSearch Serverless como eventos. Las llamadas capturadas incluyen las llamadas de la sección Serverless de la consola de OpenSearch servicio y las llamadas en código a las operaciones de la API OpenSearch Serverless.

Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para OpenSearch Serverless. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a OpenSearch Serverless, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la Guía delAWS CloudTrail usuario.

OpenSearch Información sobre sistemas sin servidor en CloudTrail

CloudTrail está habilitada en tu cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en OpenSearch Serverless, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de tus eventos Cuenta de AWS, incluidos los eventos de OpenSearch Serverless, crea una ruta. Un rastro permite CloudTrail entregar 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.

La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail servicios e integraciones compatibles
- Configuración de las notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

Todas las acciones de OpenSearch Serverless se registran CloudTrail y se documentan en la referencia de la API OpenSearch Serverless. Por ejemplo, las llamadas a las `CreateCollection` `DeleteCollection` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `ListCollections`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad le ayuda a determinar:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (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 AWS servicio.

Para obtener más información, consulte el elemento userIdentity de CloudTrail .

Descripción de las entradas de los archivos de registro OpenSearch sin servidor

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro.

Un evento representa una única solicitud desde cualquier origen. Incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a las API públicas, por lo que no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de CloudTrail registro que demuestra la `CreateCollection` acción.


```
{
   "eventVersion":"1.08",
   "userIdentity":{
      "type":"AssumedRole",
      "principalId":"AIDACKCEVSQ6C2EXAMPLE",
      "arn":"arn:aws:iam::123456789012:user/test-user",
      "accountId":"123456789012",
      "accessKeyId":"access-key",
      "sessionContext":{
         "sessionIssuer":{
            "type":"Role",
            "principalId":"AIDACKCEVSQ6C2EXAMPLE",
            "arn":"arn:aws:iam::123456789012:role/Admin",
            "accountId":"123456789012",
            "userName":"Admin"
         },
         "webIdFederationData":{
```

```
         },
         "attributes":{
            "creationDate":"2022-04-08T14:11:34Z",
            "mfaAuthenticated":"false"
         }
      }
   },
   "eventTime":"2022-04-08T14:11:49Z",
   "eventSource":"aoss.amazonaws.com",
   "eventName":"CreateCollection",
   "awsRegion":"us-east-1",
   "sourceIPAddress":"AWS Internal",
   "userAgent":"aws-cli/2.1.30 Python/3.8.8 Linux/5.4.176-103.347.amzn2int.x86_64 exe/
x86_64.amzn.2 prompt/off command/aoss.create-collection",
   "errorCode":"HttpFailureException",
   "errorMessage":"An unknown error occurred",
   "requestParameters":{
      "accountId":"123456789012",
      "name":"test-collection",
      "description":"A sample collection",
      "clientToken":"d3a227d2-a2a7-49a6-8fb2-e5c8303c0718"
   },
   "responseElements": null,
   "requestID":"12345678-1234-1234-1234-987654321098",
   "eventID":"12345678-1234-1234-1234-987654321098",
   "readOnly":false,
   "eventType":"AwsApiCall",
   "managementEvent":true,
   "recipientAccountId":"123456789012",
   "eventCategory":"Management",
   "tlsDetails":{
      "clientProvidedHostHeader":"user.aoss-sample.us-east-1.amazonaws.com"
   }
}
```


Supervisión de eventos OpenSearch sin servidor mediante Amazon EventBridge

Amazon OpenSearch Service se integra con Amazon EventBridge para notificarte determinados eventos que afectan a tus dominios. Los eventos de AWS los servicios se envían casi EventBridge en tiempo real. Los mismos eventos también se envían a Amazon CloudWatch Events, la predecesora de Amazon EventBridge. Puede crear reglas 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. Entre los ejemplos de acciones que puede activar automáticamente se incluyen los siguientes:

- Invocar una función AWS Lambda
- Invocar un Run Command de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activación de una máquina de estados AWS Step Functions
- Notificar un tema de Amazon SNS o una cola de Amazon SQS

Para obtener más información, consulta Cómo empezar con Amazon EventBridge en la Guía del EventBridge usuario de Amazon.

Configuración de notificaciones

Puede utilizar las notificacionesAWS de usuario para recibir notificaciones cuando se produzca un evento OpenSearch sin servidor. Un evento es un indicador de un cambio en un entorno OpenSearch sin servidor, por ejemplo, cuando se alcanza el límite máximo de uso de la OCU. Amazon EventBridge recibe el evento y envía una notificación al Centro de AWS Management Console notificaciones y a los canales de entrega que elijas. Recibirá una notificación cuando un evento coincida con una regla que especifique.

OpenSearch Eventos de unidades de cómputo (OCU)

OpenSearch Serverless envía los eventos al EventBridge momento en que se produce uno de los siguientes eventos relacionados con la OCU.

Uso de OCU cercano al límite máximo

OpenSearch Serverless envía este evento cuando el uso de la OCU de búsqueda o indexación alcanza el 75% del límite de capacidad. El uso de OCU se calcula en función del límite de capacidad configurado y del consumo actual de OCU.

Ejemplo

A continuación, se muestra un ejemplo de este evento (OCU de búsqueda):

```
{
  "version": "0",
```

```
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
}
```

A continuación, se muestra un ejemplo de este evento (OCU de indexación):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Approaching Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage is at 75% and is approaching the configured
 maximum limit."
  }
```

El uso de OCU ha alcanzado el límite máximo

OpenSearch Serverless envía este evento cuando el uso de la OCU de búsqueda o indexación alcanza el 100% del límite de capacidad. El uso de OCU se calcula en función del límite de capacidad configurado y del consumo actual de OCU.

Ejemplo

A continuación, se muestra un ejemplo de este evento (OCU de búsqueda):

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your search OCU usage has reached the configured maximum limit."
  }
}
```

A continuación, se muestra un ejemplo de este evento (OCU de indexación):

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "OCU Utilization Reached Max Limit",
  "source": "aws.aoss",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "eventTime" : 1678943345789,
    "description": "Your indexing OCU usage has reached the configured maximum limit."
  }
}
```

Creación y administración de dominios OpenSearch de Amazon Service

En este capítulo se describe cómo crear y gestionar los dominios OpenSearch de Amazon Service. Un dominio de OpenSearch servicio es sinónimo de OpenSearch clúster. Los dominios son clústeres con la configuración, los tipos de instancia, los recuentos de instancias y los recursos de almacenamiento que especifique.

A diferencia de las breves instrucciones incluidas en el tutorial de introducción, en este capítulo se describen todas las opciones y se proporciona información de referencia relevante. Puede completar cada procedimiento siguiendo las instrucciones de la consola de OpenSearch servicio, el AWS Command Line Interface (AWS CLI) o los AWS SDK.

Creación de dominios OpenSearch de servicio

En esta sección se describe cómo crear OpenSearch dominios de OpenSearch servicio mediante la consola de servicio o mediante el AWS CLI `create-domain` comando with.

Creación OpenSearch de dominios de servicio (consola)

Utilice el siguiente procedimiento para crear un dominio de OpenSearch servicio mediante la consola.

Para crear un dominio OpenSearch de servicio (consola)

1. Visite https://aws.amazon.com y elija Iniciar sesión en la consola.
2. En Analytics, selecciona Amazon OpenSearch Service.
3. Seleccione Create domain (Crear un dominio).
4. Para el Nombre de dominio, escriba un nombre de dominio. El nombre debe cumplir los siguientes criterios:
   - Único para su cuenta y Región de AWS
   - Comenzar por una letra minúscula.
   - Contener entre 3 y 28 caracteres.
   - Contiene únicamente letras minúsculas a-z, números de 0-9 y un guion (-).
5. Seleccione Creación estándar para el método de creación del dominio.
6. En Plantillas, seleccione la opción que mejor se ajuste a la finalidad del dominio:

- Dominios de producción para cargas de trabajo que necesitan alta disponibilidad y rendimiento. Estos dominios utilizan Multi-AZ (con o sin modo de espera) y nodos principales dedicados para una mayor disponibilidad.
- Desarrollo/pruebas para desarrollo o pruebas. Estos dominios pueden usar Multi-AZ (con o sin modo de espera) o una única zona de disponibilidad.

> **Important**
>
> Los diversos tipos de implementación presentarán opciones distintas en las páginas siguientes. Estos pasos incluyen todas las opciones.

7. En cuanto a las Opciones de implementación, seleccione Dominio con modo de espera para configurar un dominio 3-AZ, con los nodos de una de las zonas reservados como don modo de espera. Esta opción aplica una serie de prácticas recomendadas, como un recuento de nodos de datos específico, un recuento de nodos maestros, un tipo de instancia, un recuento de réplicas y una configuración de actualización de software.
8. En Versión, elija la versión del OSS Elasticsearch anterior OpenSearch o la versión anterior que desee utilizar. Le recomendamos que elija la última versión de. OpenSearch Para obtener más información, consulte the section called “Versiones compatibles de OpenSearch y Elasticsearch”.

   (Opcional) Si has elegido una OpenSearch versión para tu dominio, selecciona Habilitar el modo de compatibilidad para que su versión se OpenSearch muestre como 7.10, lo que permite que determinados clientes y complementos de Elasticsearch OSS que comprueben la versión antes de conectarse puedan seguir trabajando con el servicio.
9. En Instance type (Tipo de instancia), elija un tipo de instancia para los nodos de datos. Para obtener más información, consulte the section called “Tipos de instancias admitidas”.

   > **Note**
   >
   > No todas las zonas de disponibilidad admiten todos los tipos de instancias. Si elige Multi-AZ con o sin modo de espera, recomendamos elegir tipos de instancias de la generación actual, como R5 o I3.
10. Para el Número de nodos, elija el número de nodos de datos.

    Para ver los valores máximos, consulta Cuotas de dominios e OpenSearch instancias del servicio. Los clústeres de un solo nodo son adecuados para desarrollo y pruebas, pero no deben

utilizarse para cargas de trabajo de producción. Para obtener más información, consulte the section called “Determinación del tamaño de dominios” y the section called “Configuración de un dominio multi-AZ”.

11. Para Tipo de almacenamiento, seleccione Amazon EBS. Los tipos de volumen disponibles en la lista dependen del tipo de instancia que haya elegido. Para obtener instrucciones sobre cómo crear dominios especialmente grandes, consulte the section called “Escala de petabytes”.
12. Para el almacenamiento EBS, configure los siguientes ajustes adicionales. Es posible que algunos ajustes no aparezcan en función del tipo de volumen que elija.

Opción	Descripción
Tipo de volumen de EBS	Seleccione entre General Purpose (SSD) - gp3 (Uso general) y General Purpose (SSD) - gp2 (Uso general), o la generación anterior Provisioned IOPS (SSD) (IOPS aprovisionadas), y Magnetic (Magnético) (estándar).
Tamaño de almacenamiento de EBS por nodo	Ingrese el tamaño del volumen de EBS que desea adjuntar a cada nodo de datos. Tamaño de volumen de EBS es por cada nodo. Puede calcular el tamaño total del clúster del dominio de OpenSearch servicio multiplicando el número de nodos de datos por el tamaño del volumen de EBS. El tamaño mínimo y máximo de un volumen de EBS depende tanto del tipo de volumen de EBS especificado como del tipo de instancia al que se ha adjuntado. Para obtener más información, consulte las restricciones de tamaño del volumen de EBS.
Provisioned IOPS (IOPS aprovisionadas)	Si ha seleccionado un tipo de volumen IOPS aprovisionadas de SSD, ingrese el número de operaciones de E/S por segundo (IOPS) que puede soportar el volumen.

13. (Opcional) Si ha seleccionado un tipo de volumen gp3, amplíe la Configuración avanzada y especifique IOPS adicionales (hasta 1000 MiB/s por cada 3 TiB de tamaño de volumen aprovisionado por nodo de datos) y rendimiento (hasta 16 000 por cada 3 TiB de tamaño de volumen aprovisionado por nodo de datos) para aprovisionar para cada nodo, más allá de lo

que se incluye con el precio del almacenamiento, por un costo adicional. Para obtener más información, consulta los precios OpenSearch de Amazon Service.

14. (Opcional) Para habilitar el UltraWarm almacenamiento, selecciona Habilitar nodos UltraWarm de datos. Cada tipo de instancia tiene una cantidad máxima de almacenamiento que puede poner a disposición. Multiplique esa cantidad por el número de nodos de datos templados para obtener el almacenamiento templado total a disposición.
15. (Opcional) Para habilitar el almacenamiento en frío, seleccione Habilitar almacenamiento en frío. Debe habilitarlo UltraWarm para habilitar el almacenamiento en frío.
16. Si utiliza Multi-AZ con modo de espera, ya hay tres nodos maestros dedicados habilitados. Seleccione el tipo de nodos maestros que desee. Si eligió un dominio Multi-AZ sin modo de espera, seleccione Habilitar nodos maestros dedicados y elija el tipo y la cantidad de nodos maestros que desee. Los nodos maestros dedicados aumentan la estabilidad de los clústeres y son necesarios en los dominios que tienen un número de instancias mayor de 10. Recomendamos utilizar tres nodos maestros dedicados en los dominios de producción.

> **Note**
>
> Puede elegir tipos de instancias diferentes para los nodos maestros dedicados y los nodos de datos. Por ejemplo, para los nodos de datos, puede elegir instancias de uso general u optimizadas para el almacenamiento y, para los nodos maestros dedicados, instancias optimizadas para computación.

17. (Opcional) En el caso de los dominios que ejecutan Elasticsearch 5.3 OpenSearch o versiones posteriores, la configuración de Snapshot es irrelevante. Para obtener más información sobre las instantáneas automatizadas, consulte the section called “Crear instantáneas de índice”.
18. Si desea utilizar un punto de conexión personalizado en lugar del estándar de `https://search-`*`mydomain`*`-`*`1a2a3a4a5a6a7a8a9a0a9a8a7a`*`.`*`us-east-1`*`.es.amazonaws.com`, seleccione Habilitar punto de enlace personalizado y proporcione un nombre y un certificado. Para obtener más información, consulte the section called “Creación de un punto de conexión personalizado”.
19. En Red, seleccione Acceso a la VPC o Acceso público. Si elige Acceso público, vaya al siguiente paso. Si elige Acceso a la VPC, asegúrese de que se cumplen los requisitos previos y, a continuación, haga lo siguiente:

Opción	Descripción
VPC	Seleccione el ID de la nube privada virtual (VPC) que desee utilizar. La VPC y el dominio deben estar en el mismo Región de AWS lugar y debe seleccionar una VPC con la tenencia configurada como Predeterminada. OpenSearch El servicio aún no admite las VPC que utilizan un arrendami ento dedicado.
Subred	Seleccione una subred. Si ha activado Multi-AZ, debe elegir dos o tres subredes. OpenSearch El servicio colocará un punto final de VPC e interfaces de red elásticas en las subredes. Debe reservar suficientes direcciones IP para las interfaces de red en la subred o subredes. Para obtener más información, consulte Reserva de direcciones IP en una subred de una VPC.
Grupos de seguridad	Elija uno o más grupos de seguridad de VPC que permitan que la aplicación requerida llegue al dominio del OpenSearch servicio en los puertos (80 o 443) y protocolos (HTTP o HTTPS) expuestos por el dominio. Para obtener más información, consulte the section called “Compatibilidad con VPC”.
IAM Role	Mantenga el rol predeterminado. OpenSearch El servicio usa esta función predefinida (también conocida como función vinculada a un servicio) para acceder a la VPC y colocar un punto final de la VPC y las interfaces de red en la subred de la VPC. Para obtener más información, consulte Roles vinculados a servicios para el acceso de VPC.
Tipo de dirección IP	Seleccione el tipo de dirección IP de doble pila o IPv4. La doble pila le permite compartir los recursos del dominio entre los tipos de direcciones IPv4 e IPv6, y es la opción recomendada. Si configura el tipo de dirección IP en doble pila, no podrá cambiarlo más adelante.

20. Habilite o deshabilite el control de acceso detallado:

    - Si desea utilizar IAM para la gestión de usuarios, seleccione Establecer ARN de IAM como usuario maestro y especifique el ARN para un rol de IAM.

- Si desea utilizar la base de datos de usuarios interna, seleccione Crear usuario maestro y especifique un nombre de usuario y una contraseña.

Sea cual sea la opción que elija, el usuario maestro puede acceder a todos los índices del clúster y a todas las API. OpenSearch Para obtener información sobre qué opción elegir, consulte the section called “Conceptos clave”.

Si deshabilita el control de acceso detallado, puede controlar el acceso a su dominio al colocarlo dentro de una VPC, al aplicar una política de acceso restrictiva o puede utilizar ambas opciones. Debe habilitar el node-to-node cifrado y el cifrado en reposo para utilizar un control de acceso detallado.

> **Note**
>
> Se recomienda encarecidamente habilitar un control de acceso detallado para proteger los datos del dominio. El control de acceso detallado proporciona seguridad en los niveles de clúster, índice, documento y campo.

21. (Opcional) Si quiere usar la autenticación SAML para los OpenSearch paneles, elija Habilitar la autenticación SAML y configure las opciones de SAML para el dominio. Para ver instrucciones, consulte the section called “Autenticación SAML para paneles OpenSearch ”.
22. (Opcional) Si desea utilizar la autenticación de Amazon Cognito para los OpenSearch paneles, elija Activar la autenticación de Amazon Cognito. A continuación, elija el grupo de usuarios y el grupo de identidades de Amazon Cognito que desee utilizar para la autenticación de OpenSearch Dashboards. Para obtener orientación sobre cómo crear estos recursos, consulte the section called “Descripción de la autenticación de Amazon Cognito para OpenSearch Dashboards”.
23. En Política de acceso, seleccione una política de acceso o configure una de las que posee. Si decide crear una política personalizada, puede configurarla usted mismo o importar una de otro dominio. Para obtener más información, consulte the section called “Identity and Access Management”.

> **Note**
>
> Si habilitó el acceso de la VPC, no puede utilizar políticas basadas en IP. En su lugar, puede utilizar grupos de seguridad para controlar qué direcciones IP pueden tener

acceso al dominio. Para obtener más información, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”.

24. (Opcional) Para determinar que todas las solicitudes al dominio lleguen a través de HTTPS, seleccione Require HTTPS for all traffic to the domain (Solicitar HTTPS para todo el tráfico del dominio). Para habilitar el node-to-node cifrado, seleccione el cifrado N. ode-to-node Para obtener más información, consulte the section called “Sin ode-to-node cifrado”. Para habilitar el cifrado de los datos en reposo, seleccione Habilitar cifrado de datos en reposo. Estas opciones están preseleccionadas si elige la opción de implementación de Multi-AZ con modo de espera.
25. (Opcional) Seleccione AWS Usar una clave propia para que el OpenSearch Servicio cree una clave de AWS KMS cifrado en su nombre (o use la que ya creó). De lo contrario, elija su propia clave de KMS. Para obtener más información, consulte the section called “Cifrado en reposo”.
26. Para las Ventanas de menor actividad, seleccione una hora de inicio para programar las actualizaciones del software del servicio y las optimizaciones de ajuste automático que requieran una implementación azul/verde. Las actualizaciones en ventanas de menor actividad ayudan a minimizar la carga de los nodos maestros dedicados de un clúster durante los períodos de alto tráfico.
27. En el caso de Auto-Tune, elige si quieres que el OpenSearch Servicio sugiera cambios de configuración relacionados con la memoria en tu dominio para mejorar la velocidad y la estabilidad. Para obtener más información, consulte the section called “Ajuste automático”.

    (Opcional) Seleccione Ventana de menor actividad para programar una ventana periódica para que el ajuste automático actualice el dominio.
28. (Opcional) Seleccione Actualización automática de software para activar las actualizaciones automáticas de software.
29. (Opcional) Agregue etiquetas para describir el dominio para que pueda categorizar y filtrar esa información. Para obtener más información, consulte the section called “Etiquetado de dominios”.
30. (Opcional) Expanda y configure Advanced cluster settings (Configuración avanzada del clúster). Para obtener un resumen de estas opciones, consulte the section called “Configuración avanzada de clústeres”.
31. Seleccione Crear.

Creación de dominios de OpenSearch servicio ()AWS CLI

En lugar de crear un dominio de OpenSearch servicio mediante la consola, puede utilizar la AWS CLI. Para conocer la sintaxis, consulte Amazon OpenSearch Service en la referencia de comandos AWS CLI a.

Comandos de ejemplo

En este primer ejemplo, se muestra la siguiente configuración del dominio de OpenSearch servicio:

- Crea un dominio OpenSearch de servicio denominado mylogs con la OpenSearch versión 1.2
- Rellena el dominio con dos instancias del tipo `r6g.large.search`.
- Utiliza un volumen de EBS de uso general (SSD) `gp3` de 100 GiB para el almacenamiento de cada nodo de datos
- Permite el acceso anónimo, pero solo desde una única dirección IP: 192.0.2.0/32

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.2 \
    --cluster-config  InstanceType=r6g.large.search,InstanceCount=2 \
    --ebs-options
 EBSEnabled=true,VolumeType=gp3,VolumeSize=100,Iops=3500,Throughput=125 \
    --access-policies '{"Version": "2012-10-17", "Statement": [{"Action": "es:*",
 "Principal":"*","Effect": "Allow", "Condition": {"IpAddress":{"aws:SourceIp":
["192.0.2.0/32"]}}}]}'
```

El siguiente ejemplo muestra la siguiente configuración del dominio OpenSearch de servicio:

- Crea un dominio OpenSearch de servicio denominado mylogs con la versión 7.10 de Elasticsearch
- Rellena el dominio con seis instancias del tipo `r6g.large.search`.
- Utiliza un volumen de EBS de uso general (SSD) `gp2` de 100 GiB para el almacenamiento de cada nodo de datos
- Restringe el acceso al servicio a un solo usuario, identificado por el ID del usuario: 555555555555 Cuenta de AWS
- Distribuye las instancias entre tres zonas de disponibilidad.

```
aws opensearch create-domain \
```

```
    --domain-name mylogs \
    --engine-version Elasticsearch_7.10 \
    --cluster-config
 InstanceType=r6g.large.search,InstanceCount=6,ZoneAwarenessEnabled=true,ZoneAwarenessConfig={A
 \
    --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": {"AWS": "arn:aws:iam::555555555555:root" }, "Action":"es:*", "Resource":
 "arn:aws:es:us-east-1:555555555555:domain/mylogs/*" } ] }'
```

El siguiente ejemplo muestra la siguiente configuración del dominio de OpenSearch servicio:

- Crea un dominio OpenSearch de servicio denominado mylogs con la OpenSearch versión 1.0
- Rellena el dominio con diez instancias del tipo `r6g.xlarge.search`.
- Rellena el dominio con tres instancias del tipo `r6g.large.search` que actuarán como nodos maestros dedicados.
- Usa un volumen de EBS de IOPS aprovisionadas de 100 GiB para el almacenamiento, configurado con una velocidad de referencia de 1000 IOPS por cada nodo de datos
- Restringe el acceso a un único usuario y a un único subrecurso, la API `_search`

```
aws opensearch create-domain \
    --domain-name mylogs \
    --engine-version OpenSearch_1.0 \
    --cluster-config
 InstanceType=r6g.xlarge.search,InstanceCount=10,DedicatedMasterEnabled=true,DedicatedMasterTyp
 \
    --ebs-options EBSEnabled=true,VolumeType=io1,VolumeSize=100,Iops=1000 \
    --access-policies '{"Version": "2012-10-17", "Statement": [ { "Effect": "Allow",
 "Principal": { "AWS": "arn:aws:iam::555555555555:root" }, "Action": "es:*",
 "Resource": "arn:aws:es:us-east-1:555555555555:domain/mylogs/_search" } ] }'
```

> **Note**
>
> Si intenta crear un dominio de OpenSearch servicio y ya existe un dominio con el mismo nombre, la CLI no informa de ningún error. En su lugar, muestra los detalles sobre el dominio existente.

Creación OpenSearch de dominios de servicio (AWS SDK)

Los AWS SDK (excepto los de Android e iOS) admiten todas las acciones definidas en la referencia de la API de Amazon OpenSearch Service, incluidas las siguientes: `CreateDomain` Para ver el código de muestra, consulte the section called “Utilizar los SDK de AWS”. Para obtener más información sobre la instalación y el uso de los AWS SDK, consulte los kits de desarrollo de AWS software.

Creación de dominios OpenSearch de servicio ()AWS CloudFormation

OpenSearch El servicio está integrado con AWS CloudFormation un servicio que le ayuda a modelar y configurar sus AWS recursos para que pueda dedicar menos tiempo a crear y administrar sus recursos e infraestructura. Crea una plantilla que describe el OpenSearch dominio que desea crear y CloudFormation aprovisiona y configura el dominio por usted. Para obtener más información, incluidos ejemplos de plantillas JSON y YAML para OpenSearch dominios, consulta la referencia de tipos de recursos de Amazon OpenSearch Service en la Guía del AWS CloudFormation usuario.

Configurar políticas de acceso

Amazon OpenSearch Service ofrece varias formas de configurar el acceso a tus dominios OpenSearch de servicio. Para más información, consulte the section called “Identity and Access Management” y the section called “Control de acceso detallado”.

La consola proporciona políticas de acceso preconfiguradas que puede personalizar según las necesidades específicas de su dominio. También puede importar políticas de acceso de otros dominios OpenSearch de servicio. Para obtener información sobre cómo interactúan estas políticas de acceso con el acceso de las VPC, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”.

Para configurar políticas de acceso (consola)

1. Visite https://aws.amazon.com y elija Iniciar sesión en la consola.
2. En Analytics, selecciona Amazon OpenSearch Service.
3. En el panel de navegación, en Domains (Dominios), elija el dominio que desea actualizar.
4. Seleccione Acciones y Editar la configuración de seguridad.
5. Edite la política de acceso JSON o importe una opción preconfigurada.
6. Seleccione Guardar cambios.

Configuración avanzada de clústeres

Use opciones avanzadas para configurar lo siguiente:

Índices en los cuerpos de las solicitudes

Especifica si se permiten referencias explícitas a índices en el cuerpo de las solicitudes HTTP. Al configurar esta propiedad en `false` se evita que los usuarios eludan el control de acceso para subrecursos. De forma predeterminada, el valor es `true`. Para obtener más información, consulte the section called “Opciones avanzadas y consideraciones de la API”.

Asignación de una caché de datos de campos

Especifica el porcentaje de espacio de montón de Java que se asignará a datos de campos. De forma predeterminada, esta configuración es el 20 % de la pila de JVM.

> **Note**
>
> Muchos clientes consultan índices diarios en rotación. Recomendamos empezar a realizar ensayos de referencia con el valor `indices.fielddata.cache.size` configurado en un 40 % de la pila de JVM para la mayoría de estos casos de uso. Si tiene índices muy grandes es posible que necesite una caché de datos de campos de gran tamaño.

Recuento máximo de cláusulas

Especifica el número máximo de cláusulas permitidas en una consulta de Lucene con operadores booleanos. El valor predeterminado es 1,024. Las consultas que superen el número máximo permitido de cláusulas provocarán un error `TooManyClauses`. Para obtener más información, consulte la documentación de Lucene.

Realizar cambios de configuración en Amazon OpenSearch Service

Amazon OpenSearch Service utiliza un proceso de despliegue azul/verde al actualizar los dominios. Una implementación azul/verde crea un entorno inactivo para actualizaciones de dominio que copia el entorno de producción y dirige usuarios al nuevo entorno una vez completadas esas actualizaciones. En una implementación azul/verde, el entorno azul es el entorno de producción actual. El entorno verde es el entorno de almacenamiento inactivo.

Los datos se migran del entorno azul al entorno verde. Cuando el nuevo entorno está listo, OpenSearch Service cambia los entornos para promover que el entorno ecológico se convierta en el nuevo entorno de producción. La transición se produce sin pérdida de datos. Esta práctica minimiza el tiempo de inactividad y mantiene el entorno original en caso de que la implementación en el nuevo entorno no se produzca correctamente.

Temas

Cambios que suelen causar implementaciones azul/verde

Las siguientes operaciones provocan implementaciones azul/verde:

- Cambio del tipo de instancia
- Habilitar el control de acceso detallado
- Realización de actualizaciones de software del servicio
- Si su dominio no tiene nodos maestros dedicados, cambio de recuento de instancias de datos
- Activación o desactivación de nodos maestros dedicados
- Activación o desactivación de Multi-AZ sin modo de espera
- Cambio del tipo de almacenamiento, el tipo de volumen o el tamaño de volumen
- Selección de diferentes subredes de VPC
- Agregar o eliminar grupos de seguridad de la VPC
- Activación o desactivación de la autenticación de Amazon Cognito para paneles OpenSearch
- Elección de otro grupo de usuarios o grupo de identidades de Amazon Cognito
- Modificación de la configuración avanzada
- Actualización a una nueva OpenSearch versión (es posible que los OpenSearch paneles no estén disponibles durante una parte o durante toda la actualización)

- Habilitar el cifrado de los datos en reposo o node-to-node el cifrado
- Habilitar UltraWarm o deshabilitar el almacenamiento en frío
- Desactivación de Auto-Tune y restauración de los cambios asociados
- Asociar un complemento opcional a un dominio y disociar un complemento opcional de un dominio
- Aumentar el número de nodos maestros dedicados para los dominios con dos nodos maestros dedicados y habilitar el reconocimiento de zona
- Disminuir el tamaño del volumen de EBS
- Cambiar el tamaño del volumen, las IOPS o el rendimiento de EBS, si el último cambio que realizó está en curso o se produjo hace menos de 6 horas
- Habilitar la publicación de los registros de auditoría en. CloudWatch

En el caso de los dominios Multi-AZ con modo de espera, solo puede realizar una solicitud de cambio a la vez. Si ya hay un cambio en curso, se rechazará la nueva solicitud. Puede comprobar el estado del cambio actual con la API de la `DescribeDomainChangeProgress`.

Cambios que no suelen causar implementaciones azul/verde

En la mayoría de los casos, las siguientes operaciones no provocan implementaciones azul/verde:

- Cambio de la política de acceso
- Modificación del punto de conexión personalizado
- Cambio de la política de seguridad de la capa de transporte (TLS)
- Cambio de la hora de instantánea automatizada
- Habilitar o deshabilitar Require HTTPS
- Activación de Auto-Tune o desactivación sin revertir sus cambios
- Si su dominio tiene nodos maestros dedicados o un número de UltraWarm nodos variable
- Cambiar el recuento de nodos de datos
- Si su dominio tiene nodos maestros dedicados, cambie el tipo de instancia maestra dedicada o el número de nodos (excepto en el caso de los dominios con dos nodos maestros dedicados y el reconocimiento de zona activado)
- Habilitar o deshabilitar la publicación de registros de errores o registros lentos en CloudWatch
- Deshabilitar la publicación de los registros de auditoría en. CloudWatch

- Aumentar el tamaño del volumen, cambiar el tipo de volumen, las IOPS y el rendimiento hasta un máximo de 3 TiB por tamaño de volumen de nodo de datos
- Cómo agregar y eliminar etiquetas

> **Note**
>
> Existen algunas excepciones en función de la versión del software de servicio. Si quieres estar absolutamente seguro de que un cambio no provocará una implementación azul/verde, realiza una prueba antes de actualizar tu dominio, si esta opción está disponible. Algunos cambios no ofrecen la opción de ejecución en seco. Por lo general, recomendamos realizar cambios en el clúster fuera de las horas de mayor tráfico.

Cómo determinar si un cambio provocará una implementación azul/verde

Puede probar algunos tipos de cambios de configuración planificados para determinar si provocarán una implementación azul o verde, sin tener que comprometerse con esos cambios. Antes de iniciar un cambio de configuración, utilice la consola o una de API para realizar una comprobación de validación con el fin de asegurarse de que el dominio sea apto para una actualización.

Console

Para validar un cambio de configuración

1. Ve a la consola OpenSearch de Amazon Service enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios.
3. Seleccione el dominio para el que desee realizar un cambio de configuración. Se abrirá la página de detalles del dominio. Seleccione el menú desplegable Acciones y, a continuación, Editar configuración del clúster.
4. En la página Editar configuración del clúster, puede realizar cambios en el tipo de instancia, el número de nodos y cualquier otra configuración. Cuando haya confirmado los cambios en el panel de resumen, seleccione Ejecutar.
5. Una vez que haya finalizado la ejecución de prueba, los resultados aparecerán automáticamente en la parte inferior de la página, junto con un ID de ejecución de prueba. Estos resultados indican a qué categoría pertenece el cambio:

    - Inicia una implementación azul/verde

- No requiere una implementación azul/verde
- Contiene errores de validación que se deben corregir para poder guardar los cambios

Tenga en cuenta que cada ejecución de prueba sobrescribe la anterior. Para consultar los detalles de cada ejecución de prueba posteriormente, asegúrese de guardar el ID de la ejecución de prueba. Cada ejecución de prueba está disponible durante 90 días o hasta que se realice una actualización de la configuración.

6. Para proceder con la actualización de la configuración, seleccione Guardar cambios. De lo contrario, seleccione Cancelar. Cualquiera de las opciones lo lleva de vuelta a pestaña Configuración del clúster. En esta pestaña, se puede seleccionar Detalles de la ejecución de prueba para ver los detalles de la última ejecución de prueba. Esta página también incluye una side-by-side comparación entre la configuración previa al simulacro y la configuración del simulacro.

API

Puede realizar una validación mediante una ejecución de prueba a través de la API de configuración. Para probar los cambios con la API, establezca `DryRun` en `true`, y `DryRunMode` en `Verbose`. El modo detallado ejecuta una comprobación de validación además de determinar si el cambio iniciará una implementación azul/verde. Por ejemplo, esta UpdateDomainConfigsolicitud prueba el tipo de implementación que resulta de habilitar UltraWarm:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
config
{
   "ClusterConfig": {
    "WarmCount": 3,
    "WarmEnabled": true,
    "WarmType": "ultrawarm1.large.search"
   },
   "DryRun": true,
   "DryRunMode": "Verbose"
}
```

La solicitud ejecuta una comprobación de validación y devuelve el tipo de implementación que provocará el cambio, pero no lleva a cabo la actualización:

```
{
   "ClusterConfig": {
     ...
    },
   "DryRunResults": {
      "DeploymentType": "Blue/Green",
      "Message": "This change will require a blue/green deployment."
    }
}
```

Los tipos de implementación posibles son:

- `Blue/Green`: el cambio provocará una implementación azul/verde.
- `DynamicUpdate`: el cambio no provocará una implementación azul/verde.
- `Undetermined`: el dominio sigue en estado de procesamiento, por lo que no se puede determinar el tipo de implementación.
- `None`: sin cambio en la configuración.

Si la validación falla, devuelve una lista de errores de validación.

```
{
   "ClusterConfig":{
      "..."
   },
   "DryRunProgressStatus":{
      "CreationDate":"2023-01-12T01:14:33.847Z",
      "DryRunId":"db00ca39-48b2-4774-bbd3-252cf094d205",
      "DryRunStatus":"failed",
      "UpdateDate":"2023-01-12T01:14:33.847Z",
      "ValidationFailures":[
         {
            "Code":"Cluster.Index.WriteBlock",
            "Message":"Cluster has index write blocks."
         }
      ]
   }
}
```

Si el estado es fijo`pending`, puedes usar el ID de prueba en tu UpdateDomainConfig respuesta en DescribeDryRunProgressllamadas posteriores para comprobar el estado de la validación.

```
GET https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/
dryRun?dryRunId=my-dry-run-id
{
    "DryRunConfig": null,
    "DryRunProgressStatus": {
        "CreationDate": "2023-01-12T01:14:42.998Z",
        "DryRunId": "db00ca39-48b2-4774-bbd3-252cf094d205",
        "DryRunStatus": "succeeded",
        "UpdateDate": "2023-01-12T01:14:49.334Z",
        "ValidationFailures": null
    },
    "DryRunResults": {
        "DeploymentType": "Blue/Green",
        "Message": "This change will require a blue/green deployment."
    }
}
```

Para realizar un análisis de ejecución de prueba sin una comprobación de validación, establezca `DryRunMode` en`Basic` cuando utilice la API de configuración.

Python

El siguiente código de Python usa la UpdateDomainConfigAPI para realizar una comprobación de validación de ejecución en seco y, si la comprobación se realiza correctamente, llama a la misma API sin una ejecución en seco para iniciar la actualización. Si la comprobación no se realiza correctamente, el script imprime el error y se detiene.

```
import time
import boto3

client = boto3.client('opensearch')

response = client.UpdateDomainConfig(
    ClusterConfig={
        'WarmCount': 3,
        'WarmEnabled': True,
        'WarmCount': 123,
    },
    DomainName='test-domain',
    DryRun=True,
    DryRunMode='Verbose'
)
```

```
dry_run_id = response.DryRunProgressStatus.DryRunId

retry_count = 0

while True:

    if retry_count == 5:
        print('An error occured')
        break

    dry_run_progress_response = client.DescribeDryRunProgress('test-domain',
 dry_run_id)
    dry_run_status = dry_run_progress_response.DryRunProgressStatus.DryRunStatus

    if dry_run_status == 'succeeded':
        client.UpdateDomainConfig(
            ClusterConfig={
            'WarmCount': 3,
            'WarmEnabled': True,
            'WarmCount': 123,
        })
        break

    elif dry_run_status == 'failed':
        validation_failures_list =
 dry_run_progress_response.DryRunProgressStatus.ValidationFailures
        for item in validation_failures_list:
            print(f"Code: {item['Code']}, Message: {item['Message']}")
        break

    retry_count += 1
    time.sleep(30)
```

Iniciar y realizar un seguimiento de un cambio de configuración

> **Note**
>
> Puede solicitar un cambio de configuración a la vez. También puede agrupar varios cambios de configuración en una sola solicitud. Espere a que se modifique el estado de su dominio `Active` antes de solicitar cualquier cambio de configuración adicional.

Puedes ver los campos Domain Processing Status y Config Change Status en la consola de Amazon OpenSearch Service para realizar un seguimiento de los cambios en el dominio y la configuración. También puedes realizar un seguimiento de los cambios en el dominio y la configuración mediante `ConfigChangeStatus` los parámetros `DomainProcessingStatus` y de las respuestas de la API. Para obtener más información, consulta el tipo de DomainStatusdatos en la referencia de la API de OpenSearch servicio.

Visibilidad del estado de procesamiento del dominio: puede determinar fácilmente el estado de configuración de un dominio consultando el campo Estado de procesamiento del dominio de la consola. Del mismo modo, el parámetro de la `DomainProcessingStatus` API se puede utilizar para identificar el estado. Los siguientes valores son estados de procesamiento de un dominio:

- `Active`: No hay ningún cambio de configuración en curso. Puede enviar una nueva solicitud de cambio de configuración.
- `Creating`: Se está creando el dominio.
- `Modifying`: Se están realizando cambios de configuración, como la adición de nuevos nodos de datos, EBS, gp3, el aprovisionamiento de IOPS o la configuración de claves de KMS.

> **Note**
>
> Es posible que vea el estado `Modifying` en situaciones en las que un dominio requiere el movimiento de un fragmento para completar los cambios de configuración. Para garantizar la compatibilidad con versiones anteriores, el comportamiento del `Processing` parámetro se mantiene sin cambios en las respuestas de la API y se establece en falso tan pronto como se completan los cambios en la configuración principal, sin esperar a que se complete el movimiento del fragmento.

- `Upgrading Engine Version`: Se está actualizando la versión del motor.
- `Updating Service Software`: Hay una actualización del software de servicio en curso.
- `Deleting`: Se está eliminando el dominio.
- `Isolated`: El dominio está suspendido.

Visibilidad del estado de la configuración: los cambios de configuración los puede iniciar el operador (por ejemplo, la adición de un nuevo nodo de datos o el cambio de tipo de instancia) o el servicio (por ejemplo, el ajuste automático y las actualizaciones fuera de las horas de mayor actividad). Puedes encontrar el estado de los últimos detalles del cambio de configuración en el campo Estado

del cambio de configuración de la consola de Amazon OpenSearch Service y en la respuesta de la `ConfigChangeStatus` API. Los siguientes valores indican el estado de la configuración de un dominio:

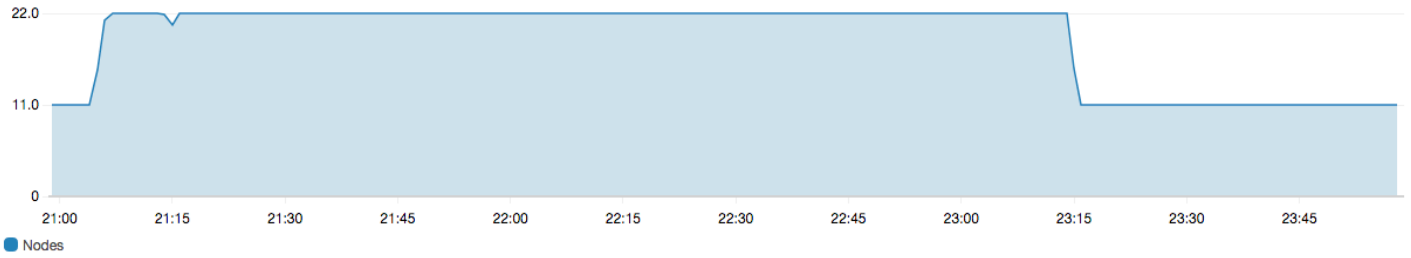
- `Pending`: Se ha enviado una solicitud de cambio de configuración.
- `Initializing`: El servicio está inicializando una solicitud de cambio de configuración.
- `Validating`: El servicio está validando los cambios solicitados y los recursos necesarios.
- `Awaiting user inputs`: Se aplica cuando el operador espera que algunos cambios de configuración, como el cambio de tipo de instancia, continúen realizándose. Puede editar los cambios de configuración.
- `Applying changes`: El servicio está aplicando los cambios de configuración solicitados.
- `Cancelled`: El cambio de configuración está cancelado. Si recibe el estado de error en la validación, puede hacer clic en Cancelar en la consola o llamar a la operación de la `CancelDomainConfigChange` API. Si lo hace, se revertirán todos los cambios aplicados.
- `Completed`: Los cambios de configuración solicitados se han realizado correctamente.
- `Validation Failed`: Los cambios solicitados no se validaron. No se aplica ningún cambio de configuración.

> **Note**
>
> Los errores de validación pueden deberse a la presencia de índices rojos en el dominio, a la falta de disponibilidad del tipo de instancia elegido o a la falta de espacio en disco. Para obtener una lista de los errores de validación, consulte. the section called “Solución de errores de validación” Durante un fallo de validación, puede cancelar, volver a intentar o editar los cambios de configuración.

Resumen de la API: puede usar las operaciones `DescribeDomainDescribeDomainChangeProgress`, y la `DescribeDomainConfig` API para obtener estados detallados de las actualizaciones de la configuración. Además, puede utilizarlas `CancelDomainConfigChange` para cancelar las actualizaciones en caso de que se produzcan errores en la validación. Para obtener más información, consulta la documentación de la API de OpenSearch servicio

Cuando se completen los cambios de configuración, el estado del dominio volverá a ser. `Active`

Puedes revisar el estado del clúster y CloudWatch las métricas de Amazon y comprobar que el número de nodos del clúster aumenta temporalmente (a menudo se duplica) mientras se actualiza el dominio. En la siguiente ilustración, puede ver el número de nodos duplicarse de 11 a 22 durante un cambio de configuración y volver a 11 una vez completada la actualización.



Este duplicado provisional puede afectar al desempeño de los nodos maestros dedicados del clúster, que repentinamente podría tener que administrar más nodos. También puede aumentar las latencias de búsqueda e indexación a medida que OpenSearch Service copia los datos del clúster antiguo al nuevo. Es importante mantener una capacidad suficiente en el clúster para administrar la sobrecarga asociada a estas implementaciones azul/verde.

> **Important**
>
> El usuario no incurrirá en ningún gasto adicional durante los cambios de configuración y el mantenimiento del servicio. Solo se facturará por el número de nodos que solicite para el clúster. Para obtener información detallada, consulte the section called “Cargos por los cambios de configuración”.

Para evitar sobrecargar los nodos maestros dedicados, puedes monitorear el uso con las CloudWatch métricas de Amazon. Para conocer los valores máximos recomendados, consulte the section called “ CloudWatch Alarmas recomendadas”.

Etapas de un cambio de configuración

Tras iniciar un cambio de configuración, OpenSearch Service sigue una serie de pasos para actualizar tu dominio. Puedes ver el progreso del cambio de configuración en el estado del cambio de configuración de la consola. Los pasos exactos por los que se realiza una actualización dependen del tipo de cambio que realices. También puede supervisar un cambio de configuración mediante la operación de la DescribeDomainChangeProgressAPI.

Las siguientes son las posibles etapas que puede realizar una actualización durante un cambio de configuración:

Nombre de la fase	Descripción
Validación	Validación de que el dominio es apto para una actualización y mostrar problemas de validación si es necesario.
Creación de un nuevo entorno	Completar los requisitos previos necesarios y crear los recursos necesarios para iniciar la implementación azul-verde.
Provisión de nuevos nodos	Creación de un nuevo conjunto de instancias en el nuevo entorno.
Enrutamiento del tráfico en nodos nuevos	Redireccionamiento del tráfico a los nodos de

Nombre de la fase	Descripción
	datos recién creados.
Enrutamiento del tráfico en nodos antiguos	Desactivación del tráfico en los nodos de datos antiguos.
Preparación de los nodos para su eliminación	Preparación para eliminar nodos. Este paso solo ocurre cuando estás reduciendo la escala de su dominio (por ejemplo, de 8 a 6 nodos).
Copia de particiones en nodos nuevos	Trasladando los fragmentos de los nodos antiguos a los nuevos.
Terminación de nodos	Finalización y eliminación de nodos antiguos después de remover los fragmentos.

Nombre de la fase	Descripción
Eliminación de recursos más antiguos	Eliminación de recursos asociados al entorno anterior (por ejemplo, equilibrador de carga).
Actualización dinámica	Se muestra cuando la actualización no requiere una implementación azul-verde y se puede aplicar dinámicamente.
Aplicación de cambios específicos relacionados con la instancia maestra	Se muestra cuando se cambia el tipo o el número de la instancia maestra dedicada.

Nombre de la fase	Descripción
Aplicación de cambios relacionados con el volumen	Se muestra cuando se modifican el tamaño, el tipo, las IOPS y el rendimiento del volumen.

Cargos por los cambios de configuración

Si cambias la configuración de un dominio, OpenSearch Service crea un nuevo clúster tal y como se describe enthe section called “Cambios de configuración”. Durante la migración de uno a otro, se devengarán los cargos siguientes:

- Si cambia el tipo de instancia, se cobrará por los dos clústeres durante la primera hora. Después de la primera hora, solo se cobrará por el clúster nuevo. Los volúmenes de EBS no se cobran dos veces porque forman parte del clúster, por lo que la facturación corresponde a la facturación de instancias.

  Ejemplo: Supongamos que cambia la configuración y pasa de tres instancias `m3.xlarge` a cuatro instancias `m4.large`. Durante la primera hora, se cobrarán los dos clústeres (3* `m3.xlarge` + 4* `m4.large`). Después de la primera hora, solo se cobrará el clúster nuevo (4 * `m4.large`).
- Si no cambia el tipo de instancia, solo se cobrará el clúster mayor durante la primera hora. Después de la primera hora, solo se cobrará por el clúster nuevo.

  Ejemplo: Supongamos que cambia la configuración y pasa de seis instancias `m3.xlarge` a tres instancias `m3.xlarge`. Durante la primera hora, se cobrará por el clúster mayor (6 * `m3.xlarge`). Después de la primera hora, solo se cobrará el clúster nuevo (3 * `m3.xlarge`).

Solución de errores de validación

Cuando inicias un cambio de configuración o realizas una actualización de una versión OpenSearch o de Elasticsearch, OpenSearch Service primero realiza una serie de comprobaciones de validación

para garantizar que tu dominio sea apto para una actualización. Si se produce un error en alguna de estas comprobaciones, recibirá una notificación en la consola con los problemas específicos que debe corregir antes de actualizar su dominio. En la siguiente tabla se enumeran los posibles problemas de dominio que pueden surgir en el OpenSearch servicio y los pasos para resolverlos.

Problema	Código de error	Pasos para la solución de problemas
No se encontró el grupo de seguridad	`SecurityGroupNotFound`	El grupo de seguridad asociado a su dominio de OpenSearch servicio no existe. Para solucionar este problema, cree un grupo de seguridad con el nombre especificado.
No se encontró la subred	`SubnetNotFound`	La subred asociada a su dominio OpenSearch de servicio no existe. Para solucionar este problema, cree una subred en la VPC.
No se configuró el rol vinculado al servicio	`SLRNotConfigured`	La función vinculada al servicio para el OpenSearch Servicio no está configurada. El rol vinculado al servicio está predefinido por el OpenSearch Servicio e incluye todos los permisos que el servicio necesita para llamar a otros AWS servicios en su nombre. Si el rol no existe, es posible que tenga que crearlo manualmente.
No hay suficientes direcciones IP	`InsufficientFreeIPsForSubnets`	Una o más de las subredes de VPC no tienen suficientes direcciones IP para actualizar el dominio. Para calcular el número de direcciones IP que necesita, consulte the section called “Reserva de direcciones IP en una subred de una VPC”.
No existe el grupo de usuarios de Cognito	`CognitoUserPoolNotFound`	OpenSearch El servicio no encuentra el grupo de usuarios de Amazon Cognito. Verifique que creó uno y que tiene el ID correcto. Para encontrar el ID, puede utilizar la consola de Amazon Cognito o el siguiente comando de la AWS CLI : `aws cognito-idp list-user-pools --max-results 60 --region us-east-1`
El grupo de	`CognitoIdentityPoo`	OpenSearch El servicio no encuentra el grupo de identidades de Cognito. Verifique que creó uno y que tiene el ID correcto. Para

Problema	Código de error	Pasos para la solución de problemas
identidades de Cognito no existe	`lNotFound`	encontrar el ID, puede utilizar la consola de Amazon Cognito o el siguiente comando de la AWS CLI : `aws cognito-identity list-identity-pools --max-results 60 --region us-east-1`
No se encontró el dominio de Cognito para el grupo de usuarios	`CognitoDomainNotFound`	El grupo de usuarios no tiene un nombre de dominio. Puede configurar uno mediante la consola de Amazon Cognito o el siguiente comando: AWS CLI `aws cognito-idp create-user-pool-domain --domain my-domain --user-pool-id id`
No se configuró el rol de Cognito	`CognitoRoleNotConfigured`	La función de IAM que concede al OpenSearch Servicio el permiso para configurar los grupos de usuarios e identidades de Amazon Cognito y utilizarlos para la autenticación no está configurada. Configure el rol con un conjunto de permisos y una relación de confianza adecuados. Puede usar la consola, que crea el CognitoAccessForAmazonOpenSearchrol predeterminado para usted, o puede configurar un rol manualmente mediante el SDK AWS CLI o el AWS mismo.
No se puede describir el grupo de usuarios	`UserPoolNotDescribable`	El rol de Amazon Cognito especificado no tiene permiso para describir el grupo de usuarios asociado a su dominio. Asegúrese de que la política de permisos de rol permita la acción `cognito-identity:DescribeUserPool` . Consulte the section called “Acerca del rol CognitoAccessForAmazonOpenSearch” para ver la política de permisos completa.

Problema	Código de error	Pasos para la solución de problemas
No se puede describir el grupo de identidades	`IdentityPoolNotDescribable`	El rol de Amazon Cognito especificado no tiene permiso para describir el grupo de identidades asociado a su dominio. Asegúrese de que la política de permisos de rol permita la acción `cognito-identity:DescribeIdentityPool`. Consulte the section called “Acerca del rol CognitoAccessForAmazonOpenSearch” para ver la política de permisos completa.
No se pueden describir los grupos de usuarios y de identidades	`CognitoPoolsNotDescribable`	El rol de Amazon Cognito especificado no tiene permiso para describir los grupos de usuarios e identidades asociados a su dominio. Asegúrese de que la política de permisos de rol permita las acciones `cognito-identity:DescribeIdentityPool` y `cognito-identity:DescribeUserPool`. Consulte the section called “Acerca del rol CognitoAccessForAmazonOpenSearch” para ver la política de permisos completa.
La clave de KMS no está habilitada	`KMSKeyNotEnabled`	La clave AWS Key Management Service (AWS KMS) utilizada para cifrar tu dominio está deshabilitada. Vuelva a habilitar la clave inmediatamente.
El estado del certificado personalizado no es ISSUED (EMITIDO)	`InvalidCertificate`	Si tu dominio usa un punto final personalizado, lo proteges generando un certificado SSL en AWS Certificate Manager (ACM) o importando uno propio. El estado del certificado debe ser Emitido. Si aparece este error, compruebe el estado del certificado en la consola de ACM. Si el estado aparece como Expired (Vencido), Failed (Error), Inactive (Inactivo) o Pending validation (Pendiente de validación), consulte la documentación sobre solución de problemas de ACM para solucionar el problema.

Problema	Código de error	Pasos para la solución de problemas
No hay capacidad suficiente para lanzar el tipo de instancia elegido	`InsufficientInstanceCapacity`	La capacidad del tipo de instancia solicitada no está disponible. Por ejemplo, es posible que hayas solicitado cinco `i3.16xlarge.search` nodos, pero el OpenSearch Servicio no tiene suficientes `i3.16xlarge.search` hosts disponibles, por lo que no se puede tramitar la solicitud. Comprueba los tipos de instancia compatibles en OpenSearch Service y elige otro tipo de instancia.
Índices rojos en clúster	`RedCluster`	Uno o más índices del clúster tienen un estado rojo, lo que lleva a un estado rojo general del clúster. Para solucionar este problema, consulte the section called “Estado rojo del clúster”.
Interruptor de circuitos de memoria, demasiadas solicitudes	`TooManyRequests`	Hay demasiadas solicitudes de búsqueda y escritura en tu dominio, por lo que OpenSearch Service no puede actualizar su configuración. Puede reducir la cantidad de solicitudes, escalar las instancias verticalmente hasta 64 GiB de RAM o escalar horizontalmente mediante la adición de instancias.
La nueva configuración no puede almacenar datos (poco espacio en disco)	`InsufficientStorageCapacity`	El tamaño de almacenamiento configurado no puede contener todos los datos de su dominio. Para solucionar este problema, elija un volumen mayor, elimine los índices que no se utilizan o aumente la cantidad de nodos del clúster para liberar espacio en el disco de inmediato.

Problema	Código de error	Pasos para la solución de problemas

Particiones ancladas a nodos específicos	`ShardMovementBlocked`	Uno o más índices de su dominio están adjuntos a nodos específicos y no se pueden reasignar. Lo más probable es que esto suceda porque se configuró el filtrado de asignación de particiones, que le permite especificar qué nodos tienen permiso para alojar las particiones de un índice en particular.
		
		Para solucionar este problema, elimine los filtros de asignación de particiones de todos los índices afectados:
		
		`PUT my-index/_settings`
		`{`
		`  "settings": {`
		`  "index.routing.allocation.require._name": null`
		`  }`
		`}`

La nueva configuración no puede contener todas las particiones (recuento de particiones)	`TooManyShards`	El número de fragmentos de tu dominio es demasiado alto, lo que impide que OpenSearch Service los traslade a la nueva configuración. Para solucionar este problema, escale su dominio horizontalmente. Para ello, agregue nodos del mismo tipo de configuración que los nodos actuales del clúster. Tenga en cuenta que el tamaño máximo de volumen de EBS depende del tipo de instancia del nodo. Para evitar este problema en el futuro, consulte the section called “Selección del número de particiones” y defina una estrategia de partición que sea adecuada para su caso de uso.
La subred asociada al dominio no admite direcciones IPv4	`ResultCodeIPv4BlockNotExists`	Para resolver este problema, cree una subred o actualice la subred existente en la VPC según el tipo de dirección IP configurada del dominio. Si su dominio usa un tipo de dirección únicamente para IPv4, use una subred solo para IPv4. Si su dominio usa el modo de doble pila, use una subred de doble pila.

Problema	Código de error	Pasos para la solución de problemas
La subred asociada al dominio no admite direcciones IPv6	`ResultCodeIPv6BlockNotExists`	Para resolver este problema, cree una subred o actualice la subred existente en la VPC según el tipo de dirección IP configurada del dominio. Si su dominio usa un tipo de dirección únicamente para IPv4, use una subred solo para IPv4. Si su dominio usa el modo de doble pila, use una subred de doble pila.

Actualizaciones de software de servicio en Amazon OpenSearch Service

> **Note**
>
> Para obtener una explicación de los cambios y adiciones realizados en cada actualización del software de servicio principal (sin parches), consulte las notas de la versión.

Amazon OpenSearch Service publica periódicamente actualizaciones de software de servicio que añaden funciones o mejoran tus dominios. El panel Notificaciones en la consola es la forma más sencilla para ver si hay disponible una actualización o para verificar el estado de una actualización. Cada notificación incluye detalles sobre la actualización del software del servicio. Todas las actualizaciones de software utilizan implementaciones azul/verde para minimizar el tiempo de inactividad.

Las actualizaciones del software del servicio son diferentes de las actualizaciones de las OpenSearch versiones. Para obtener información sobre la actualización a una versión posterior de OpenSearch, consultethe section called “Actualización de dominios”.

Temas

- Actualizaciones opcionales frente a actualizaciones obligatorias
- Actualizaciones de revisión
- Consideraciones
- Iniciar una actualización del software de servicio

- Programación de actualizaciones del software durante las ventanas de menor actividad
- Supervisar actualizaciones de software de servicio
- Cuando los dominios no son aptos para una actualización

Actualizaciones opcionales frente a actualizaciones obligatorias

OpenSearch El servicio tiene dos categorías amplias de actualizaciones de software de servicio:

Actualizaciones opcionales

Las actualizaciones del software de servicio opcionales generalmente incluyen mejoras y soporte para nuevas características o funcionalidades. Las actualizaciones opcionales no se aplican a sus dominios y no hay un plazo fijo para instalarlas. La disponibilidad de la actualización se comunica por correo electrónico y una notificación en la consola. Puede optar por aplicar la actualización inmediatamente o reprogramarla para una fecha y hora más adecuadas. También puede programarla durante la ventana de menor actividad del dominio. La mayoría de las actualizaciones de software son opcionales.

Independientemente de si programa o no una actualización, si realiza un cambio en el dominio que provoque una implementación azul/verde, OpenSearch Service actualizará automáticamente el software del servicio por usted.

Puede configurar su dominio para que aplique automáticamente las actualizaciones opcionales durante la ventana de menor actividad. Cuando esta opción está activada, el OpenSearch Servicio espera al menos 13 días desde que esté disponible una actualización opcional y, a continuación, programa la actualización después de 72 horas (tres días). Recibirá una notificación en la consola cuando la actualización esté programada y podrá elegir reprogramarla para una fecha posterior.

Para activar las actualizaciones de software automáticas, seleccione Habilitar la actualización automática de software al crear o actualizar su dominio. Para configurar el mismo ajuste mediante el AWS CLI, `--software-update-options true` establézcalo al crear o actualizar el dominio.

Actualizaciones requeridas

Las actualizaciones de software de servicio requeridas suelen incluir correcciones de seguridad críticas u otras actualizaciones obligatorias para garantizar la integridad y la funcionalidad continuas de su dominio. Algunos ejemplos de actualizaciones requeridas son las vulnerabilidades y

exposiciones comunes (CVE) de Log4j y la aplicación de Servicio de metadatos de instancia Versión 2 (IMDSv2). El número de actualizaciones obligatorias en un año suele ser inferior a tres.

OpenSearch El servicio programa automáticamente estas actualizaciones y te lo notifica 72 horas (tres días) antes de la actualización programada por correo electrónico y una notificación de consola. Puede optar por aplicar la actualización inmediatamente o reprogramarla para una fecha y hora más adecuadas dentro del plazo permitido. También puede programarla durante la próxima ventana de menor actividad del dominio. Si no realizas ninguna acción en relación con una actualización obligatoria y no realizas ningún cambio en el dominio que provoque una implementación azul o verde, el OpenSearch Servicio puede iniciar la actualización en cualquier momento después de la fecha límite especificada (normalmente 14 días a partir de la disponibilidad), dentro del período de menor actividad del dominio.

Independientemente de cuándo esté programada la actualización, si realizas un cambio en el dominio que provoque un despliegue azul/verde, OpenSearch Service actualizará tu dominio automáticamente.

Actualizaciones de revisión

Las versiones de software de servicio que terminan en “-P” y un número, como R20211203-*P4*, son versiones de revisión. Es probable que las revisiones incluyan mejoras de rendimiento, correcciones de errores menores y correcciones de seguridad o mejoras de posición. Las versiones de revisión no incluyen nuevas características ni cambios extraordinarios y, por lo general, no tienen un impacto directo o notable en los usuarios. La notificación del software de servicio le indica si el lanzamiento de una revisión es opcional u obligatoria.

Consideraciones

Tenga en cuenta lo siguiente cuando tenga que tomar una decisión sobre la actualización del dominio:

- La actualización manual del dominio permite aprovechar las nuevas características de forma más rápida. Si eliges Actualizar, el OpenSearch Servicio coloca la solicitud en una cola y comienza la actualización cuando tiene tiempo.
- Al iniciar una actualización del software del servicio, el OpenSearch Servicio envía una notificación cuando se inicia la actualización y cuando se completa.
- Las actualizaciones de software utilizan implementaciones azul/verde para minimizar el tiempo de inactividad. Las actualizaciones pueden sobrecargar temporalmente los nodos maestros dedicados

de un clúster, así que asegúrese de mantener la capacidad suficiente para manejar la sobrecarga asociada.

- Normalmente, las actualizaciones se completan en cuestión de minutos, pero también pueden tardar varias horas o incluso días si el sistema experimenta una carga pesada. Considere actualizar el dominio durante la ventana de menor actividad configurada para evitar largos periodos de actualización.

Iniciar una actualización del software de servicio

Puede solicitar una actualización del software del servicio a través de la consola de OpenSearch servicio AWS CLI, el SDK o uno de los SDK.

Consola

Cómo solicitar una actualización del software de servicio

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre de dominio para abrir su configuración.
3. Seleccione Acciones, Actualizar y seleccione una de las siguientes opciones:

   - Aplicar la actualización ahora: programa de inmediato la acción para que se lleve a cabo en la hora actual si hay capacidad disponible. Si no hay capacidad disponible, ofrecemos otras franjas horarias disponibles para elegir.
   - Programarla en una ventana de menor actividad: solo está disponible si la ventana de menor actividad está activada para el dominio. Programa la actualización para que se lleve a cabo durante la ventana de menor actividad configurada en el dominio. No hay garantía de que la actualización se produzca durante la siguiente ventana inmediata. Dependiendo de la capacidad, podría producirse en los días siguientes. Para obtener más información, consulte the section called “Intervalos de menor demanda”.
   - Programar para una fecha y hora específicas: programa la actualización para que se lleve a cabo en una fecha y hora específicas. Si la hora que especifica no está disponible por motivos de capacidad, puede seleccionar una franja horaria diferente.

   Si programa la actualización para una fecha posterior (dentro o fuera de la ventana de menor actividad del dominio), puede reprogramarla en cualquier momento. Para ver instrucciones, consulte the section called “Reprogramar acciones”.

4. Seleccione Confirmar.

AWS CLI

Envía una start-service-software-update AWS CLI solicitud para iniciar una actualización del software del servicio. En este ejemplo, se añade la actualización a la cola de forma inmediata:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "NOW"
```

Respuesta:

```
{
    "ServiceSoftwareOptions": {
        "CurrentVersion": "R20220928-P1",
        "NewVersion": "R20220928-P2",
        "UpdateAvailable": true,
        "Cancellable": true,
        "UpdateStatus": "PENDING_UPDATE",
        "Description": "",
        "AutomatedUpdateDate": "1969-12-31T16:00:00-08:00",
        "OptionalDeployment": true
    }
}
```

> **Tip**
>
> Después de solicitar una actualización, dispone de una pequeña ventana de tiempo para cancelarla. La duración de este `PENDING_UPDATE` estado puede variar considerablemente y depende de usted Región de AWS y del número de actualizaciones simultáneas que realice el OpenSearch Servicio. Para cancelar una actualización, usa la consola o el `cancel-service-software-update` AWS CLI comando.

Si la solicitud falla con una `BaseException`, eso significa que la hora que especificó no está disponible por motivos de capacidad y debe especificar una hora diferente. OpenSearch El servicio proporciona sugerencias alternativas de ranuras disponibles en la respuesta.

AWS SDK

Este ejemplo de script de Python utiliza los métodos describe_domain y start_service_software_update de AWS SDK for Python (Boto3) para comprobar si un dominio es apto para una actualización de software de servicio y, de ser así, inicia la actualización. Se debe proporcionar un valor para `domain_name`.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)

domain_name = ''  # The name of the domain to check and update

client = boto3.client('opensearch', config=my_config)


def getUpdateStatus(client):
    """Determines whether the domain is eligible for an update"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    sso = response['DomainStatus']['ServiceSoftwareOptions']
    if sso['UpdateStatus'] == 'ELIGIBLE':
        print('Domain [' + domain_name + '] is eligible for a service software update
 from version ' +
              sso['CurrentVersion'] + ' to version ' + sso['NewVersion'])
        updateDomain(client)
    else:
        print('Domain is not eligible for an update at this time.')


def updateDomain(client):
    """Starts a service software update for the eligible domain"""
    response = client.start_service_software_update(
```

```
        DomainName=domain_name
    )
    print('Updating domain [' + domain_name + '] to version ' +
          response['ServiceSoftwareOptions']['NewVersion'] + '...')
    waitForUpdate(client)


def waitForUpdate(client):
    """Waits for the domain to finish updating"""
    response = client.describe_domain(
        DomainName=domain_name
    )
    status = response['DomainStatus']['ServiceSoftwareOptions']['UpdateStatus']
    if status == 'PENDING_UPDATE' or status == 'IN_PROGRESS':
        time.sleep(30)
        waitForUpdate(client)
    elif status == 'COMPLETED':
        print('Domain [' + domain_name +
              '] successfully updated to the latest software version')
    else:
        print('Domain is not currently being updated.')

def main():
    getUpdateStatus(client)
```

Programación de actualizaciones del software durante las ventanas de menor actividad

Cada dominio OpenSearch de servicio creado después del 16 de febrero de 2023 tiene un período diario de 10 horas entre las 22:00 y las 8:00 a. m., hora local, que consideramos el período de menor actividad. OpenSearch El servicio usa esta ventana para programar las actualizaciones del software del servicio para el dominio. Las actualizaciones fuera de las horas pico ayudan a minimizar la carga de los nodos maestros dedicados de un clúster durante los períodos de mayor tráfico. OpenSearch El servicio no puede iniciar las actualizaciones fuera de este período de 10 horas sin su consentimiento.

- En el caso de las actualizaciones opcionales, el OpenSearch Servicio te notifica la disponibilidad de la actualización y te pide que la programes durante las próximas horas de menor actividad.
- En el caso de las actualizaciones necesarias, el OpenSearch Servicio programa automáticamente la actualización durante las próximas horas de menor actividad y te lo notifica con tres días de

antelación. Puede reprogramar la actualización (dentro o fuera de la ventana de menor actividad), pero solo dentro del plazo requerido para que se complete la actualización.

Para cada dominio, puede optar por anular la hora de inicio predeterminada a las 22:00 por una hora personalizada. Para ver instrucciones, consulte the section called “Configurar un intervalo de menor demanda personalizado”.

Consola

Cómo programar una actualización durante una próxima ventana de menor actividad

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre de dominio para abrir su configuración.
3. Seleccione Acciones, Actualizar.
4. Seleccione Programarla en la ventana de menor actividad.
5. Seleccione Confirmar.

Puede ver la acción programada en la pestaña de la ventana de menor actividad y reprogramarla en cualquier momento. Consulte the section called “Visualización de acciones programadas”.

CLI

Para programar una actualización durante una próxima temporada de menor actividad mediante el AWS CLI, envíe una StartServiceSoftwareUpdatesolicitud y especifique `OFF_PEAK_WINDOW` el `--schedule-at` parámetro:

```
aws opensearch start-service-software-update \
  --domain-name my-domain \
  --schedule-at "OFF_PEAK_WINDOW"
```

Supervisar actualizaciones de software de servicio

OpenSearch El servicio envía una notificación cuando una actualización del software del servicio está disponible, es necesaria, se ha iniciado, se ha completado o se ha producido un error. Puede ver estas notificaciones en el panel de notificaciones de la consola de OpenSearch servicio.
La gravedad de la notificación es `Informational` si la actualización es opcional y `High` si es necesaria.

OpenSearch El servicio también envía eventos de software de servicio a Amazon EventBridge. Puede utilizarlas EventBridge para configurar reglas que envíen un correo electrónico o realicen una acción específica cuando se recibe un evento. Para ver un tutorial de ejemplo, consulte the section called “Tutorial: Sending SNS alerts for available updates”.

Para ver el formato de cada evento de software de servicio enviado a Amazon EventBridge, consultathe section called “Eventos de actualización del software de servicio”.

Cuando los dominios no son aptos para una actualización

El dominio no es apto para una actualización del software de servicio si está en cualquiera de los estados que se muestran a continuación:

Estado	Descripción
Dominio en procesamiento	El dominio está en medio de un cambio de configuración. Compruebe si es posible optar a la actualización una vez que se complete la operación.
Estado rojo del clúster	Uno o varios índices en el clúster aparecen en rojo. Para ver los pasos de solución de problemas, consulte the section called “Estado rojo del clúster”.
Tasa de errores alta	El OpenSearch clúster devuelve una gran cantidad de errores de 5 xx al intentar procesar las solicitudes. Este problema suele ser el resultado de demasiadas solicitudes de lectura o escritura simultáneas. Considere la posibilidad de reducir el tráfico hacia el clúster o el escalado del dominio.
Cerebro dividido	El cerebro dividido significa que el OpenSearch clúster tiene más de un nodo maestro y se ha dividido en dos clústeres que nunca volverán a unirse por sí solos. Puede evitar un cerebro dividido con el número recomendado de nodos maestros dedicados. Para obtener ayuda a fin de recuperar un cerebro dividido, póngase en contacto con AWS Support.
Problema de integración de Amazon Cognito	Tu dominio usa la autenticación para los OpenSearch paneles y el OpenSearch Servicio no puede encontrar uno o más recursos de Amazon Cognito. Este problema suele producirse si no se encuentra el grupo de usuarios de Amazon Cognito. Para corregir el problema,

Estado	Descripción
	vuelva a crear el recurso que falta y configure el dominio del OpenSearch servicio para usarlo.
Otro problema de servicio	Los problemas relacionados con el propio OpenSearch Servicio pueden hacer que tu dominio aparezca como no apto para una actualización. Si en su dominio no se aplican ninguna de las condiciones anteriores y el problema persiste durante más de un día, póngase en contacto con AWS Support.

Definición de ventanas fuera de las horas pico para Amazon Service OpenSearch

Cuando creas un dominio de Amazon OpenSearch Service, defines un período diario de 10 horas que se considera horas de menor actividad. OpenSearch El servicio utiliza esta ventana para programar las actualizaciones del software del servicio y las optimizaciones de Auto-Tune que requieren una implementación azul/verde durante tiempos de tráfico comparativamente más bajos, siempre que sea posible. Azul/verde se refiere al proceso de crear un nuevo entorno para actualizaciones de dominio y redirigir a los usuarios al nuevo entorno una vez completadas dichas actualizaciones.

Si bien las implementaciones azul/verde no son disruptivas, para minimizar cualquier posible impacto en el rendimiento mientras se consumen los recursos de una implementación azul/verde, le recomendamos que programe estas implementaciones durante el intervalo de menor demanda configurada en el dominio. Las actualizaciones, como las sustituciones de nodos o las que deben implementarse en el dominio de forma inmediata, no utilizan el intervalo de menor demanda.

Puede modificar la hora de inicio del intervalo de menor demanda, pero no puede modificar la longitud del intervalo.

> **Note**
>
> Los intervalos de menor demanda se introdujeron el 16 de febrero de 2023. Todos los dominios creados antes de esta fecha tienen el intervalo de menor demanda desactivado de forma predeterminada. Debe habilitar y configurar manualmente el intervalo de menor demanda para estos dominios. Todos los dominios creados después de esta fecha tendrán

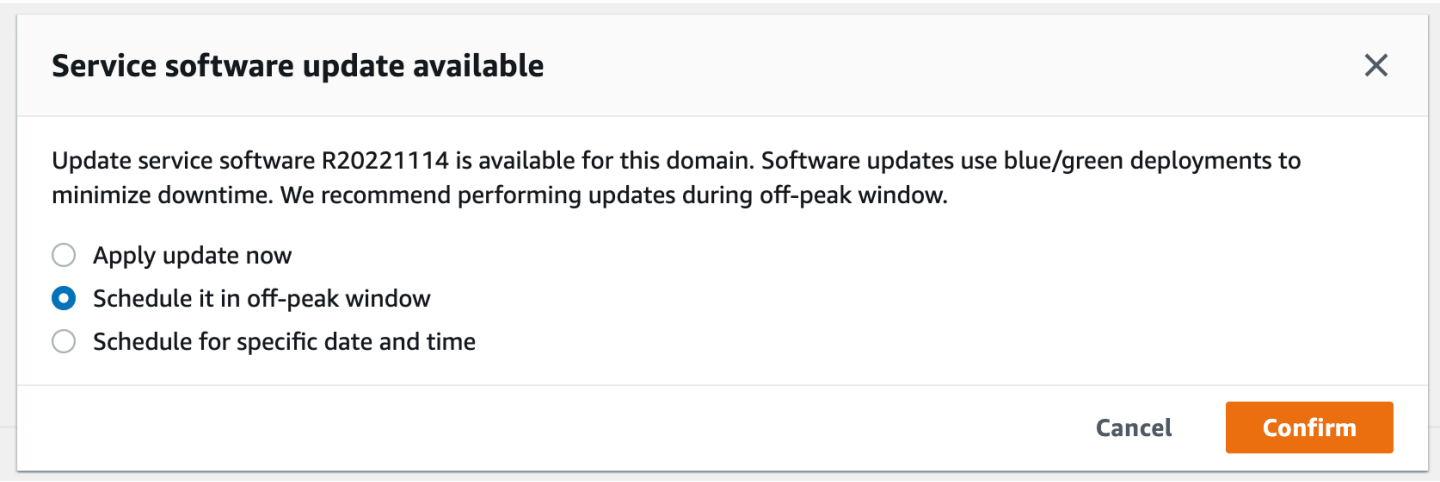
habilitado el intervalo de menor demanda de forma predeterminada. No puede deshabilitar el intervalo de menor demanda de un dominio una vez que esté habilitado.

Temas

Actualizaciones de software de servicio de menor demanda

OpenSearch El servicio tiene dos categorías amplias de actualizaciones de software de servicio: opcionales y obligatorias. Ambos tipos requieren implementaciones azul/verde. Las actualizaciones opcionales no se aplican en los dominios, mientras que las actualizaciones obligatorias se instalan automáticamente si no realiza ninguna acción antes de la fecha límite especificada (normalmente dos semanas después de la disponibilidad). Para más información, consulte the section called "Actualizaciones opcionales frente a actualizaciones obligatorias".

Cuando inicia una actualización opcional, tiene la opción de aplicarla inmediatamente, programarla para un intervalo de menor demanda posterior o especificar una fecha y hora personalizadas para aplicarla.



En el caso de las actualizaciones necesarias, el OpenSearch servicio programa automáticamente una fecha y una hora durante las horas de menor actividad para realizar la actualización. Recibe una notificación tres días antes de la actualización programada, y puede optar por reprogramarla para una fecha y hora posteriores dentro del intervalo de implementación obligatorio. Para ver las instrucciones, consulte the section called “Reprogramar acciones”.

Optimizaciones de ajuste automático durante horas de menor demanda

Anteriormente, el ajuste automático utilizaba intervalos de mantenimiento para programar los cambios que requerían una implementación azul/verde. Los dominios que ya tenían habilitados ajuste automático y los intervalos de mantenimiento antes de la introducción de los intervalos de menor demanda seguirán utilizando los intervalos de mantenimiento para estas actualizaciones, a menos que los migre para utilizar los intervalos de menor demanda.

Le recomendamos que migre sus dominios para utilizar el intervalo de menor demanda, ya que se utiliza para programar otras actividades en el dominio, como las actualizaciones del software de servicio. Para ver las instrucciones, consulte the section called “Migración desde los intervalos de mantenimiento de ajuste automático”. No puede volver a usar los intervalos de mantenimiento después de migrar su dominio a los intervalos de menor demanda.

Todos los dominios creados después del 16 de febrero de 2023 utilizarán el intervalo de menor demanda, en lugar de los intervalos de mantenimiento tradicionales, para programar las implementaciones azul/verde. No puede deshabilitar el intervalo de menor demanda de un dominio. Para ver una lista de las optimizaciones de ajuste automático que requieren implementaciones azul/verde, consulte the section called “Tipos de cambios”.

Habilitar el intervalo de menor demanda

Todos los dominios creados antes del 16 de febrero de 2023 (cuando se introdujeron los intervalos de menor demanda) tienen esa característica desactivada de forma predeterminada. Debe habilitarlo manualmente para estos dominios. No puede deshabilitar el intervalo de menor demanda después de activarlo.

Consola

Para habilitar el intervalo de menor demanda en un dominio

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre del dominio para abrir la configuración.

3. Acceda a la pestaña de intervalo de menor demanda y seleccione Editar.
4. Especifique una hora de inicio personalizada de acuerdo con la hora universal coordinad (UTC). Por ejemplo, para configurar una hora de inicio a las 23:30 en la región Oeste de EE. UU. (Oregón), especifique 07:30.
5. Elija Guardar cambios.

CLI

Para modificar la ventana de menor actividad mediante elAWS CLI, envíe una UpdateDomainConfigsolicitud:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'Enabled=true,
 OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Si no especifica una hora de inicio personalizada para el intervalo, el valor predeterminado es 00:00 UTC.

Configurar un intervalo de menor demanda personalizado

Debe especificar un intervalo de menor demanda personalizado para su dominio usando la hora universal coordinada (UTC). Por ejemplo, si desea que el intervalo de menor demanda comience a las 23:00 para un dominio en la región Este de EE. UU. (Norte de Virginia), debe especificar a las 04:00 UTC.

Consola

Para modificar el intervalo de horas de menor demanda de un dominio

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre del dominio para abrir la configuración.
3. Acceda a la pestaña del intervalo de menor demanda. Puede ver el intervalo de menor demanda configurado y una lista de las próximas acciones programadas para el dominio.
4. Seleccione Editar y especifique una nueva hora de inicio en UTC. Por ejemplo, para configurar la hora de inicio a las 21:00 en la región Este de EE. UU. (Norte de Virginia), especifique 02:00 UCT.

5. Elija Guardar cambios.

CLI

Para configurar una ventana personalizada fuera de las horas pico mediante elAWS CLI, envíe una UpdateDomainConfigsolicitud y especifique la hora y los minutos en formato horario de 24 horas.

Por ejemplo, la siguiente solicitud cambia la hora de inicio del intervalo a las 2:00 a. m. UTC:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --off-peak-window-options 'OffPeakWindow={WindowStartTime={Hours=02,Minutes=00}}'
```

Si no especifica la hora de inicio del intervalo, el valor predeterminado es las 10:00 p. m., hora local, para la Región de AWS en la que se crea el dominio.

Visualización de acciones programadas

Puede ver todas las acciones que están actualmente programadas, en curso o pendientes para cada uno de sus dominios. Las acciones pueden tener una gravedad de `HIGH`, `MEDIUM` y `LOW`.

Las acciones pueden tener los siguientes estados:

- `Pending update`: la acción está en la cola para ser procesada.
- `In progress`: la acción está actualmente en curso.
- `Failed`: la acción no pudo completarse.
- `Completed`: la acción ha finalizado correctamente.
- `Not eligible`: solo para actualizaciones de software de servicio. La actualización no puede continuar porque el clúster está en mal estado.
- `Eligible`: solo para actualizaciones de software de servicio. El dominio es elegible para una actualización.

Consola

La consola OpenSearch de servicio muestra todas las acciones programadas en la configuración del dominio, junto con la gravedad y el estado actual de cada acción.

Para ver las acciones programadas de un dominio

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre del dominio para abrir la configuración.
3. Acceda a la pestaña del intervalo de menor demanda.
4. En Acciones programadas, consulte todas las acciones que están actualmente programadas, en curso o pendientes en el dominio.

CLI

Para ver las acciones programadas mediante elAWS CLI, envíe una ListScheduledActionssolicitud:

```
aws opensearch list-scheduled-actions \
  --domain-name my-domain
```

Respuesta:

```
{
    "ScheduledActions": [
        {
            "Cancellable": true,
            "Description": "The Deployment type is : BLUE_GREEN.",
            "ID": "R20220721-P13",
            "Mandatory": false,
            "Severity": "HIGH",
            "ScheduledBy": "CUSTOMER",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "SERVICE_SOFTWARE_UPDATE",
        },
        {
            "Cancellable": true,
            "Description": "Amazon Opensearch will adjust the young generation JVM
 arguments on your domain to improve performance",
            "ID": "Auto-Tune",
            "Mandatory": true,
            "Severity": "MEDIUM",
            "ScheduledBy": "SYSTEM",
            "ScheduledTime": 1.673871601E9,
            "Status": "PENDING_UPDATE",
            "Type": "JVM_HEAP_SIZE_TUNING",
```

```
        }
    ]
}
```

Reprogramar acciones

OpenSearch El servicio le notifica las actualizaciones programadas del software del servicio y las optimizaciones de Auto-Tune. Puede optar por aplicar el cambio de inmediato o reprogramarlo para una fecha y hora posteriores.

> **Note**
>
> OpenSearch El servicio puede programar la acción en un plazo de una hora a partir de la hora que usted seleccione. Por ejemplo, si decide aplicar una actualización a las 17:00 horas, puede aplicarla entre las 17:00 y las 18:00 horas.

Consola

Para reprogramar una acción

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el nombre del dominio para abrir la configuración.
3. Acceda a la pestaña del intervalo de menor demanda.
4. En Acciones programadas, seleccione la acción y elija Reprogramar.
5. Elija una de las opciones siguientes:

   - Aplicar la actualización ahora: programa de inmediato la acción para que se lleve a cabo en la hora actual si hay capacidad disponible. Si no hay capacidad disponible, ofrecemos otras franjas horarias disponibles para elegir.
   - Programarla en un intervalo de menor demanda: marca la acción para que se retome durante un próximo intervalo de menor demanda. No hay garantía de que el cambio se implemente durante el intervalo inmediatamente siguiente. Dependiendo de la capacidad, podría producirse en los días siguientes.
   - Reprogramar esta actualización: permite especificar una fecha y hora personalizadas para aplicar el cambio. Si la hora que especifica no está disponible por motivos de capacidad, puede seleccionar una franja horaria diferente.

- Cancelar actualización programada: cancela la actualización. Esta opción solo está disponible para las actualizaciones de software de servicio opcionales. No está disponible para las acciones de ajuste automático ni para las actualizaciones de software obligatorias.

6. Elija Guardar cambios.

CLI

Para reprogramar una acción mediante elAWS CLI, envíe una UpdateScheduledActionsolicitud. Para recuperar el ID de la acción, envíe una solicitud `ListScheduledActions`.

La siguiente solicitud reprograma una actualización del software de servicio para una fecha y hora específicas:

```
aws opensearch update-scheduled-action \
  --domain-name my-domain \
  --action-id R20220721-P13 \
  --action-type "SERVICE_SOFTWARE_UPDATE" \
  --desired-start-time 1677348395000 \
  --schedule-at TIMESTAMP
```

Respuesta:

```
{
   "ScheduledAction": {
      "Cancellable": true,
      "Description": "Cluster status is updated.",
      "Id": "R20220721-P13",
      "Mandatory": false,
      "ScheduledBy": "CUSTOMER",
      "ScheduledTime": 1677348395000,
      "Severity": "HIGH",
      "Status": "PENDING_UPDATE",
      "Type": "SERVICE_SOFTWARE_UPDATE"
   }
}
```

Si la solicitud falla con una `SlotNotAvailableException`, eso significa que la hora que especificó no está disponible por motivos de capacidad y debe especificar una hora diferente. OpenSearch El servicio proporciona sugerencias alternativas de franjas horarias disponibles en la respuesta.

Migración desde los intervalos de mantenimiento de ajuste automático

Si un dominio se creó antes del 16 de febrero de 2023, podría utilizar los intervalos de mantenimiento para programar las optimizaciones de ajuste automático que requieran una implementación azul/verde. Puede migrar los dominios de ajuste automático existentes para utilizar en su lugar el intervalo de menor demanda.

> **Note**
>
> No puede volver a usar los intervalos de mantenimiento después de migrar su dominio para usar los intervalos de menor demanda.

Consola

Para migrar un dominio y utilizar el intervalo de menor demanda

1. En la consola OpenSearch de Amazon Service, selecciona el nombre del dominio para abrir su configuración.
2. Vaya a la pestaña Ajuste automático y seleccione Editar.
3. Seleccione Migrar al intervalo de menor demanda.
4. En Hora de inicio (UTC), indique una hora de inicio diaria para el intervalo de menor demanda en la hora universal coordinada (UTC).
5. Elija Guardar cambios.

CLI

Para migrar de un período de mantenimiento de Auto-Tune a un período de menor actividad mediante elAWS CLI, envíe una UpdateDomainConfigsolicitud:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=[]
```

El intervalo de menor demanda debe estar activado para poder migrar un dominio del intervalo de mantenimiento de ajuste automático al intervalo de menor demanda. Puede activar el intervalo de

menor demanda en una solicitud independiente o en la misma solicitud. Para obtener instrucciones, consulte the section called “Habilitar el intervalo de menor demanda”.

Notificaciones en Amazon OpenSearch Service

Las notificaciones de Amazon OpenSearch Service contienen información importante sobre el rendimiento y el estado de tus dominios. OpenSearch El servicio le notifica sobre las actualizaciones del software del servicio, las mejoras de Auto-Tune, los problemas de estado del clúster y los errores de dominio. Las notificaciones están disponibles para todas las versiones de Elasticsearch OpenSearch OSS.

Puede ver las notificaciones en el panel de notificaciones de la consola de OpenSearch servicio. Todas las notificaciones OpenSearch del Servicio también aparecen en Amazon EventBridge. Para obtener una lista completa de las notificaciones y los eventos de muestra, consulte the section called “Supervisión de eventos”.

Temas

- Introducción a las notificaciones
- Severidad de las notificaciones
- Ejemplo de evento EventBridge

Introducción a las notificaciones

Las notificaciones se habilitan automáticamente al crear un dominio. Ve al panel de notificaciones de la consola de OpenSearch servicio para supervisar y confirmar las notificaciones. Cada notificación incluye información, como la hora en que se publicó, el dominio con el que se relaciona, un nivel de severidad y estado y una breve explicación. Puede ver notificaciones históricas de hasta 90 días en la consola.

Después de acceder al panel Notifications (Notificaciones) o de confirmar la recepción de una notificación, es posible que reciba un mensaje de error en el que se indique que no tiene permisos para realizar `es:ListNotifications` o `es:UpdateNotificationStatus`. Para resolver este problema, otorgue a su usuario o rol los siguientes permisos en IAM:

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

```
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "es:UpdateNotificationStatus",
      "es:ListNotifications"
    ],
    "Resource": "arn:aws:es:*:123456789012:domain/*"
  }]
}
```

La consola de IAM genera el error “IAM does not recognize one or more actions” (“IAM no reconoce una o varias acciones”) que se puede ignorar sin riesgo. También puede restringir la acción `es:UpdateNotificationStatus` en determinados dominios. Para obtener más información, consulte the section called “Referencia de los elementos de las políticas”.

Severidad de las notificaciones

Las notificaciones del OpenSearch Servicio pueden ser informativas, relacionadas con cualquier acción que ya hayas realizado o con las operaciones de tu dominio, o procesables, ya que requieren que tomes medidas específicas, como la aplicación de un parche de seguridad obligatorio. Cada notificación tiene una severidad asociada, que puede ser `Informational`, `Low`, `Medium`, `High` o `Critical`. En la siguiente tabla se resumen las severidades:

Gravedad	Descripción	Ejemplos
`Informational`	Información relacionada con la operación del dominio.	• Actualización del software de servicio disponible • Ajuste automático iniciado
`Low`	Una acción recomendada, pero que no tiene ningún impacto negativo en la disponibilidad o el rendimiento del dominio si no se la realiza.	• Ajuste automático cancelado • Advertencia de alto recuento de fragmentos
`Medium`	Puede haber una consecuencia si no se realiza la acción	• Error al actualizar el software del servicio • Límite de recuento de fragmentos superado

Gravedad	Descripción	Ejemplos
	recomendada, pero cuenta con una ventana de tiempo extendida para la acción que se va a realizar.	
`High`	Es necesario realizar acciones urgentes para evitar efectos adversos.	• Se requiere actualización del software de servicio • Clave KMS inaccesible
`Critical`	Se requiere una acción inmediata para evitar efectos adversos, o para recuperarse de ellos.	Ninguno disponible

Ejemplo de evento EventBridge

El siguiente ejemplo muestra un evento OpenSearch de notificación de servicio enviado a Amazon EventBridge. La notificación tiene una severidad `Informational` porque la actualización es opcional:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] available."
  }
}
```

Configuración de un dominio multi-AZ en Amazon OpenSearch Service

Para evitar la pérdida de datos y minimizar el tiempo de inactividad del clúster de Amazon OpenSearch Service en caso de interrupción del servicio, puede distribuir los nodos en dos o tres zonas de disponibilidad de la misma región, una configuración conocida como Multi-AZ. Las zonas de disponibilidad son ubicaciones aisladas dentro de cada región de AWS.

Para los dominios que ejecutan cargas de trabajo de producción, recomendamos la opción de implementación de Multi-AZ con modo de espera, que crea la siguiente configuración:

- El dominio implementado en tres zonas.
- Tipo de instancia de la generación actual para los nodos maestros dedicados y los nodos de datos.
- Tres nodos maestros dedicados y tres (o un múltiplo de tres) nodos de datos.
- Al menos dos réplicas para cada índice de su dominio o un múltiplo de tres copias de datos (incluidos los nodos principales y las réplicas).

El resto de esta sección contiene explicaciones y contextos sobre estas configuraciones.

Multi-AZ con modo de espera

Multi-AZ con modo de espera es una opción de implementación para los dominios de Amazon OpenSearch Service que ofrece una disponibilidad del 99,99 %, un rendimiento uniforme para las cargas de trabajo de producción y una configuración y administración de dominios simplificadas. Cuando utilice Multi-AZ con modo de espera, los dominios son resistentes a los fallos de infraestructura, sin que ello afecte al rendimiento ni a la disponibilidad. Esta opción de implementación cumple con este estándar al exigir una serie de prácticas recomendadas, como un recuento específico de nodos de datos, un recuento de nodos maestros, un tipo de instancia, un recuento de réplicas, la configuración de las actualizaciones de software y la activación del ajuste automático.

Al utilizar Multi-AZ con modo de espera, OpenSearch Service crea un dominio en tres zonas de disponibilidad, cada una de las cuales contiene una copia completa de los datos y los datos se distribuyen equitativamente en cada una de las zonas. Su dominio reserva los nodos de una de estas zonas como en espera, lo que significa que no atienden solicitudes de búsqueda. Cuando OpenSearch Service detecta un fallo en la infraestructura subyacente, activa automáticamente los

nodos en espera en menos de un minuto. El dominio sigue atendiendo las solicitudes de indexación y búsqueda, y cualquier impacto se limita al tiempo que se tarda en realizar la conmutación por error. No hay redistribución de los datos o los recursos, por lo que el rendimiento del clúster no se ve afectado y no hay riesgo de que se degrade la disponibilidad. Multi-AZ con modo de espera está disponible sin costo adicional.

Tiene dos opciones para crear un dominio con el modo de espera en AWS Management Console. En primer lugar, puede crear un dominio con el método de Creación fácil y OpenSearch Service utilizará automáticamente una configuración predeterminada, que incluye lo siguiente:

- Tres zonas de disponibilidad, una de las cuales actúa como zona de espera
- Tres nodos maestros y de datos dedicados
- El ajuste automático está habilitado en el dominio
- Almacenamiento GP3 para los nodos de datos

También puede elegir el método de Creación estándar y seleccionar Dominio con modo de espera como opción de implementación. Esto le permite personalizar su dominio sin dejar de utilizar las funciones clave del modo de espera, como tres zonas y tres nodos maestros. Recomendamos elegir un recuento de nodos de datos que sea múltiplo de tres (el número de zonas de disponibilidad).

Una vez que haya creado su dominio, puede ir a las páginas de detalles del dominio y, en la pestaña Configuración del clúster, confirmar que en las zonas de disponibilidad aparezca 3-AZ con modo de espera.

Si tiene problemas para migrar un dominio existente a Multi-AZ con modo de espera, consulte Error al migrar a Multi-AZ con modo de espera en la guía de solución de problemas.

Limitaciones

Al configurar un dominio con Multi-AZ con modo de espera, tenga en cuenta las siguientes limitaciones:

- El número total de particiones de un nodo no puede superar los 1000, el número total de particiones de un clúster no puede superar los 75 000 y el tamaño de una sola partición no puede superar los 65 GB.
- Multi-AZ con modo de espera solo funciona con los tipos de instancia `m5`, `c5`, `r5`, `r6g`, `c6g`, `m6g`, `r6gd` y `i3`. Para obtener más información sobre los tipos de instancias admitidos, consulte Tipos de instancias admitidos.

- Solo puede utilizar un SSD de IOPS aprovisionado, un SSD de uso general (GP3) o un almacenamiento respaldado por instancias con modo de espera.

Multi-AZ sin modo de espera

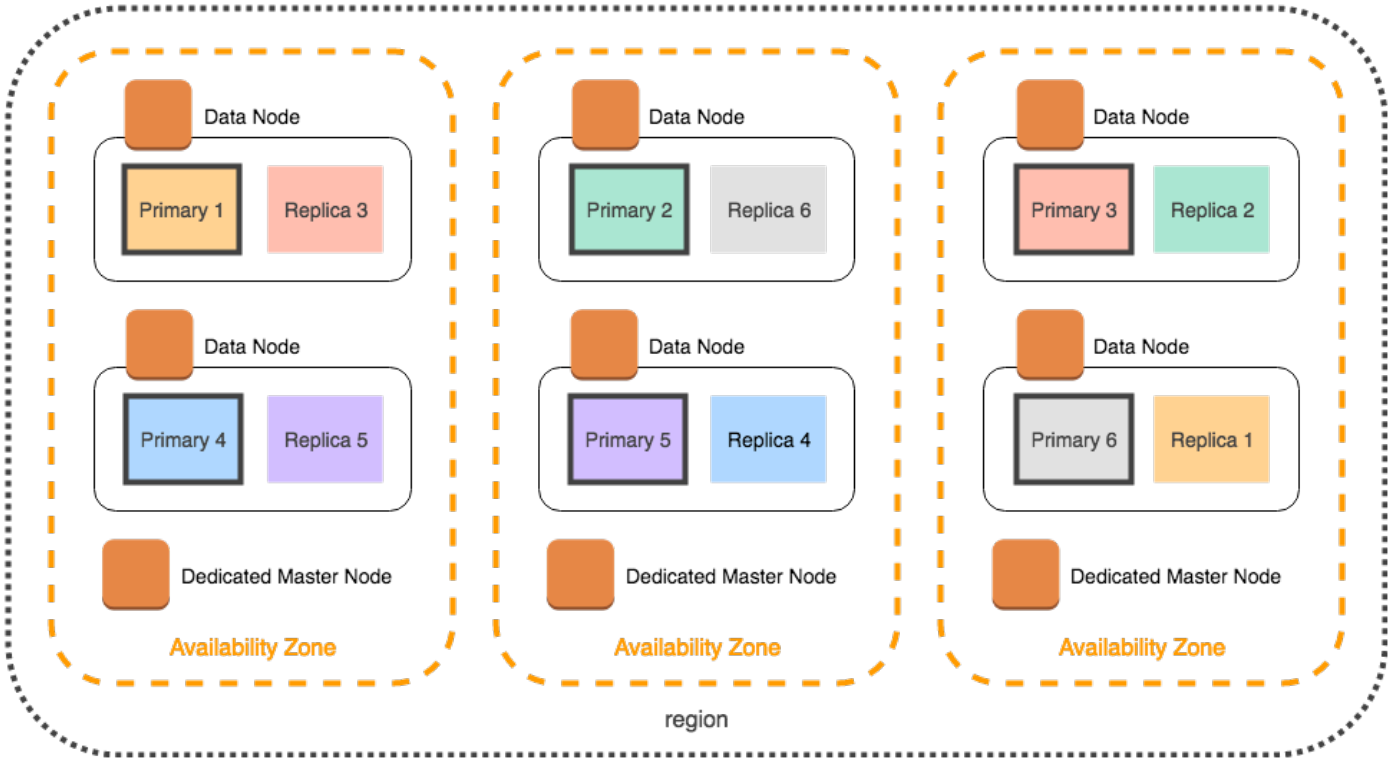
El servicio OpenSearch sigue siendo compatible con Multi-AZ sin modo de espera, lo que ofrece una disponibilidad del 99,9%. Los nodos se distribuyen en las zonas de disponibilidad y la disponibilidad depende del número de zonas de disponibilidad y de las copias de los datos. Mientras que en el modo de espera hay que configurar el dominio según las prácticas recomendadas, sin el modo de espera puede elegir su propio número de zonas de disponibilidad, nodos y réplicas. No recomendamos esta opción a menos que tenga flujos de trabajo existentes que se verían interrumpidos al crear dominios con el modo de espera.

Si elige esta opción, le recomendamos que seleccione tres zonas de disponibilidad para seguir siendo resistente a los errores de nodos, discos y zonas de disponibilidad única. Cuando se produce un error, el clúster redistribuye los datos entre los recursos restantes para mantener la disponibilidad y la redundancia. Este movimiento de datos aumenta el uso de recursos en el clúster y puede afectar al rendimiento. Si el clúster no tiene el tamaño adecuado, puede experimentar una disminución de la disponibilidad, lo que en gran medida va en contra del propósito de las zonas de disponibilidad múltiples.

La única forma de configurar un dominio sin modo de espera en el AWS Management Console es elegir el método de creación Creación estándar y seleccionar Dominio sin modo de espera como opción de implementación.

Distribución de particiones

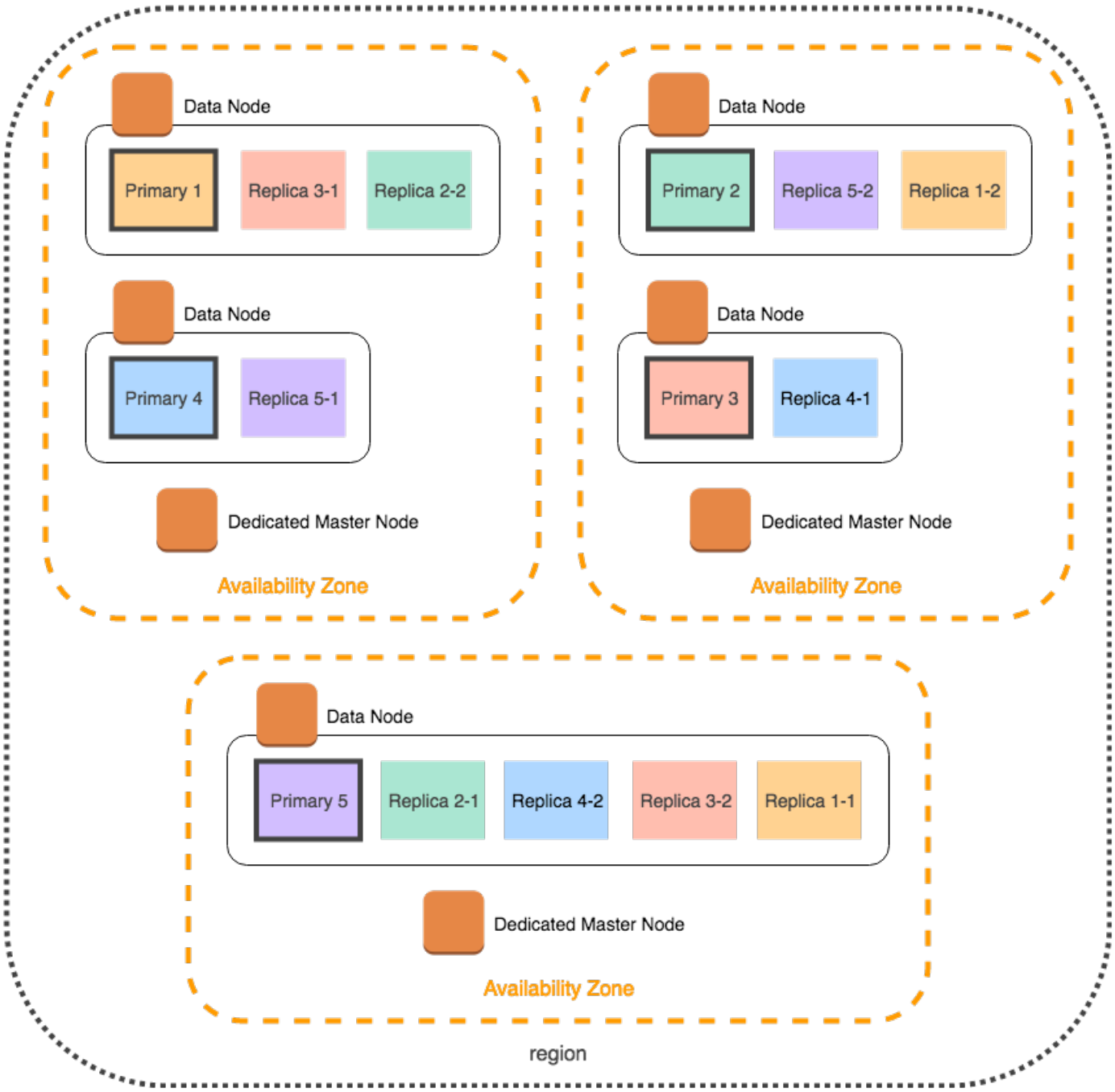
Si habilita Multi-AZ sin modo de espera, debe haber al menos una réplica por cada índice del clúster. Sin réplicas, OpenSearch Service no puede distribuir copias de sus datos a otras zonas de disponibilidad. Afortunadamente, la configuración predeterminada para cualquier índice es un recuento de réplicas de 1. Como se muestra en el siguiente diagrama, OpenSearch Service hace lo mejor posible para distribuir las particiones principales y sus particiones de réplica correspondientes entre diferentes zonas.



Además de distribuir las particiones por zona de disponibilidad, OpenSearch Service las distribuye también por nodo. Sin embargo, ciertas configuraciones de dominio pueden generar un número desequilibrado de particiones. Imagine el siguiente dominio:

- 5 nodos de datos
- 5 particiones principales
- 2 réplicas
- 3 zonas de disponibilidad

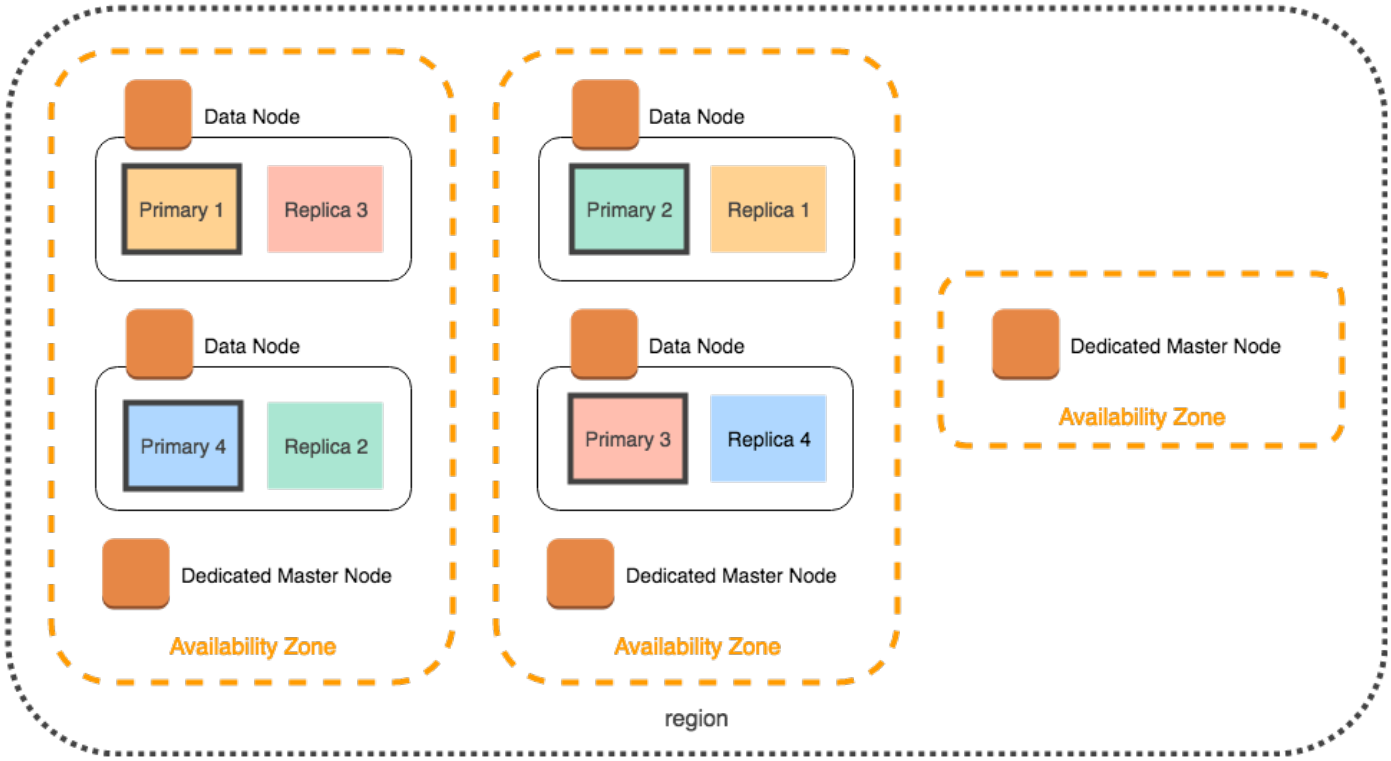
En esta situación, OpenSearch Service tiene que sobrecargar uno de los nodos para distribuir la carga de las particiones principales y replicadas entre las zonas, tal y como se muestra en el siguiente diagrama.



Para evitar este tipo de situaciones, que pueden ejercer demasiada presión sobre determinados nodos y menoscabar el rendimiento, le recomendamos que elija multi-AZ con modo de espera, cuando planea tener dos o más réplicas por cada índice, o elija un número de instancias que sea múltiplo de tres.

Distribución de nodos maestros dedicados

Aunque seleccione dos zonas de disponibilidad al configurar el dominio, OpenSearch Service distribuirá automáticamente los nodos principales dedicados en tres zonas de disponibilidad. Esta distribución ayuda a evitar el tiempo de inactividad del clúster si una zona experimenta una interrupción del servicio. Si está utilizando los tres nodos principales dedicados recomendados y una zona de disponibilidad deja de funcionar, el clúster seguirá teniendo un quorum (2) de nodos principales dedicados y podrá seleccionar un nuevo nodo principal. En el siguiente diagrama, se muestra esta configuración.



Si selecciona un tipo de instancia de una generación anterior que no esté disponible en tres zonas de disponibilidad, pueden producirse las siguientes situaciones:

- Si seleccionó tres zonas de disponibilidad para el dominio, OpenSearch Service generará un error. Elija un tipo de instancia distinto y vuelva a intentarlo.
- Si seleccionó dos zonas de disponibilidad para el dominio, OpenSearch Service distribuirá los nodos maestros dedicados en dos zonas.

Interrupción de las zonas de disponibilidad

No es frecuente que el servicio se interrumpa en las zonas de disponibilidad, pero puede ocurrir. En la siguiente tabla, se muestran diferentes configuraciones de Multi-AZ y los comportamientos durante una interrupción. La última fila de la tabla se aplica a Multi-AZ con modo de espera, mientras que todas las demás filas tienen configuraciones que solo se aplican a Multi-AZ sin modo de espera.

Número de zonas de disponibilidad de una región	Número de zonas de disponibilidad seleccionado	Número de nodos maestros dedicados	Comportamiento si se interrumpe una zona de disponibilidad
2 o más	2	0	Tiempo de inactividad. El clúster pierde la mitad de los nodos de datos y debe sustituir al menos uno en la zona de disponibilidad que queda antes de poder elegir un nodo principal.
2	2.	3	50/50 de posibilidades de tiempo de inactividad. OpenSearch Service distribuye dos nodos maestros dedicados en una zona de disponibilidad y uno en la otra: • Si la zona de disponibilidad con un nodo principal dedicado se interrumpe, los dos nodos principales dedicados de la otra zona de disponibilidad pueden elegir un nodo principal. • Si la zona de disponibilidad con dos nodos maestros dedicados experimenta una interrupción, el clúster no estará disponible hasta que la zona de disponibilidad restante se recupere.
3 o más	2	3	No hay tiempo de inactividad. OpenSearch Service distribuye automáticamente los nodos maestros dedicados entre tres zonas de disponibilidad, por lo que los dos nodos

Número de zonas de disponibilidad de una región	Número de zonas de disponibilidad seleccionado	Número de nodos maestros dedicados	Comportamiento si se interrumpe una zona de disponibilidad
			maestros dedicados pueden elegir un nodo maestro.
3 o más	3	0	No hay tiempo de inactividad. Aproximad amente dos tercios de los nodos de datos seguirán estando disponibles para elegir un nodo principal.
3 o más	3	3	No hay tiempo de inactividad. Los otros dos nodos principales dedicados pueden elegir un nodo principal.

En todas las configuraciones, independientemente de la causa, los errores en los nodos pueden hacer que los nodos de datos restantes del clúster experimenten un periodo de aumento de la carga mientras OpenSearch Service configura automáticamente nuevos nodos para sustituir a los que faltan.

Por ejemplo, en caso de que se interrumpa una zona de disponibilidad de una configuración de tres zonas, solo dos tercios de los nodos de datos tendrán que procesar tantas solicitudes como lleguen al clúster. A medida que se procesen estas solicitudes, los nodos restantes irán replicando particiones en los nuevos nodos tan pronto como se conecten, lo que podría afectar aún más al rendimiento. Si la disponibilidad es esencial para la carga de trabajo, considere la posibilidad de añadir más recursos al clúster para mitigar este problema.

> **Note**
>
> OpenSearch Service administra dominios Multi-AZ de forma transparente, por lo que no puede simular manualmente interrupciones de las zonas de disponibilidad.

Lanzamiento de tus dominios OpenSearch de Amazon Service dentro de una VPC

Puede lanzar AWS recursos, como dominios de Amazon OpenSearch Service, en una nube privada virtual (VPC). Una VPC es una red virtual dedicada a usted. Cuenta de AWSEsta infraestructura en la nube está aislada lógicamente de otras redes virtuales de la nube de AWS . La ubicación de un dominio de OpenSearch servicio dentro de una VPC permite una comunicación segura entre el OpenSearch Servicio y otros servicios de la VPC sin necesidad de una puerta de enlace a Internet, un dispositivo NAT o una conexión VPN. Todo el tráfico permanece seguro dentro de la AWS nube.

> **Note**
>
> Si coloca su dominio OpenSearch de servicio en una VPC, su equipo debe poder conectarse a la VPC. Esta conexión a menudo adopta la forma de VPN, transit gateway, red administrada o servidor proxy. No puede acceder directamente a sus dominios desde fuera de la VPC.

Temas

VPC frente a dominios públicos

Las siguientes son algunas de las formas en que los dominios de VPC difieren de los dominios públicos. Cada diferencia se describe más adelante con más detalle.

- Debido a su aislamiento lógico, los dominios que residen dentro de una VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos.
- Aunque se puede acceder a los dominios públicos desde cualquier dispositivo conectado a Internet, los dominios de VPC requieren algún tipo de VPN o proxy.
- En comparación con los dominios públicos, los dominios VPC muestran menos información en la consola de . En concreto, la pestaña Cluster health (Estado del clúster) no incluye información de particiones y la pestaña Indices (Índices) no aparece.

- Los puntos de conexión del dominio adoptan formas diferentes (`https://search-domain-name` frente a `https://vpc-domain-name`).
- No puede aplicar estas políticas de acceso basado en IP a los dominios que residan dentro de una VPC porque los grupos de seguridad ya aplican políticas de acceso basadas en IP.

Limitaciones

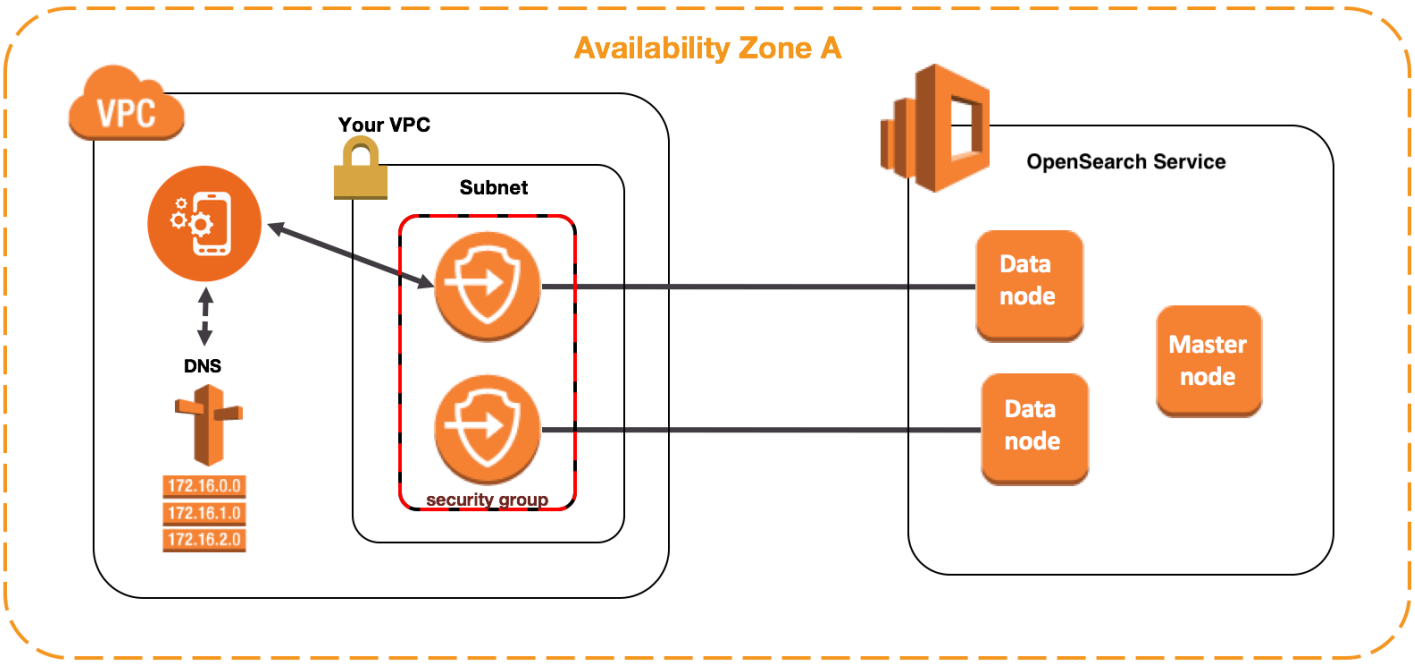
La operación de un dominio de OpenSearch servicio dentro de una VPC tiene las siguientes limitaciones:

- Si se lanza un dominio en una VPC, no se puede cambiar posteriormente para que utilice un punto de conexión público. Lo contrario también es cierto: si se crea un dominio con un punto de conexión público, no es posible situarlo posteriormente en una VPC. En lugar de ello, se debe crear un dominio nuevo y migrar los datos.
- Es posible lanzar el dominio dentro de una VPC o utilizar un punto de conexión público, pero no es posible hacer las dos cosas. Se debe elegir una de ellas al crear un dominio.
- No puede lanzar el dominio en una VPC que utilice tenencia dedicada. Debe utilizar una VPC con la tenencia establecida en Default (Predeterminada).
- Después de situar un dominio dentro de una VPC, no se puede mover a otra VPC, pero puede cambiar la configuración de subredes y grupos de seguridad.
- Para acceder a la instalación predeterminada de los OpenSearch paneles de control de un dominio que reside en una VPC, los usuarios deben tener acceso a la VPC. Este proceso depende de la configuración de la red, pero probablemente implica conectarse a una VPN o a una red gestionada, o utilizar un servidor proxy o transit gateway. Para obtener más información, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”, la Guía del usuario de Amazon VPC y the section called “Controlar el acceso a los paneles OpenSearch ”.

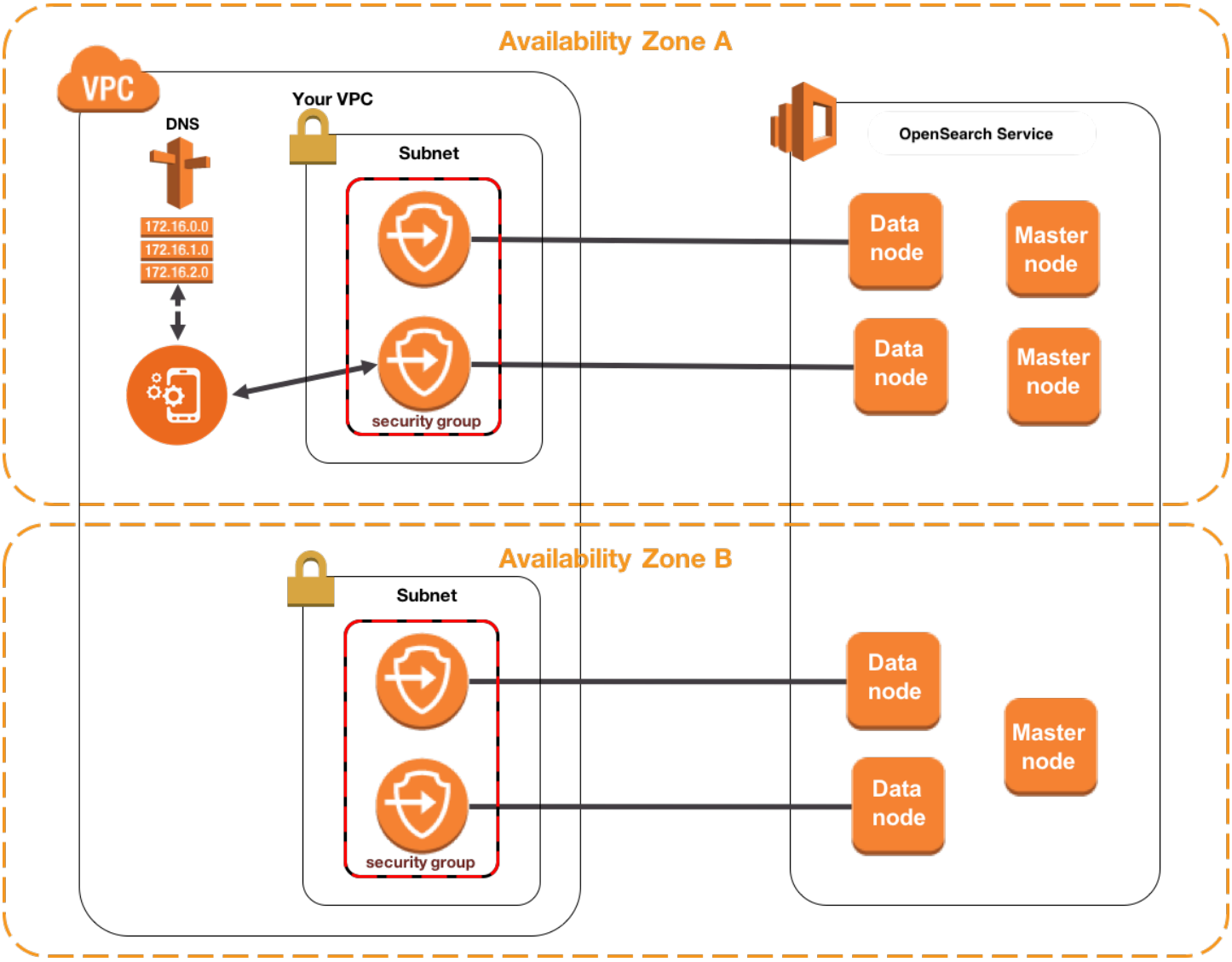
Arquitectura

Para admitir las VPC, OpenSearch Service coloca un punto final en una, dos o tres subredes de la VPC. Si habilita varias zonas de disponibilidad para su dominio, cada subred debe estar en una zona de disponibilidad diferente de la misma región. Si solo usa una zona de disponibilidad, el OpenSearch servicio coloca un punto final en una sola subred.

En la siguiente ilustración, se muestra la arquitectura de una VPC para una zona de disponibilidad.



En la siguiente ilustración, se muestra la arquitectura de una VPC para dos zonas de disponibilidad.



OpenSearch El servicio también coloca una interface de red elástica (ENI) en la VPC para cada uno de los nodos de datos. OpenSearch El servicio asigna a cada ENI una dirección IP privada del rango de direcciones IPv4 de su subred. El servicio también asigna un nombre de host de DNS pública (que es el punto de conexión del dominio) para las direcciones IP. Es necesario utilizar un servicio DNS público para resolver el punto de conexión (que es un nombre de host DNS) a las direcciones IP adecuadas de los nodos de datos:

- Si su VPC utiliza el servidor DNS proporcionado por Amazon configurando la `enableDnsSupport` opción en `true` (el valor predeterminado), la resolución del punto final del OpenSearch servicio se realizará correctamente.

- Si la VPC usa un servidor DNS privado y el servidor puede acceder a los servidores DNS públicos autorizados para resolver los nombres de host DNS, la resolución del punto final del OpenSearch servicio también se realizará correctamente.

Dado que las direcciones IP podrían cambiar, conviene resolver periódicamente el punto de conexión del dominio para no dejar de tener acceso a los nodos de datos correctos. Recomendamos establecer el intervalo de resolución de DNS en un minuto. Si se utiliza un cliente, también conviene asegurarse de que se borra la caché de DNS del cliente.

Migración del acceso público al acceso mediante VPC

Cuando se crea un dominio, se debe especificar si debe tener un punto de conexión público o residir dentro de una VPC. Una vez creado, no se puede cambiar de un tipo a otro. Lo que hay que hacer es crear un dominio nuevo y migrar los datos o reindexarlo manualmente. Las instantáneas son un método cómodo para migrar los datos. Para obtener información sobre cómo tomar instantáneas y restaurarlas, consulte the section called “Crear instantáneas de índice”.

Acerca de las políticas de acceso en los dominios de VPC

Colocar su dominio de OpenSearch servicio dentro de una VPC proporciona una capa de seguridad sólida e inherente. Cuando crea un dominio con el acceso público, el punto de conexión adopta la siguiente forma:

```
https://search-domain-name-identifier.region.es.amazonaws.com
```

Como sugiere la etiqueta “público”, esto es punto de conexión es accesible desde cualquier dispositivo conectado a Internet, aunque puede (y debería) controlar el acceso al mismo. Si accede al punto de conexión en un navegador web, es posible que reciba un mensaje `Not Authorized`, pero la solicitud llega al dominio.

Cuando crea un dominio con acceso VPC, el punto de enlace parece similar a un punto de conexión público:

```
https://vpc-domain-name-identifier.region.es.amazonaws.com
```

Si intenta acceder al punto de conexión en un navegador web, sin embargo, podría encontrar que la solicitud agota el tiempo de espera. Para realizar solicitudes `GET` incluso básicas, su equipo debe poder conectarse a la VPC. Esta conexión a menudo adopta la forma de VPN, transit gateway, red administrada o servidor proxy. Para obtener más información sobre las distintas formas puede

adoptar, consulte Ejemplos de VPC en la Guía del usuario del Amazon VPC. Para un ejemplo de desarrollo detallado, consulte the section called “Probar los dominios de VPC”.

Además de este requisito de conectividad, las VPC le permiten administrar el acceso al dominio a través de grupos de seguridad. Para muchos casos de uso, esta combinación de características de seguridad es suficiente, y es posible que se sienta cómodo aplicando una política de acceso abierto al dominio.

Operar con una política de acceso abierto no significa que cualquier usuario de Internet pueda acceder al dominio del OpenSearch servicio. Más bien, significa que si una solicitud llega al dominio del OpenSearch servicio y los grupos de seguridad asociados lo permiten, el dominio la acepta. La única excepción es si se utiliza un control de acceso detallado o una política de acceso que especifique roles de IAM. En estas situaciones, para que el dominio acepte una solicitud, los grupos de seguridad deben permitirla y debe estar firmada con credenciales válidas.

> **Note**
>
> Como los grupos de seguridad ya aplican políticas de acceso basadas en IP, no puede aplicar políticas de acceso basadas en IP a los dominios de OpenSearch servicio que residen en una VPC. Si utiliza acceso público, las políticas basadas en IP siguen estando disponibles.

Antes de comenzar: Requisitos previos para el acceso mediante VPC

Antes de poder habilitar una conexión entre una VPC y su nuevo dominio de OpenSearch servicio, debe hacer lo siguiente:

- Creación de una VPC

  Para crear su VPC, puede utilizar la consola de Amazon VPC, la AWS CLI o uno de los SDK. AWS Para obtener más información, consulte Uso de VPC en la Guía del usuario de Amazon VPC. Si ya tiene una VPC, puede omitir este paso.
- Reservar direcciones IP

  OpenSearch El servicio permite la conexión de una VPC a un dominio al colocar las interfaces de red en una subred de la VPC. Cada interfaz de red tiene asociada una dirección IP. Debe reservar un número suficiente de direcciones IP en la subred para las interfaces de red. Para obtener más información, consulte Reserva de direcciones IP en una subred de una VPC.

Probar los dominios de VPC

La seguridad mejorada de una VPC puede hacer que la conexión a su dominio y la ejecución de pruebas básicas se convierta en un reto. Si ya tienes un dominio de VPC de OpenSearch servicio y prefieres no crear un servidor VPN, prueba el siguiente proceso:

1. Para la política de acceso del dominio, elija Only use fine-grained access control (Utilizar únicamente control de acceso detallado). Siempre puede actualizar esta configuración después de finalizar las pruebas.
2. Cree una instancia Amazon EC2 de Amazon Linux en la misma VPC, subred y grupo de seguridad que su dominio de servicio. OpenSearch

   Dado que esta instancia es para fines de prueba con muy poco trabajo, elija un tipo de instancia económica como `t2.micro`. Asigne a la instancia una dirección IP pública y cree un nuevo par de claves o elija uno existente. Si crea una nueva clave, descárguela en su directorio `~/.ssh`.

   Para obtener más información acerca de la creación de instancias, consulte Introducción a las instancias de Amazon EC2 Linux.
3. Agregue un gateway de Internet a su VPC.
4. En la tabla de ruta de la VPC, agregue una nueva ruta. En Destination (Destino), especifique un bloque de CIDR que contenga la dirección IP pública de su equipo. En Target (Destino), especifique el gateway de Internet que acaba de crear.

   Por ejemplo, puede especificar solo `123.123.123.123/32` para su equipo o `123.123.123.0/24` para varios equipos.
5. Para el grupo de seguridad, especifique dos reglas de entrada:

Tipo	Protocolo	Rango de puertos	Origen
SSH (22)	TCP (6)	22	*your-cidr-block*
HTTPS (443)	TCP (6)	443	*your-security-group-id*

   La primera regla le permite usar SSH en la instancia EC2. La segunda permite que la instancia EC2 se comunique con el dominio del OpenSearch servicio a través de HTTPS.
6. En el terminal ejecute el comando siguiente:

```
ssh -i ~/.ssh/your-key.pem ec2-user@your-ec2-instance-public-ip -N -L
 9200:vpc-domain-name.region.es.amazonaws.com:443
```

Este comando crea un túnel SSH que reenvía las solicitudes a https://localhost:9200 a su dominio de OpenSearch servicio a través de la instancia EC2. Al especificar el puerto 9200 en el comando, se simula una OpenSearch instalación local, pero utilice el puerto que desee. OpenSearch El servicio solo acepta conexiones a través del puerto 80 (HTTP) o 443 (HTTPS).

El comando no proporciona comentarios y se ejecuta de forma indefinida. Para detenerlo, presione `Ctrl + C`.

7. Dirígete a https://localhost:9200/_dashboards/ en tu navegador web. Es posible que tenga que reconocer una excepción de seguridad.

   Si lo desea, puede enviar solicitudes a https://localhost:9200 mediante curl, Postman o su lenguaje de programación favorito.

> **Tip**
>
> Si detecta errores de curl debido a que los certificados no coinciden, pruebe con la marca `--insecure`.

Reserva de direcciones IP en una subred de una VPC

OpenSearch El servicio conecta un dominio a una VPC mediante la colocación de las interfaces de red en una subred de la VPC (o en varias subredes de la VPC si se habilitan varias zonas de disponibilidad). Cada interfaz de red tiene asociada una dirección IP. Antes de crear el dominio de OpenSearch servicio, debe tener un número suficiente de direcciones IP disponibles en cada subred para dar cabida a las interfaces de red.

Esta es la fórmula básica: la cantidad de direcciones IP que el OpenSearch Servicio reserva en cada subred es tres veces la cantidad de nodos de datos, dividida por la cantidad de zonas de disponibilidad.

Ejemplos

- Si un dominio tiene diez nodos de datos en tres zonas de disponibilidad, el recuento de direcciones IP por cada subred será 9 * 3 / 3 = 9.

- Si un dominio tiene ocho nodos de datos en dos zonas de disponibilidad, el recuento de direcciones IP por cada subred será 8 * 3 / 2 = 12.
- Si un dominio tiene seis nodos de datos en una zona de disponibilidad, el recuento de direcciones IP por cada subred será 6 * 3 / 1 = 18.

Al crear el dominio, el OpenSearch Servicio reserva las direcciones IP, utiliza algunas para el dominio y reserva el resto para despliegues azules o verdes. Puede ver las interfaces de red y sus direcciones IP asociadas en la sección Network Interfaces (Interfaces de red) de la consola de Amazon EC2. La columna Descripción muestra el dominio del OpenSearch servicio al que está asociada la interfaz de red.

> **Tip**
>
> Se recomienda crear subredes dedicadas para las direcciones IP reservadas del OpenSearch Servicio. Mediante el uso de subredes dedicadas, evitará solapamientos con otras aplicaciones y servicios, y se asegurará de que podrá reservar direcciones IP adicionales si necesita escalar el clúster en el futuro. Para obtener más información, consulte Creación de una subred en la VPC.

Roles vinculados a servicios para el acceso mediante VPC

Un rol vinculado a un servicio es un tipo único de rol de IAM que delega permisos a un servicio para que pueda crear y administrar recursos en su nombre. OpenSearch El servicio requiere un rol vinculado al servicio para acceder a la VPC, crear el punto final del dominio y colocar las interfaces de red en una subred de la VPC.

OpenSearch El servicio crea automáticamente el rol cuando usas la consola de OpenSearch servicio para crear un dominio dentro de una VPC. Para que esta creación automática se realice correctamente, es necesario disponer de permisos para la acción `iam:CreateServiceLinkedRole`. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Una vez que OpenSearch Service haya creado el rol, podrá verlo (`AWSServiceRoleForAmazonOpenSearchService`) mediante la consola de IAM.

Para obtener más información acerca de los permisos de este rol y como eliminarlo, consulte the section called “Uso de roles vinculados a servicios”.

Creación de instantáneas de índices en Amazon Service OpenSearch

Las instantáneas de Amazon OpenSearch Service son copias de seguridad de los índices y el estado de un clúster. Estado incluye configuraciones de clúster, información de nodos, configuración de índices y asignación de partición.

OpenSearch Las instantáneas de servicio se presentan en las siguientes formas:

- Las instantáneas automatizadas son solo para la recuperación de clústeres. Puede utilizarlas para restaurar el dominio en caso de que se produzca un estado rojo del clúster o se pierdan datos. Para obtener más información, consulte Restauración de instantáneas a continuación. OpenSearch El servicio almacena las instantáneas automatizadas en un bucket de Amazon S3 preconfigurado sin coste adicional.
- Las instantáneas manuales son para la recuperación de clústeres o para el traslado de datos de un clúster a otro. Debe iniciar instantáneas manuales. Estas instantáneas se almacenan en su propio bucket de Amazon S3 y se aplican cargos estándar de S3. Si tiene una instantánea de un OpenSearch clúster autogestionado, puede utilizarla para migrar a un OpenSearch dominio de servicio. Para obtener más información, consulta Migración a Amazon OpenSearch Service.

Todos los dominios de OpenSearch servicio toman instantáneas automatizadas, pero la frecuencia varía de las siguientes maneras:

- En el caso de los dominios que ejecutan Elasticsearch 5.3 OpenSearch o versiones posteriores, OpenSearch Service toma instantáneas automatizadas cada hora y las conserva hasta 336 durante 14 días. Las instantáneas por hora son menos disruptivas, debido a su naturaleza progresiva. También proporcionan un punto de recuperación más reciente en caso de problemas del dominio.
- En el caso de los dominios que ejecutan Elasticsearch 5.1 o versiones anteriores, OpenSearch Service toma instantáneas automatizadas a diario durante la hora que especifiques, conserva hasta 14 de ellas y no conserva ningún dato de las instantáneas durante más de 30 días.

Si el clúster pasa al estado rojo, se produce un error en todas las instantáneas automatizadas mientras persiste el estado del clúster. Si no corrige el problema en dos semanas, puede perder de forma permanente los datos del clúster. Para ver los pasos de solución de problemas, consulte the section called “Estado rojo del clúster”.

Temas

Requisitos previos

Para crear instantáneas manualmente, debe trabajar con IAM y Amazon S3. Compruebe que cumple los siguientes requisitos previos antes de intentar tomar una instantánea:

Requisito previo	Descripción
Bucket de S3	Cree un depósito de S3 para almacenar las instantáneas manuales de su dominio de servicio. OpenSearch Para ver las instrucciones, consulte Creación de un Bucket en la Guía del usuario de Amazon Simple Storage Service. Recuerde el nombre del bucket para utilizarlo en los siguientes lugares: • La instrucción `Resource` de la política de IAM que se adjunta al rol de IAM • El cliente Python utilizado para registrar un repositorio de instantáneas (si utiliza este método) **Important** No aplique una regla de ciclo de vida de S3 Glacier a este bucket. Las instantáneas manuales no admiten la clase de almacenamiento de S3 Glacier.

Requisito previo	Descripción
Rol de IAM	Cree un rol de IAM para delegar los permisos al OpenSearch Servicio. Para obtener instrucciones, consulte Creación de roles de IAM (consola) en la Guía del usuario de IAM. En el resto de este capítulo, este rol se denomina `TheSnapshotRole` . Adjuntar una política de IAM Adjunte la siguiente política a `TheSnapshotRole` para permitir el acceso al bucket de S3: `{ "Version": "2012-10-17", "Statement": [{ "Action": [ "s3:ListBucket" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: s3-bucket-name " ] }, { "Action": [ "s3:GetObject", "s3:PutObject", "s3:DeleteObject" ], "Effect": "Allow", "Resource": [ "arn:aws:s3::: s3-bucket-name /*" ] } ] }` Para ver instrucciones sobre cómo adjuntar una política a un rol, consulte Agregar permisos de identidad de IAM en la Guía del usuario de IAM.

Requisito previo	Descripción
	Modificar la relación de confianza Edite la relación de confianza de `TheSnapshotRole` para especificar el OpenSearch servicio en la `Principal` declaración, como se muestra en el siguiente ejemplo: `{ "Version": "2012-10-17", "Statement": [{ "Sid": "", "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com" }, "Action": "sts:AssumeRole" }] }` Para obtener instrucciones a fin de editar la relación de confianza, consulte Modificación de una política de confianza de rol en la Guía del usuario de IAM.

Requisito previo	Descripción

Permisos	Para registrar el repositorio de instantáneas, debe poder pasarlo `TheSnapshotRole` a OpenSearch Service. También necesita tener acceso a la acción `es:ESHttpPut`. Para conceder estos dos permisos, asocie la siguiente política al rol de IAM cuyas credenciales se utilicen para firmar la solicitud:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": "iam:PassRole", "Resource": "arn:aws:iam::  123456789012 :role/TheSnapshotRole " }, { "Effect": "Allow", "Action": "es:ESHttpPut", "Resource": "arn:aws:es:  region:123456789012 :domain/domain-name /*" } ] }`
	
	Si su usuario o rol no tiene permisos de `iam:PassRole` para transferir `TheSnapshotRole`, puede que se produzca el siguiente error común cuando intente registrar un repositorio en el siguiente paso:
	
	`$ python register-repo.py {"Message":"User: arn:aws:iam::  123456789012 :user/MyUserAccount is not authorized to perform: iam:PassRole on resource: arn:aws:iam:: 123456789012 :role/TheSnapshotRole "}`

Registrar un repositorio de instantáneas manuales

Debe registrar un repositorio de instantáneas en OpenSearch Service antes de poder realizar instantáneas de índices manuales. Esta operación única requiere que firme la AWS solicitud con

las credenciales a las que se permite el accesoTheSnapshotRole, tal y como se describe enthe section called “Requisitos previos”.

Paso 1: Asigne la función de captura de pantalla en los OpenSearch paneles (si utiliza un control de acceso detallado)

El control de acceso detallado presenta un paso adicional al registrar un repositorio. Incluso si utiliza autenticación HTTP básica para todos los demás fines, debe asignar el rol `manage_snapshots` al rol de IAM que tenga permisos `iam:PassRole` para transferir `TheSnapshotRole`.

1. Navegue hasta el complemento OpenSearch Dashboards de su dominio de servicio. OpenSearch Puedes encontrar el punto de conexión de Dashboards en el panel de control de tu dominio, en la consola de OpenSearch servicio.
2. En el menú principal, seleccione Seguridad, Roles y seleccione el rol manage_snapshots.
3. Seleccione Usuarios asignados, Administrar mapeo.
4. Agregue el ARN del rol que tenga permisos para transferir `TheSnapshotRole`. Coloque los ARN de los roles en Roles de backend.

   ```
   arn:aws:iam::123456789123:role/role-name
   ```

5. Seleccione Asignar y confirme que el usuario o el rol aparecen en Usuarios asignados.

Paso 2: registrar un repositorio

La siguiente pestaña Instantáneas muestra cómo registrar un directorio de instantáneas. Para ver las opciones específicas para cifrar una instantánea manual y registrarla después de migrarla a un nuevo dominio, consulte las pestañas correspondientes.

Snapshots

Para registrar un repositorio de instantáneas, envía una solicitud PUT al punto final del dominio del OpenSearch servicio. Puede usar curl, el cliente Python de muestra, Postman o algún otro método para enviar una solicitud firmada para registrar el repositorio de instantáneas. Tenga en cuenta que no puede usar una solicitud PUT en la consola de OpenSearch Dashboards para registrar el repositorio.

La solicitud tiene el siguiente formato:

```
PUT domain-endpoint/_snapshot/my-snapshot-repo-name
```

```
{
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "region",
    "role_arn": "arn:aws:iam::123456789012:role/TheSnapshotRole"
  }
}
```

> **Note**
>
> Los nombres de repositorio no pueden comenzar por “cs-”. Además, no debe escribir en el mismo repositorio desde varios dominios. Solo un dominio debe tener acceso de escritura al repositorio.

Si el dominio reside en una nube privada virtual (VPC), la computadora debe estar conectada a la VPC para que la solicitud registre correctamente el repositorio de instantáneas. El acceso a una VPC depende de la configuración de red, pero probablemente implica conectarse a una VPN o a una red corporativa. Para comprobar que puede acceder al dominio del OpenSearch servicio, navegue `https://your-vpc-domain.region.es.amazonaws.com` en un navegador web y compruebe que recibe la respuesta JSON predeterminada.

Cuando su bucket de Amazon S3 se encuentre en un dominio Región de AWS que no sea su OpenSearch dominio, añada el parámetro `"endpoint": "s3.amazonaws.com"` a la solicitud.

Encrypted snapshots

Actualmente no puede usar claves AWS Key Management Service (KMS) para cifrar instantáneas manuales, pero puede protegerlas mediante el cifrado del lado del servidor (SSE).

Para activar el SSE con claves administradas de S3 para el bucket que utiliza como repositorio de instantáneas, agregue `"server_side_encryption": true` al bloque `"settings"` de la solicitud PUT. Para más información, consulte Protección de datos mediante cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 en la Guía del usuario de Amazon Simple Storage Service.

Como alternativa, puede usar AWS KMS claves para el cifrado del lado del servidor en el bucket de S3 que utiliza como repositorio de instantáneas. Si utiliza este enfoque, asegúrese de dar

`TheSnapshotRole` permiso a la AWS KMS clave utilizada para cifrar el depósito de S3. Para más información, consulte Políticas de claves en AWS KMS.

Domain migration

El registro de un repositorio de instantáneas es una operación que se realiza una vez. Sin embargo, para migrar de un dominio a otro, debe registrar el mismo repositorio de instantáneas en el dominio antiguo y en el nuevo. El nombre del repositorio es arbitrario.

Tenga en cuenta las siguientes pautas al migrar a un nuevo dominio o registrar el mismo repositorio con varios dominios:

- Al registrar el repositorio en el nuevo dominio, agregue `"readonly": true` al bloque `"settings"` de la solicitud PUT. Esta configuración impide sobrescribir accidentalmente datos del dominio antiguo. Solo un dominio debe tener acceso de escritura al repositorio.
- Si migra datos a un dominio en una Región de AWS diferente (por ejemplo, desde un dominio antiguo y un bucket ubicado en us-east-2 a un nuevo dominio en us-west-2), reemplace `"region": "region"` por `"endpoint": "s3.amazonaws.com"` en la instrucción PUT y vuelva a enviar la solicitud.

Utilizar el cliente de Python de ejemplo

El cliente de Python es más fácil de automatizar que una simple solicitud HTTP y tiene una mejor reutilización. Si elige utilizar este método para registrar un repositorio de instantáneas, guarde el siguiente código de muestra de Python como archivo Python, por ejemplo `register-repo.py`. El cliente necesita AWS SDK for Python (Boto3), solicitudes y paquetes requests-aws4auth. El cliente contiene ejemplos de otras operaciones de instantánea que están marcados como comentarios.

Actualice las variables siguientes en el código de muestra: `host`, `region`, `path` y `payload`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = '' # domain endpoint
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)
```

```
# Register repository

path = '/_snapshot/my-snapshot-repo-name' # the OpenSearch API endpoint
url = host + path

payload = {
  "type": "s3",
  "settings": {
    "bucket": "s3-bucket-name",
    "base_path": "my/snapshot/directory",
    "region": "us-west-1",
    "role_arn": "arn:aws:iam::123456789012:role/snapshot-role"
  }
}

headers = {"Content-Type": "application/json"}

r = requests.put(url, auth=awsauth, json=payload, headers=headers)

print(r.status_code)
print(r.text)

# # Take snapshot
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot'
# url = host + path
#
# r = requests.put(url, auth=awsauth)
#
# print(r.text)
#
# # Delete index
#
# path = 'my-index'
# url = host + path
#
# r = requests.delete(url, auth=awsauth)
#
# print(r.text)
#
# # Restore snapshot (all indexes except Dashboards and fine-grained access control)
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
```

```
#
# payload = {
#   "indices": "-.kibana*,-.opendistro_security,-.opendistro-*",
#   "include_global_state": False
# }
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
#
# # Restore snapshot (one index)
#
# path = '_snapshot/my-snapshot-repo-name/my-snapshot/_restore'
# url = host + path
#
# payload = {"indices": "my-index"}
#
# headers = {"Content-Type": "application/json"}
#
# r = requests.post(url, auth=awsauth, json=payload, headers=headers)
#
# print(r.text)
```

Tomar instantáneas manuales

Las instantáneas no son inmediatas. Tardan tiempo en completarse y no representan point-in-time vistas perfectas del clúster. Mientras que una instantánea está en curso, puede indexar los documentos y realizar otras solicitudes al clúster, pero los nuevos documentos y las actualizaciones de los existentes no suelen estar incluidos en la instantánea. La instantánea incluye los fragmentos principales tal como estaban cuando se OpenSearch inició la instantánea. En función del tamaño del grupo de subprocesos de la instantánea, se podrían incluir diferentes particiones en la instantánea a horas ligeramente diferentes. Para ver las prácticas recomendadas para instantáneas, consulte the section called “Cómo mejorar el rendimiento de las instantáneas”.

Almacenamiento y rendimiento de instantáneas

OpenSearch Las instantáneas son incrementales, lo que significa que solo almacenan los datos que han cambiado desde la última instantánea correcta. Esta naturaleza progresiva significa que la diferencia en la utilización de disco entre instantáneas frecuentes e infrecuentes suele ser mínima.

En otras palabras, tomar instantáneas cada hora durante una semana (lo que equivale a un total de 168 instantáneas) no usaría mucho más espacio en disco que una sola instantánea al final de la semana. Además, cuanto mayor sea la frecuencia con la que toma las instantáneas, menor será el tiempo que lleve completarse. Por ejemplo, las instantáneas diarias pueden tardar entre 20 y 30 minutos en completarse, mientras que las instantáneas por hora pueden completarse en pocos minutos. Algunos OpenSearch usuarios toman instantáneas cada media hora.

Tome una instantánea

Cuando crea una instantánea, especifica la siguiente información:

- El nombre del repositorio de instantáneas
- Un nombre de la instantánea

En los ejemplos que aparecen en este capítulo, se utiliza curl, un cliente HTTP común, por motivos de comodidad y brevedad. Para pasar un nombre de usuario y una contraseña a su solicitud de curl, consulte el tutorial de introducción.

Si las políticas de acceso especifican usuarios o roles, debe firmar las solicitudes de instantáneas. Para curl, puede usar la opción `--aws-sigv4` con la versión 7.75.0 o posterior. También puede utilizar los ejemplos comentados en el cliente Python de ejemplo para realizar solicitudes HTTP firmadas para los mismos puntos de conexión que utilizan los comandos curl.

Para realizar una instantánea manual, siga estos pasos:

1. No puede tomar una instantánea si hay alguna en curso. Para comprobarlo, ejecute el siguiente comando:

   ```
   curl -XGET 'domain-endpoint/_snapshot/_status'
   ```

2. Ejecute el siguiente comando para tomar una instantánea manual:

   ```
   curl -XPUT 'domain-endpoint/_snapshot/repository-name/snapshot-name'
   ```

   Para incluir o excluir ciertos índices y especificar otras configuraciones, agregue un cuerpo de la solicitud. Para conocer la estructura de la solicitud, consulte Tomar instantáneas en la OpenSearch documentación.

> **Note**
>
> El tiempo necesario para tomar una instantánea aumenta con el tamaño del dominio del OpenSearch servicio. Cuando una operación de instantánea tarda mucho tiempo en ejecutarse, en ocasiones se genera el siguiente error: `504 GATEWAY_TIMEOUT`. Normalmente, puede hacer caso omiso de estos errores y esperar a que la operación se complete correctamente. Ejecute el siguiente comando para comprobar el estado de todas las instantáneas del dominio:
>
> ```
> curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
> ```

Restaurar instantáneas

Antes de restaurar una instantánea, asegúrese de que el dominio de destino no utilice Multi-AZ con modo de espera. Si el modo de espera está activado, se produce un error en la operación de restauración.

> **Warning**
>
> Si utiliza alias de índice, debe detener las solicitudes de escritura a un alias, o cambiar el alias a otro índice, antes de borrar su índice. Al detener las solicitudes de escritura ayuda a evitar la siguiente situación:
>
> 1. Elimina un índice, de modo que también elimina su alias.
> 2. Una solicitud de escritura errante al alias que se ha eliminado crea un nuevo índice con el mismo nombre que el alias.
> 3. Ya no puede usar el alias debido a un conflicto de nombres con el nuevo índice. Si ha cambiado el alias a otro índice, especifique `"include_aliases": false` al realizar la restauración a partir de una instantánea.

Para restablecer una instantánea

1. Identifique la instantánea que desea restaurar. Asegúrese de que todos los ajustes de este índice, como los paquetes de analizadores personalizados o los ajustes de requisitos de

asignación, sean compatibles con el dominio. Para ver todos los repositorios de instantáneas, ejecute el siguiente comando:

```
curl -XGET 'domain-endpoint/_snapshot?pretty'
```

Cuando identifique el repositorio, ejecute el siguiente comando para ver todas las instantáneas:

```
curl -XGET 'domain-endpoint/_snapshot/repository-name/_all?pretty'
```

> **Note**
>
> La mayoría de las instantáneas automatizadas se almacenan en el repositorio `cs-automated`. Si su dominio cifra datos en reposo, se almacenan en el repositorio `cs-automated-enc`. Si no ve el repositorio de instantáneas manuales que busca, asegúrese de que lo haya registrado en el dominio.

2. (Opcional) Elimine o cambie el nombre de uno o más índices del dominio del OpenSearch servicio si hay conflictos de nomenclatura entre los índices del clúster y los índices de la instantánea. No puede restaurar una instantánea de los índices en un OpenSearch clúster que ya contenga índices con los mismos nombres.

   Puede seleccionar las siguientes opciones si tiene conflictos de nomenclatura de índice:

   - Elimine los índices del dominio de OpenSearch servicio existente y, a continuación, restaure la instantánea.
   - Cambie el nombre de los índices a medida que los restaure desde la instantánea y vuelva a indexarlos más tarde.
   - Restaure la instantánea en un dominio OpenSearch de servicio diferente (solo es posible con instantáneas manuales).

   El siguiente comando elimina todos los índices existentes en un dominio:

   ```
   curl -XDELETE 'domain-endpoint/_all'
   ```

   Sin embargo, si no piensa restaurar todos los índices, solo puede eliminar uno:

```
curl -XDELETE 'domain-endpoint/index-name'
```

3. Para restaurar una instantánea, ejecute el siguiente comando:

```
curl -XPOST 'domain-endpoint/_snapshot/repository-name/snapshot-name/_restore'
```

Debido a los permisos especiales en los OpenSearch paneles y a los índices de control de acceso detallados, los intentos de restaurar todos los índices pueden fallar, especialmente si se intenta restaurar desde una instantánea automática. En el siguiente ejemplo, se restaura un solo índice, `my-index`, a partir de `2020-snapshot` en el repositorio de instantáneas `cs-automated`:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "my-index"}' \
-H 'Content-Type: application/json'
```

También puede que quiera restaurar todos los índices excepto los índices de control de acceso detallado y paneles:

```
curl -XPOST 'domain-endpoint/_snapshot/cs-automated/2020-snapshot/_restore' \
-d '{"indices": "-.kibana*,-.opendistro*"}' \
-H 'Content-Type: application/json'
```

Puede restaurar una instantánea sin eliminar sus datos mediante los parámetros `rename_pattern` y `rename_replacement`. Para obtener más información sobre estos parámetros, consulte los campos de solicitud de la API Restore Snapshot y la solicitud de ejemplo en la documentación. OpenSearch

> **Note**
>
> Si no están disponibles todas las particiones principales para los índices implicados, es posible que una instantánea tenga `state` establecido como `PARTIAL`. Este valor indica que los datos de al menos una partición no se han almacenado correctamente. Puede continuar con la restauración a partir de una instantánea parcial, pero es posible que tenga que utilizar instantáneas anteriores para restaurar los índices que falten.

Eliminar instantáneas manuales

Ejecute el siguiente comando para tomar una instantánea manual:

```
DELETE _snapshot/repository-name/snapshot-name
```

Automatizar instantáneas con la administración de instantáneas

Puede configurar una política de administración de instantáneas (SM) en los OpenSearch paneles para automatizar la creación y eliminación periódicas de instantáneas. SM puede tomar una instantánea de un grupo de índices, mientras que Administración de estados de índice solo puede tomar una instantánea por índice. Para utilizar SM in OpenSearch Service, debe registrar su propio repositorio de Amazon S3. Para ver instrucciones sobre cómo registrar su repositorio, consulte Registrar un repositorio de instantáneas manuales.

Antes de SM, OpenSearch Service ofrecía una función de instantáneas automática y gratuita que todavía está activada de forma predeterminada. Esta característica envía las instantáneas al repositorio mantenido por el servicio`cs-*`. Para desactivar la característica, póngase en contacto con AWS Support.

Para obtener más información sobre la función SM, consulte la administración de instantáneas en la OpenSearch documentación.

Actualmente, SM no admite la creación de instantáneas en varios tipos de índices. Por ejemplo, si intenta crear una instantánea en varios índices con * y algunos índices están en el nivel semiactivo, la creación de la instantánea producirá un error. Si necesita que la instantánea contenga varios tipos de índices, utilice la acción de instantánea de ISM hasta que SM admita esta opción.

Configuración de permisos de

Si va a actualizar a la versión 2.5 desde una versión anterior del dominio de OpenSearch servicio, es posible que los permisos de seguridad de administración de instantáneas no estén definidos en el dominio. Los usuarios que no sean administradores deben estar asignados a este rol para usar la administración de instantáneas en los dominios mediante un control de acceso detallado. Para crear el rol de administración de instantáneas de forma manual, siga estos pasos:

1. En los OpenSearch paneles, vaya a Seguridad y elija Permisos.
2. Seleccione Crear grupo de acciones y configure los siguientes grupos:

Nombre del grupo	Permisos
`snapshot_management_full_access`	• `cluster:admin/opensearch/snapshot_management/*` • `cluster:admin/opensearch/notifications/feature/publish` • `cluster:admin/repository/*` • `cluster:admin/snapshot/*`
`snapshot_management_read_access`	• `cluster:admin/opensearch/snapshot_management/policy/get` • `cluster:admin/opensearch/snapshot_management/policy/search` • `cluster:admin/opensearch/snapshot_management/policy/explain` • `cluster:admin/repository/get` • `cluster:admin/snapshot/get`

3. Seleccione Roles y, a continuación, Crear rol.
4. Asigne el nombre snapshot_management_role al rol.
5. Para Permisos de clúster, seleccione `snapshot_management_full_access` o `snapshot_management_read_access`.
6. Seleccione Crear.
7. Después de crear el rol, debe mapearlo a cualquier rol de usuario o backend que administre instantáneas.

Consideraciones

Tenga en cuenta lo siguiente al configurar la administración de instantáneas:

- Se permite una política por repositorio.
- Se permiten hasta 400 instantáneas para una política.
- Esta característica no se ejecutará si su dominio tiene un estado rojo, está sometido a una presión elevada por la JVM (un 85 % o más) o tiene una característica de captura bloqueada. Si

el rendimiento general de indexación y búsqueda de su clúster se ve afectado, es posible que SM también se vea afectado.

- Una operación de instantánea solo comienza una vez finalizada la operación anterior, por lo que una política no activa ninguna operación de instantánea simultánea.
- Varias políticas con la misma programación pueden provocar un pico de recursos. Si los índices instantáneos de las políticas se superponen, las operaciones de instantáneas a nivel de partición solo se pueden ejecutar de forma secuencial, lo que puede provocar un problema de rendimiento en cascada. Si las políticas comparten un repositorio, habrá un pico de operaciones de escritura en ese repositorio.
- Le recomendamos que programe la automatización de sus operaciones instantáneas para que no se realice más de una vez por hora, a menos que se trate de un caso de uso especial.

Automatizar instantáneas con la administración de estado de índice

Puede utilizar la operación `snapshot` de administración de estado de índice (ISM) para activar automáticamente instantáneas de índices en función de los cambios en su antigüedad, tamaño o número de documentos. ISM es la mejor opción cuando se necesita una instantánea por índice. Si necesita hacer una instantánea de un grupo de índices, consulte Automatizar instantáneas con la administración de instantáneas.

Para utilizar SM in OpenSearch Service, debe registrar su propio repositorio de Amazon S3. Para obtener un ejemplo de política ISM con la operación `snapshot`, consulte Políticas de muestra.

Utilizar Curator para instantáneas

Si ISM no funciona para la administración de índices e instantáneas, puede utilizar Curator en su lugar. Ofrece una funcionalidad avanzada de filtrado que ayuda a simplificar tareas de administración en clústeres complejos. Utilice pip para instalar Curator:

```
pip install elasticsearch-curator
```

Puede utilizar Curator como una interfaz de línea de comandos (CLI) o una API de Python. Si utiliza la API de Python, debe utilizar la versión 7.13.4 o anterior del cliente elasticsearch-py heredado. No admite el cliente opensearch-py.

Si utiliza la CLI, exporte sus credenciales en la línea de comandos y configure `curator.yml` como se indica a continuación:

```
client:
  hosts: search-my-domain.us-west-1.es.amazonaws.com
  port: 443
  use_ssl: True
  aws_region: us-west-1
  aws_sign_request: True
  ssl_no_validate: False
  timeout: 60

logging:
  loglevel: INFO
```

Actualización de los dominios OpenSearch de Amazon Service

> **Note**
>
> OpenSearch y las actualizaciones de la versión de Elasticsearch son diferentes de las actualizaciones del software del servicio. Para obtener información sobre cómo actualizar el software de servicio para su dominio OpenSearch de servicio, consulte. the section called "Actualizaciones del software del servicio"

Amazon OpenSearch Service ofrece actualizaciones locales para dominios que ejecutan la OpenSearch versión 1.0 o una versión posterior, o Elasticsearch 5.1 o una versión posterior. Si utilizas servicios como Amazon Data Firehose o Amazon CloudWatch Logs para transmitir datos a OpenSearch Service, comprueba que estos servicios sean compatibles con la versión más reciente de OpenSearch antes de realizar la migración.

Temas

Rutas de actualización admitidas

Actualmente, el OpenSearch servicio admite las siguientes rutas de actualización:

Desde la versión	Hasta la versión
OpenSearch 1.3 o 2. x	OpenSearch 2. x El control de versiones 2.3 incluye los siguientes cambios importantes: • El `type` parámetro se eliminó de todos los puntos finales de la OpenSearch API en la versión 2.0. Para más información, consulte Cambios bruscos. • Si tu dominio contiene índices (activos o fríos) que se crearon originalmente en Elasticsearch 6.8, esos índices no son compatibles con la 2.3. UltraWarm OpenSearch Antes de actualizar a la versión 2.3, debe volver a indexar los índices incompatibles. En el caso de índices incompatibles UltraWarm o en frío, migre los datos a un almacenamiento activo, vuelva a indexar los datos y, a continuación, vuelva a migrarlos a un almacenamiento caliente o frío. También puede quitar índices si ya no los necesita. Si actualiza accidentalmente su dominio al control de versiones 2.3 sin realizar primero estos pasos, no podrá migrar los índices incompatibles fuera de su nivel de almacenamiento actual. La única opción es eliminarlos.
OpenSearch 1. x	OpenSearch 1. x
Elasticsearch 7.x	Elasticsearch 7. x o 1. OpenSearch x **Important** OpenSearch 1. x introduce numerosos cambios importantes. Para más información, consulte Cambio de nombre de Amazon OpenSearch Service.

Desde la versión	Hasta la versión
Elasticsearch 6.8	Elasticsearch 7. x o 1. OpenSearch x **Important** Elasticsearch 7.0 y OpenSearch 1.0 incluyen numerosos cambios importantes. Antes de iniciar una actualización local, recomendamos realizar una instantánea manual de la versión 6. x dominio, restaurándolo en una prueba 7. x o OpenSearch 1. dominio x y usar ese dominio de prueba para identificar posibles problemas de actualización. Para ver los cambios más importantes en la OpenSearch versión 1.0, consulteCambio de nombre de Amazon OpenSearch Service. Al igual que Elasticsearch 6.x, los índices solo pueden contener un tipo de mapeo, pero ese tipo debe denominarse `_doc`. Como resultado, determinadas API ya no requieren un tipo de mapeo en el cuerpo de la solicitud (como, por ejemplo, la API `_bulk`). Para índices nuevos, Elasticsearch 7 se hospedó automáticamente. x y 1. OpenSearch x tienen un recuento de fragmentos predeterminado de uno. OpenSearch Dominios de servicio en Elasticsearch 7. x y las versiones posteriores conservan el valor predeterminado anterior de cinco.
Elasticsearch 6.x	Elasticsearch 6.x

Desde la versión	Hasta la versión
Elasticsearch 5.6	Elasticsearch 6.x **Important** Los índices creados en la versión 6.x ya no admiten varios tipos de mapeo. Los índices creados en la versión 5.x siguen admitiendo varios tipos de mapeo cuando se restauran en un clúster 6.x. Compruebe que el código de cliente solo cree un único tipo de mapeo por índice. Para minimizar el tiempo de inactividad durante la actualización de Elasticsearch 5.6 a 6. x, OpenSearch Service vuelve a indexar el `.kibana` índice, lo elimina `.kibana-6` `.kibana`, crea un nombre `.kibana` de alias y asigna el nuevo índice al nuevo alias.
Elasticsearch 5.x	Elasticsearch 5.x

El proceso de actualización consta de tres pasos:

1. Comprobaciones previas a la actualización: el OpenSearch servicio comprueba si hay problemas que puedan bloquear una actualización y no pasa al siguiente paso a menos que estas comprobaciones se realicen correctamente.
2. Instantánea: el OpenSearch servicio toma una instantánea del clúster OpenSearch o del clúster de Elasticsearch y no pasa al siguiente paso a menos que la instantánea se realice correctamente. Si se produce un error en la actualización, OpenSearch Service usa esta instantánea para restaurar el clúster a su estado original. Para más información, consulte the section called “No se puede cambiar a una versión anterior después de una actualización”.
3. Actualización: el OpenSearch servicio inicia la actualización, que puede tardar entre 15 minutos y varias horas en completarse. OpenSearch Es posible que los paneles no estén disponibles durante una parte o durante toda la actualización.

Inicio de una actualización (consola)

El proceso de actualización es irreversible y no se puede pausar ni cancelar. Durante una actualización no puede realizar cambios de configuración en el dominio. Antes de comenzar una actualización, compruebe que desea continuar. Puede utilizar estos mismos pasos para realizar la verificación de actualización sin iniciar realmente una actualización.

Si el clúster tiene nodos maestros dedicados, OpenSearch las actualizaciones se completan sin tiempo de inactividad. De lo contrario, el clúster podría no responder durante varios segundos después de la actualización mientras elige un nodo maestro.

Para actualizar un dominio a una versión posterior de OpenSearch Elasticsearch

1. Tome una instantánea manual de su dominio. Esta instantánea sirve como copia de seguridad que puede restaurar en un dominio nuevo si desea volver a usar la versión anterior OpenSearch .
2. Visite https://aws.amazon.com y elija Iniciar sesión en la consola.
3. En Analytics, selecciona Amazon OpenSearch Service.
4. En el panel de navegación, en Dominios, seleccione el dominio que desea actualizar.
5. Seleccione Acciones y Actualizar.
6. Seleccione la version a la que actualizar. Si vas a actualizar a una OpenSearch versión, aparecerá la opción Habilitar el modo de compatibilidad. Si habilitas esta configuración, indicará que OpenSearch su versión es 7.10 para permitir que los clientes y complementos de Elasticsearch OSS, como Logstash, sigan funcionando con Amazon Service. OpenSearch Podrá desactivar esta configuración más tarde
7. Seleccione Actualizar.
8. Verifique el Estado en el panel del dominio para monitorear el estado de la actualización.

Inicio de una actualización (CLI)

Puedes usar las siguientes operaciones para identificar la versión correcta de Elasticsearch OpenSearch o Elasticsearch para tu dominio, iniciar una actualización local, realizar la comprobación previa a la actualización y ver el progreso:

- `get-compatible-versions` (`GetCompatibleVersions`)
- `upgrade-domain` (`UpgradeDomain`)

- `get-upgrade-status` (`GetUpgradeStatus`)
- `get-upgrade-history` (`GetUpgradeHistory`)

Para obtener más información, consulta la referencia de comandos deAWS CLI y la referencia de la API de Amazon OpenSearch Service.

Inicio de una actualización (SDK)

En este ejemplo, se utiliza el cliente Python de OpenSearchServicebajo nivel del AWS SDK for Python (Boto) para comprobar si un dominio es apto para la actualización a una versión específica, lo actualiza y comprueba continuamente el estado de la actualización.

```
import boto3
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default Region.

DOMAIN_NAME = ''  # The name of the domain to upgrade
TARGET_VERSION = ''  # The version you want to upgrade the domain to. For example,
 OpenSearch_1.1

my_config = Config(
    # Optionally lets you specify a Region other than your default.
    region_name='us-east-1'
)
client = boto3.client('opensearch', config=my_config)


def check_versions():
    """Determine whether domain is eligible for upgrade"""
    response = client.get_compatible_versions(
        DomainName=DOMAIN_NAME
    )
    compatible_versions = response['CompatibleVersions']
    for i in range(len(compatible_versions)):
        if TARGET_VERSION in compatible_versions[i]["TargetVersions"]:
            print('Domain is eligible for upgrade to ' + TARGET_VERSION)
            upgrade_domain()
            print(response)
```

```
        else:
            print('Domain not eligible for upgrade to ' + TARGET_VERSION)


def upgrade_domain():
    """Upgrades the domain"""
    response = client.upgrade_domain(
        DomainName=DOMAIN_NAME,
        TargetVersion=TARGET_VERSION
    )
    print('Upgrading domain to ' + TARGET_VERSION + '...' + response)
    time.sleep(5)
    wait_for_upgrade()


def wait_for_upgrade():
    """Get the status of the upgrade"""
    response = client.get_upgrade_status(
        DomainName=DOMAIN_NAME
    )
    if (response['UpgradeStep']) == 'UPGRADE' and (response['StepStatus']) ==
 'SUCCEEDED':
        print('Domain successfully upgraded to ' + TARGET_VERSION)
    elif (response['StepStatus']) == 'FAILED':
        print('Upgrade failed. Please try again.')
    elif (response['StepStatus']) == 'SUCCEEDED_WITH_ISSUES':
        print('Upgrade succeeded with issues')
    elif (response['StepStatus']) == 'IN_PROGRESS':
        time.sleep(30)
        wait_for_upgrade()


def main():
    check_versions()


if __name__ == "__main__":
    main()
```

Solución de errores de validación

Cuando inicias una actualización de una versión OpenSearch o de Elasticsearch, OpenSearch Service primero realiza una serie de comprobaciones de validación para garantizar que tu dominio

sea apto para una actualización. Si se produce un error en alguna de estas comprobaciones, recibirá una notificación con los problemas específicos que debe corregir antes de actualizar su dominio. Para obtener una lista de posibles problemas y los pasos para resolverlos, consulte the section called "Solución de errores de validación".

Solución de problemas de una actualización

Las actualizaciones locales requieren dominios en buen estado. Es posible que su dominio no pueda optar por una actualización o que no se actualice por diversas razones. La siguiente tabla muestra los problemas más comunes.

Problema	Descripción
No se admite el complemento opcional	Cuando actualizas un dominio con complementos opcionales, OpenSearch Service también actualiza automáticamente los complemen tos. Por lo tanto, la versión de destino de su dominio también debe admitir estos complementos opcionales. Si el dominio tiene instalado un complemento opcional que no está disponible para la versión de destino, se produce un error en la solicitud de actualización.
Demasiadas particion es por nodo	OpenSearch, así como 7. x versiones de Elasticsearch, tienen una configuración predeterminada de no más de 1000 particiones por nodo. Si un nodo de tu clúster actual supera esta configuración, el OpenSearc h servicio no te permite realizar la actualización. Consulte the section called "Límite máximo de fragmentos superado" para obtener opciones de solución de problemas.
Dominio en procesamiento	El dominio está en medio de un cambio de configuración. Compruebe si es posible optar a la actualización una vez que se complete la operación.
Estado rojo del clúster	Uno o varios índices en el clúster aparecen en rojo. Para ver los pasos de solución de problemas, consulte the section called "Estado rojo del clúster".
Tasa de errores alta	El clúster devuelve un gran número de errores 5xx al intentar procesar solicitudes. Este problema suele ser el resultado de demasiadas solicitud es de lectura o escritura simultáneas. Considere la posibilidad de reducir el tráfico hacia el clúster o el escalado del dominio.

Problema	Descripción
Cerebro dividido	Cerebro dividido significa que el clúster tiene más de un nodo maestro y se ha dividido en dos clústeres que nunca se volverán a unir por sí mismos. Puede evitar un cerebro dividido con el número recomendado de nodos maestros dedicados. Para obtener ayuda a fin de recuperar un cerebro dividido, póngase en contacto con AWS Support.
Nodo maestro no encontrado	OpenSearch El servicio no encuentra el nodo principal del clúster. Si el dominio utiliza Multi-AZ, es posible que un error de una zona de disponibilidad haya hecho que el clúster pierda el quorum y no pueda elegir un nuevo nodo maestro. Si el problema no se resuelve por sí solo, póngase en contacto con AWS Support.
Demasiadas tareas pendientes	El nodo maestro está bajo una gran carga y tiene muchas tareas pendientes. Considere la posibilidad de reducir el tráfico hacia el clúster o el escalado del dominio.
Volumen de almacenamiento dañado	El volumen de disco de uno o más nodos no funciona correctamente. Este problema a menudo ocurre junto con otros problemas, como una alta tasa de error o demasiadas tareas pendientes. Si se produce aisladamente y no se resuelve por sí solo, póngase en contacto con AWS Support.
Problema de clave de KMS	La clave de KMS que se utiliza para cifrar el dominio está inaccesible o no está. Para más información, consulte the section called “Monitorear dominios que cifran los datos en reposo”.
Snapshot en proceso de creación	El dominio está tomando una instantánea en este momento. Compruebe si es posible optar a la actualización una vez que se complete la instantánea. Compruebe también si puede hacer una lista de los repositorios de instantáneas manuales, una lista de instantáneas dentro de dichos repositorios y tomar instantáneas manuales. Si el OpenSearch servicio no puede comprobar si una instantánea está en curso, las actualizaciones pueden fallar.

Problema	Descripción
Error en instantánea o tiempo de espera agotado	La instantánea previa a la actualización ha tardado demasiado tiempo en completarse o ha generado un error. Compruebe el estado del clúster y vuelva a intentarlo. Si el problema sigue sin resolverse, póngase en contacto con AWS Support.
Índices incompatibles	Uno o varios índices son incompatibles con la versión de destino. Este problema puede producirse si migraste los índices desde una versión anterior de OpenSearch Elasticsearch. Reindexe los índices e inténtelo de nuevo.
Alto uso del disco	El uso del disco para el clúster es superior al 90 %. Elimine los datos o escale el dominio, e inténtelo de nuevo.
Alto uso de JVM	La presión de memoria de JVM es superior al 75 %. Reduzca el tráfico hacia el clúster o amplíe el dominio, e inténtelo de nuevo.
OpenSearch Problema con el alias de los paneles	`.dashboards` ya está configurado como un alias y se asigna a un índice incompatible, probablemente uno de una versión anterior de OpenSearch Dashboards. Vuelva a indexar e inténtelo de nuevo.
Estado rojo de Dashboards	OpenSearch El estado del panel es rojo. Intente utilizar Dashboards cuando se complete la actualización. Si el estado rojo persiste, resuélval o manualmente, e inténtelo de nuevo.
Compatibilidad entre clústeres	Solo puede actualizar si se mantiene la compatibilidad entre clústeres entre los dominios de origen y destino después de la actualización. Durante el proceso de actualización, se identifican las conexiones incompatibles. Para continuar, actualice el dominio remoto o elimine las conexiones incompatibles. Tenga en cuenta que si la replicación está activa en el dominio, no podrá reanudarla una vez que elimine la conexión.
Otro problema con OpenSearch el servicio	Los problemas con el propio OpenSearch Servicio pueden hacer que tu dominio aparezca como no apto para una actualización. Si a su dominio no se aplica ninguna de las condiciones anteriores y el problema persiste durante más de un día, póngase en contacto con AWS Support.

Uso de una instantánea para migrar datos

Las actualizaciones locales son la forma más fácil, rápida y confiable de actualizar un dominio a una versión posterior OpenSearch o a una versión de Elasticsearch. Las instantáneas son una buena opción si tiene que migrar de una versión previa a la 5.1 de Elasticsearch o si desea migrar a un clúster totalmente nuevo.

La siguiente tabla muestra cómo usar las instantáneas para migrar datos a un dominio que usa una versión diferente OpenSearch o de Elasticsearch. Para obtener información sobre cómo tomar instantáneas y restaurarlas, consulte the section called “Crear instantáneas de índice”.

Desde la versión	Hasta la versión	Proceso de migración

OpenSearch 1.3 o 2. x	OpenSearch 2. x	1. Revise los cambios más recientes de la versión OpenSearch 2.3 para ver si necesita realizar ajustes en sus índices o aplicaciones.
		2. Cree una instantánea manualmente del dominio 1.3 o 2.x.
		3. Cree un dominio 2.x que sea una versión superior al dominio 1.3 o 2.x original.
		4. Restaure la instantánea desde el dominio original al dominio 2.x. Durante la operación, es probable que tenga que restaurar el índice `.opensearch` con un nuevo nombre:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		A continuación, puede reindexar `.backup-opensearch` en el nuevo dominio y asignarlo a `.opensearch`. Tenga en cuenta que la llamada

Desde la versión	Hasta la versión	Proceso de migración
		REST `_restore` no incluye `include_global_state` porque la entrada predeterminada en `_restore` es falsa. Como resultado, el dominio de prueba no incluirá ninguna plantilla de índice y no tendrá el estado completo de la copia de seguridad. 5. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración

OpenSearch 1. x	OpenSearch 1. x	1. Cree una instantánea manual del dominio 1.x.
		2. Cree un dominio 1.x que sea una versión superior al dominio 1.x original.
		3. Restaure la instantánea desde el dominio original al nuevo dominio 1.x. Durante la operación, es probable que tenga que restaurar el índice `.opensearch` con un nuevo nombre:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".opensearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		A continuación, puede reindexar `.backup-opensearch` en el nuevo dominio y asignarlo a `.opensearch`. Tenga en cuenta que la llamada REST `_restore` no incluye `include_global_state` porque la entrada predeterminada en `_restore` es falsa. Como resultado, el dominio de prueba no incluirá ninguna plantilla de índice y no tendrá el estado completo de la copia de seguridad.
		4. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración

Elasticsearch 6.x o 7.x	OpenSearch 1. x	1. Revise los cambios más recientes de la OpenSearch versión 1.0 para ver si necesita realizar ajustes en sus índices o aplicaciones.
		2. Cree una instantánea manualmente del dominio de Elasticsearch 7.x o 6.x.
		3. Cree un OpenSearch 1. dominio x.
		4. Restaure la instantánea del dominio de Elasticsearch al OpenSearch dominio. Durante la operación, es probable que tenga que restaurar el índice `.elasticsearch` con un nuevo nombre:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-opensearch"`
		`}`
		A continuación, puede reindexar `.backup-opensearch` en el nuevo dominio y asignarlo a `.elasticsearch`. Tenga en cuenta que la llamada REST `_restore` no incluye `include_global_state` porque la entrada predeterminada en `_restore` es falsa. Como resultado, el dominio de prueba no incluirá ninguna plantilla de índice y no tendrá el estado completo de la copia de seguridad.
		5. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración

Elasticsearch 6.x	Elasticsearch 7.x	1. Consulte los cambios importantes en 7.0 para saber si necesita realizar ajustes en los índices o en la aplicación.
		2. Cree una instantánea manual del dominio 6.x.
		3. Cree un dominio de la versión 7x.
		4. Restaure la instantánea desde el dominio original al dominio 7x. Durante la operación, es probable que tenga que restaurar el índice `.opensearch` con un nuevo nombre:
		`POST _snapshot/ <repository-name> /<snapshot-name>/_restore`
		`{`
		`  "indices": "*",`
		`  "ignore_unavailable": true,`
		`  "rename_pattern": ".elasticsearch",`
		`  "rename_replacement": ".backup-elasticsearch"`
		`}`
		A continuación, puede reindexar `.backup-elasticsearch` en el nuevo dominio y asignarlo a `.elasticsearch` . Tenga en cuenta que la llamada REST `_restore` no incluye `include_global_state` porque la entrada predeterminada en `_restore` es falsa. Como resultado, el dominio de prueba no incluirá ninguna plantilla de índice y no tendrá el estado completo de la copia de seguridad.
		5. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración
Elasticsearch 6.x	Elasticsearch 6.8	1. Cree una instantánea manual del dominio 6.x. 2. Cree un dominio de la versión 6.8. 3. Restaure la instantánea desde el dominio original al dominio 6.8. 4. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.
Elasticsearch 5.x	Elasticsearch 6.x	1. Consulte los cambios importantes en 6.0 para saber si necesita realizar ajustes en los índices o en la aplicación. 2. Cree una instantánea manual del dominio 5.x. 3. Cree un dominio de la versión 6.x. 4. Restaure la instantánea desde el dominio original al dominio 6.x. 5. Si ya no necesita el dominio 5.x, elimínelo. De lo contrario, el dominio seguirá generando costos.
Elasticsearch 5.x	Elasticsearch 5.6	1. Cree una instantánea manual del dominio 5.x. 2. Cree un dominio de la versión 5.6. 3. Restaure la instantánea desde el dominio original al dominio 5.6. 4. Si ya no necesita el dominio original, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración
Elasticsearch 2.3	Elasticsearch 6.x	Las instantáneas de Elasticsearch 2.3 no son compatibl es con la versión 6.x. Para migrar sus datos directamente de la versión 2.3 a 6.x, debe volver a crear manualmente sus índices en el nuevo dominio. Como alternativa, puede seguir los pasos del cambio de la versión 2.3 a 5.x de esta tabla, realizar las operaciones de `_reindex` en el nuevo dominio 5.x para convertir sus índices 2.3 en índices 5.x y después seguir los pasos del cambio de la versión 5.x a 6.x.
Elasticsearch 2.3	Elasticsearch 5.x	1. Consulte los cambios importantes en 5.0 para saber si necesita realizar ajustes en los índices o en la aplicación. 2. Cree una instantánea manualmente del dominio 2.3. 3. Cree un dominio de la versión 5.x. 4. Restaure la instantánea desde el dominio 2.3 al dominio 5.x. 5. Si ya no necesita el dominio 2.3, elimínelo. De lo contrario, el dominio seguirá generando costos.

Desde la versión	Hasta la versión	Proceso de migración
Elasticsearch 1.5	Elasticsearch 5.x	Las instantáneas de Elasticsearch 1.5 no son compatibles con la versión 5.x. Para migrar sus datos de la versión 1.5 a 5.x, debe volver a crear manualmente sus índices en el nuevo dominio. **Important** Las instantáneas de la versión 1.5 son compatibles con la versión 2.3, pero los dominios del OpenSearch Servicio 2.3 no admiten esta operación. `_reindex` Dado que no puede reindexarlos, los índices que se originaron en un dominio 1.5 siguen sin restaurar instantáneas de 2.3 a dominios 5x.
Elasticsearch 1.5	Elasticsearch 2.3	1. Utilice el complemento de migración para saber si puede hacer directamente la actualización a la versión 2.3. Es posible que tenga que realizar cambios en los datos antes de la migración. a. En un navegador web, abra `http://`*`domain-endpoint`*` /_plugin/migration/` . b. Seleccione Realizar comprobaciones ahora. c. Revise los resultados y, si es necesario, siga las instrucciones para realizar cambios en los datos. 2. Cree una instantánea manualmente del dominio 1.5. 3. Cree un dominio de la versión 2.3. 4. Restaure la instantánea desde el dominio 1.5 al dominio 2.3. 5. Si ya no necesita el dominio 1.5, elimínelo. De lo contrario, el dominio seguirá generando costos.

Creación de un punto de conexión personalizado para Amazon OpenSearch Service

La creación de un punto de conexión personalizado para un dominio de Amazon OpenSearch Service facilita la consulta de las direcciones URL de OpenSearch y de OpenSearch Dashboards. Puede incluir la marca de su empresa o simplemente utilizar un punto de conexión más corto y fácil de recordar que el estándar.

Si alguna vez necesita cambiar a un nuevo dominio, simplemente actualice el DNS para que apunte a la nueva URL y continúe utilizando el mismo punto de conexión anterior.

Proteja los puntos de conexión personalizados mediante la generación de un certificado en AWS Certificate Manager (ACM) o la importación de uno propio.

Puntos de conexión personalizados para nuevos dominios

Puede habilitar un punto de conexión personalizado para un nuevo dominio de OpenSearch Service mediante la consola de OpenSearch Service, la AWS CLI o la API de configuración.

Para personalizar el punto de conexión (consola)

1. En la consola de OpenSearch Service, elija Crear dominio y proporcione un nombre para el dominio.
2. En Punto de conexión personalizado, seleccione Habilitar punto de conexión personalizado.
3. En Nombre de anfitrión personalizado, ingrese el nombre de anfitrión del punto de conexión personalizado preferido. El nombre de anfitrión debe ser un nombre de dominio completo (FQDN), como www.yourdomain.com o example.yourdomain.com.

   > **Note**
   >
   > Si no dispone de un certificado comodín, es posible que necesite obtener un nuevo certificado para los subdominios del punto de conexión personalizado.

4. En Certificado de AWS, elija el certificado SSL que desee utilizar con el dominio. Si no hay certificados disponibles, puede importar uno a ACM o utilizar ACM para aprovisionar uno. Para más información, consulte Emisión y gestión de certificados en la Guía del usuario de Certificate Manager de AWS.

> **Note**
>
> El certificado debe tener el nombre del punto de conexión personalizado y debe estar en la misma cuenta que el dominio de OpenSearch Service. El estado del certificado debe ser EMITIDO.

- Siga el resto de pasos para crear el dominio y elija Crear.
- Seleccione el dominio, cuando se haya terminado de procesar, para ver el punto de conexión personalizado.

Para utilizar la CLI o la API de configuración, utilice las operaciones `CreateDomain` y `UpdateDomainConfig`. Para más información, consulte la AWS CLIReferencia de los comandos y la Referencia de API de Amazon OpenSearch Service.

Puntos de conexión personalizados para dominios existentes

Para agregar un punto de conexión personalizado a un dominio existente de OpenSearch Service, elija Editar y siga los pasos 2 a 4 anteriores.

Pasos siguientes

Después de habilitar un punto de conexión personalizado para el dominio de OpenSearch Service, debe crear un mapeo CNAME en Amazon Route 53 (o en el proveedor de servicios DNS preferido). Esto se hace para enrutar el tráfico al punto de conexión personalizado y sus subdominios. Sin este mapeo, el punto de conexión personalizado no funcionará. A fin de conocer los pasos para crear este mapeo en Route 53, consulte Configuración del enrutamiento de DNS para un nuevo dominio y Creación de una zona alojada para un subdominio. Para otros proveedores, consulte su documentación.

Cree un registro CNAME en el que el punto de conexión personalizado apunte al punto de conexión del dominio generado automáticamente. Si el dominio es de doble pila, puede apuntar su registro CNAME a cualquiera de los dos puntos de conexión generados por el servicio. La capacidad de doble pila del punto de conexión personalizado depende del punto de conexión generado por el servicio al que apunte el registro CNAME. El nombre de host del punto de conexión personalizado es el nombre del registro CNAME y el nombre de host del punto de conexión del dominio es el valor del registro CNAME.

Si utiliza Autenticación SAML para OpenSearch Dashboards, debe actualizar su IdP con la nueva URL de SSO.

Ajuste automático para Amazon OpenSearch Service

La función de ajuste automático en Amazon OpenSearch Service utiliza métricas de rendimiento y uso de un clúster de OpenSearch para sugerir cambios de configuración relacionados con la memoria, incluidos los tamaños de cola y caché y la configuración de máquina virtual Java (JVM) en los nodos. Estos cambios opcionales mejoran la velocidad y la estabilidad del clúster.

Algunos cambios se implementan inmediatamente, mientras que otros se programan durante la ventana de menor actividad de su dominio. Puede volver a la configuración predeterminada de OpenSearch Service en cualquier momento. A medida que la función de ajuste automático recopila y analiza las métricas de rendimiento del dominio, puede ver recomendaciones en la consola de OpenSearch Service en la página Notificaciones.

La función de ajuste automático está disponible en las Regiones de AWS comerciales para dominios que ejecutan cualquier versión de OpenSearch, o Elasticsearch 6.7 o posterior, con un tipo de instancia compatible.

Temas

Tipos de cambios

La función de ajuste automático cuenta con dos amplias categorías de cambios:

- Cambios no disruptivos que aplica a medida que se ejecuta el clúster.
- Cambios que requieren una implementación azul/verde, que se aplica durante el período de menor actividad del dominio.

Según las métricas de rendimiento del dominio, la función de ajuste automático puede sugerir realizar ajustes en las siguientes configuraciones:

Cambio de tipo	Categoría	Descripción
Tamaño de la pila de JVM	Azul/verde	De forma predeterminada, OpenSearch Service utiliza el 50 % de la RAM de una instancia para la pila de JVM, hasta un tamaño de 32 GiB. Aumentar este porcentaje proporciona más memoria a OpenSearch, pero deja menos memoria para el sistema operativo y otros procesos. Los valores más altos pueden disminuir el número de pausas de recolección de basura, pero pueden aumentar la amplitud de esas pausas.
Configuración de JVM de nueva generación	Azul/verde	La configuración de JVM de “nueva generación” afecta la frecuencia de recolecciones de basura menores. Las recolecciones menores más frecuentes pueden disminuir el número de recolecciones principales y pausas.
Tamaño de la cola	No disruptivo	De forma predeterminada, el tamaño de la cola de búsqueda es `1000` y el tamaño de la cola de escritura es `10000`. La función de ajuste automático escala automáticamente las colas de búsqueda y escritura si hay una pila adicional disponible para encargarse de las solicitudes.
Tamaño de caché	No disruptivo	La caché de campo monitorea las estructuras de datos en la pila, por lo que es importante monitorear el uso de la caché. La función de ajuste automático escala el tamaño de la caché de datos de campo para evitar problemas de memoria y con los interruptores de circuito. La caché de solicitudes de partición se administra a nivel del nodo y tiene un tamaño máximo predeterminado del 1 % de la pila. La función de ajuste automático escala el tamaño de la caché de solicitudes de partición para aceptar más solicitudes de búsqueda e índice de las que puede manejar el clúster configurado.
Solicitar tamaño	No disruptivo	De forma predeterminada, cuando el tamaño agregado de las solicitudes en vuelo supera el 10 % del total de JVM (2 % para

Cambio de tipo	Categoría	Descripción
		tipos de instancia `t2` y 1 % para `t3.small`), OpenSearch llimita toda nueva solicitud `_search` y `_bulk` hasta que se completen las solicitudes existentes. Auto-Tune ajusta automáticamente este umbral, normalmente entre el 5-15 %, basándose en la cantidad de JVM que está actualmente ocupada en el sistema. Por ejemplo, si la presión de la memoria de la JVM es alta, el ajuste automático podría reducir el umbral al 5%, momento en el que podría ver más rechazos hasta que el clúster se estabilice y el umbral aumente.

Habilitar o deshabilitar la función de ajuste automático

OpenSearch Service habilita la función de ajuste automático de forma predeterminada en nuevos dominios. Para habilitar o deshabilitar la función de ajuste automático en dominios existentes, recomendamos utilizar la consola, lo cual simplifica el proceso. Al habilitar la función de ajuste automático no se produce una implementación azul/verde.

Actualmente no se puede habilitar o desactivar la función de ajuste automático mediante AWS CloudFormation.

Consola

Para habilitar el ajuste automático en un dominio existente

1. Abra la consola de Amazon OpenSearch Service enhttps://console.aws.amazon.com/aos/home.
2. En el panel de navegación, en Dominios, elija el nombre del dominio para abrir la configuración del clúster.
3. Seleccione Activar si el ajuste automático aún no está activado.
4. Si lo desea, seleccione Ventana de menor actividad para programar las optimizaciones que requieran una implementación azul/verde durante la ventana de menor actividad configurada en el dominio. Para obtener más información, consulte the section called “Programar mejoras de ajuste automático”.
5. Elija Guardar cambios.

CLI

Para habilitar el ajuste automático mediante el AWS CLI, envíe una solicitud UpdateDomainConfig:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options DesiredState=ENABLED
```

Programar mejoras de ajuste automático

Antes del 16 de febrero de 2023, ajuste automático utilizaba ventanas de mantenimiento para programar los cambios que requerían una implementación azul/verde. Las ventanas de mantenimiento ahora están en desuso en favor de los períodos de menor actividad, que es un bloque de tiempo diario de 10 horas durante el cual su dominio suele experimentar poco tráfico. Puede modificar la hora de inicio predeterminada para la ventana de menor actividad, pero no puede modificar la duración.

Todos los dominios que tenían habilitados los períodos de mantenimiento de ajuste automático antes de la introducción de las ventanas de menor actividad el 16 de febrero de 2023 pueden seguir utilizando las ventanas de mantenimiento antiguas sin interrupciones. Sin embargo, le recomendamos que migre sus dominios actuales para utilizar en su lugar la ventana de menor actividad para el mantenimiento de los dominios. Para obtener instrucciones, consulte the section called “Migración desde los intervalos de mantenimiento de ajuste automático”.

Consola

Para programar las acciones de ajuste automático, en las ventanas de menor actividad

1. Abra la consola de Amazon OpenSearch Service enhttps://console.aws.amazon.com/aos/home.
2. En el panel de navegación, en Dominios, elija el nombre del dominio para abrir la configuración del clúster.
3. Vaya a la pestaña Ajuste automático y seleccione Editar.
4. Seleccione Activar si el ajuste automático aún no está activado.
5. En Programar optimizaciones durante la ventana de menor actividad, seleccione Ventana de menor actividad.
6. Elija Guardar cambios.

CLI

Para configurar su dominio para programar acciones de ajuste automático durante la ventana de menor actividad configurada, incluya `UseOffPeakWindow` en la solicitud UpdateDomainConfig:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --auto-tune-options
 DesiredState=ENABLED,UseOffPeakWindow=true,MaintenanceSchedules=null
```

Supervisión de cambios de ajuste automático

Puede supervisar las estadísticas de ajuste automático en Amazon CloudWatch. Para obtener una lista completa de las métricas, consulte the section called “Métricas de ajuste automático”.

OpenSearch Service envía eventos de ajuste automático a Amazon EventBridge. Puede utilizar EventBridge para configurar reglas que envíen un correo electrónico o realicen una acción específica cuando se reciba un evento. Para ver el formato de cada evento de ajuste automático enviado a EventBridge, consulte. the section called “Eventos de ajuste automático”

Etiquetado de dominios de Amazon OpenSearch Service

Las etiquetas te permiten asignar información arbitraria a un dominio de Amazon OpenSearch Service para que puedas categorizar y filtrar esa información. Una etiqueta es un par clave-valor que se define y se asocia a un OpenSearch dominio de servicio. Puede usar estas etiquetas para realizar un seguimiento de los costos agrupando los gastos de los recursos etiquetados de manera similar. AWS no aplica ningún significado semántico a tus etiquetas. Las etiquetas se interpretan estrictamente como cadenas de caracteres. Todas las etiquetas presentan los siguientes elementos:

Elemento de etiqueta	Descripción	Obligatorio
Clave de etiqueta	La clave de la etiqueta es el nombre de la etiqueta. La clave debe ser exclusiva del dominio del OpenSearch servicio al que está asociada. Para obtener una lista de restricciones básicas relativas a las claves y valores de las etiquetas, consulte Restricciones de las etiquetas definidas por el usuario.	Sí

Elemento de etiqueta	Descripción	Obligatorio
Valor de etiqueta	El valor de etiqueta es un valor de cadena en la etiqueta. Los valores de etiquetas pueden ser `null` y no tienen que ser únicos dentro de un conjunto de etiquetas. Por ejemplo, puede tener un par valor de clave en un conjunto de etiquetas en proyecto/Trinity y centro-de-costes/Trinity. Para obtener una lista de restricciones básicas relativas a las claves y valores de las etiquetas, consulte Restricciones de las etiquetas definidas por el usuario.	No

Cada dominio OpenSearch de servicio tiene un conjunto de etiquetas, que contiene todas las etiquetas asignadas a ese dominio OpenSearch de servicio. AWS no asigna automáticamente ninguna etiqueta a los dominios OpenSearch de servicio. Un conjunto de etiquetas puede contener entre 0 y 50 etiquetas. Si agrega una etiqueta a un dominio con la misma clave que una etiqueta existente en un recurso, el nuevo valor sobrescribirá el antiguo.

Ejemplos de etiquetas

Puede utilizar una clave para definir una categoría, y el valor podría ser un elemento dentro de esa categoría. Por ejemplo, puede definir una clave de etiqueta `project` y un valor de etiqueta de`Salix`, que indiquen que el dominio de OpenSearch servicio está asignado al proyecto de Salix. También puede usar etiquetas para designar los dominios de OpenSearch servicio que se utilizan para pruebas o producción mediante una clave como `environment=test` o`environment=production`. Intente utilizar un conjunto coherente de claves de etiquetas para facilitar el seguimiento de los metadatos asociados a los dominios OpenSearch de servicio.

También puedes usar etiquetas para organizar tu AWS factura y reflejar tu propia estructura de costos. Para ello, regístrate para recibir tu Cuenta de AWS factura con los valores clave de las etiquetas incluidos. A continuación, para ver los costes de los recursos combinados, organice la información de facturación de acuerdo con los recursos que tienen los mismos valores de clave de etiqueta. Por ejemplo, puedes etiquetar varios dominios de OpenSearch servicio con pares clave-valor y, a continuación, organizar la información de facturación para ver el coste total de cada dominio en varios servicios. Para obtener más información, consulte Uso de etiquetas de asignación de costos en la documentación de administración de costos y facturación deAWS .

> **Note**
>
> Las etiquetas se almacenan en caché con fines de autorización. Por este motivo, es posible que las adiciones y actualizaciones de las etiquetas OpenSearch de los dominios de servicio tarden varios minutos en estar disponibles.

Uso de etiquetas (consola)

La consola es la forma más sencilla de etiquetas de un dominio.

Para crear una etiqueta (consola)

1. Visite https://aws.amazon.com y, a continuación, seleccione Iniciar sesión en la consola.
2. En Analytics, selecciona Amazon OpenSearch Service.
3. Seleccione el dominio al que desee agregar etiquetas y vaya a la pestaña Tags (Etiquetas).
4. Seleccione Administrar y Add new tag (Agregar nueva etiqueta).
5. Introduzca una clave de etiqueta y un valor opcional.
6. Seleccione guardar.

Para eliminar una etiqueta, siga los mismos pasos y elija Quitar en la página Administrar etiquetas.

Para obtener más información sobre cómo utilizar la consola para trabajar con etiquetas, consulte Tag Editor en la Guía de introducción a la consola de administración deAWS .

Uso de etiquetas (AWS CLI)

Puede crear etiquetas de recursos mediante el AWS CLI --add-tags comando with.

Sintaxis

```
add-tags --arn=<domain_arn> --tag-list Key=<key>,Value=<value>
```

Parámetro	Descripción
`--arn`	Nombre de recurso de Amazon para el dominio de OpenSearch servicio al que se adjunta la etiqueta.

Parámetro	Descripción
`--tag-list`	Conjunto de pares de clave-valor separados por espacios con el siguiente formato: `Key=<key>,Value=<value>`

Ejemplo

En el siguiente ejemplo se crean dos etiquetas para el dominio registros:

```
aws opensearch add-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-list
 Key=service,Value=OpenSearch Key=instances,Value=m3.2xlarge
```

Puede eliminar etiquetas de un dominio OpenSearch de servicio mediante el --remove-tags comando.

Sintaxis

```
remove-tags --arn=<domain_arn> --tag-keys Key=<key>,Value=<value>
```

Parámetro	Descripción
`--arn`	Nombre de recurso de Amazon (ARN) para el dominio de OpenSearch servicio al que está asociada la etiqueta.
`--tag-keys`	Conjunto de pares clave-valor separados por espacios que desea eliminar del dominio del servicio. OpenSearch

Ejemplo

En el siguiente ejemplo se eliminan dos etiquetas del dominio logs que se crearon en el ejemplo anterior:

```
aws opensearch remove-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs --tag-
keys service instances
```

Puede ver las etiquetas existentes de un dominio de OpenSearch servicio con el comando: --list-tags

Sintaxis

```
list-tags --arn=<domain_arn>
```

Parámetro	Descripción
`--arn`	Nombre de recurso de Amazon (ARN) para el dominio de OpenSearch servicio al que se adjuntan las etiquetas.

Ejemplo

En el siguiente ejemplo se muestran todas las etiquetas de recursos del dominio logs:

```
aws opensearch list-tags --arn arn:aws:es:us-east-1:379931976431:domain/logs
```

Trabajar con etiquetas (AWS SDK)

AWS Los SDK (excepto los de Android e iOS) admiten todas las acciones definidas en la referencia de la API de Amazon OpenSearch Service, incluidas las `AddTags` operaciones `ListTags` y`RemoveTags`. Para obtener más información sobre la instalación y el uso de los AWS SDK, consulte los kits de desarrollo de AWS software.

Python

En este ejemplo, se utiliza el cliente Python de OpenSearchServicebajo nivel del SDK de AWS para Python (Boto) para añadir una etiqueta a un dominio, enumerar la etiqueta adjunta al dominio y eliminar una etiqueta del dominio. Debe proporcionar valores para `DOMAIN_ARN`, `TAG_KEY` y `TAG_VALUE`.

```
import boto3
from botocore.config import Config  # import configuration

DOMAIN_ARN = ''  # ARN for the domain. i.e "arn:aws:es:us-east-1:123456789012:domain/
my-domain
TAG_KEY = ''  # The name of the tag key. i.e 'Smileyface'
TAG_VALUE = ''  # The value assigned to the tag. i.e 'Practicetag'

# defines the configurations parameters such as region

my_config = Config(region_name='us-east-1')
```

```
client = boto3.client('opensearch', config=my_config)


# defines the client variable

def addTags():
    """Adds tags to the domain"""

    response = client.add_tags(ARN=DOMAIN_ARN,
                               TagList=[{'Key': TAG_KEY,
                                         'Value': TAG_VALUE}])

    print(response)


def listTags():
    """List tags that have been added to the domain"""

    response = client.list_tags(ARN=DOMAIN_ARN)
    print(response)


def removeTags():
    """Remove tags that have been added to the domain"""

    response = client.remove_tags(ARN=DOMAIN_ARN, TagKeys=[TAG_KEY])

    print('Tag removed')
    return response
```

Realizar acciones administrativas en los dominios OpenSearch de Amazon Service

Amazon OpenSearch Service ofrece varias opciones administrativas que proporcionan un control detallado si necesitas solucionar problemas con tu dominio. Estas opciones incluyen la posibilidad de reiniciar el OpenSearch proceso en un nodo de datos y la posibilidad de reiniciar un nodo de datos.

OpenSearch El servicio monitorea los parámetros de estado de los nodos y, cuando hay anomalías, toma medidas correctivas para mantener la estabilidad de los dominios. Con las opciones administrativas para reiniciar el OpenSearch proceso en un nodo y reiniciar el propio nodo, usted tiene el control de algunas de estas acciones de mitigación.

Puede usar el AWS Management Console, el AWS CLI, o el AWS SDK para realizar estas acciones. En las siguientes secciones, se explica cómo realizar estas acciones con la consola.

Reinicie el OpenSearch proceso en un nodo

Para reiniciar el OpenSearch proceso en un nodo

1. Diríjase a la consola de OpenSearch servicio enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios. Elija el nombre del dominio con el que desea trabajar.
3. Cuando se abra la página de detalles del dominio, vaya a la pestaña Estado de la instancia.
4. En Nodos de datos, seleccione el botón situado junto al nodo en el que desea reiniciar el proceso.
5. Selecciona el menú desplegable Acciones y selecciona Reiniciar el proceso de OpenSearch / Elasticsearch.
6. Seleccione Confirmar en el modal.
7. Para ver el estado de la acción que ha iniciado, seleccione el nombre del nodo. Cuando se abra la página de detalles del nodo, seleccione la pestaña Eventos situada debajo del nombre del nodo para ver una lista de los eventos asociados a ese nodo.

Reinicie un nodo de datos

Para reiniciar un nodo de datos

1. Diríjase a la consola de servicio en OpenSearch . https://console.aws.amazon.com/aos/
2. En el panel de navegación izquierdo, seleccione Dominios. Elija el nombre del dominio con el que desea trabajar.
3. Cuando se abra la página de detalles del dominio, vaya a la pestaña Estado de la instancia.
4. En Nodos de datos, seleccione el botón situado junto al nodo en el que desea reiniciar el proceso.
5. Seleccione el menú desplegable Acciones y elija Nodo de reinicio.
6. Seleccione Confirmar en el modal.
7. Para ver el estado de la acción que ha iniciado, seleccione el nombre del nodo. Cuando se abra la página de detalles del nodo, seleccione la pestaña Eventos situada debajo del nombre del nodo para ver una lista de los eventos asociados a ese nodo.

Reinicie el proceso Dashboard o Kibana en un nodo

Para reiniciar el proceso Dashboard o Kibana en un nodo

1. Diríjase a la consola de OpenSearch servicio enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios. Elija el nombre del dominio con el que desea trabajar.
3. Cuando se abra la página de detalles del dominio, vaya a la pestaña Estado de la instancia.
4. En Nodos de datos, seleccione el botón situado junto al nodo en el que desea reiniciar el proceso.
5. Seleccione el menú desplegable Acciones y elija Reiniciar el proceso Dashboard/Kibana.
6. Seleccione Confirmar en el modal.
7. Para ver el estado de la acción que ha iniciado, seleccione el nombre del nodo. Cuando se abra la página de detalles del nodo, seleccione la pestaña Eventos situada debajo del nombre del nodo para ver una lista de los eventos asociados a ese nodo.

Limitaciones

Las opciones administrativas presentan las siguientes limitaciones:

- Las opciones administrativas se admiten en las versiones 7.x y superiores de Elasticsearch.
- Las opciones administrativas no admiten dominios con Multi-AZ con modo de espera activado.
- El reinicio del proceso OpenSearch y Elasticsearch se admite en dominios con tres o más nodos de datos.
- La compatibilidad con los procesos de Dashboards y Kibana se admite en dominios con dos o más nodos de datos.
- Para reiniciar el OpenSearch proceso en un nodo o reiniciar un nodo, el dominio no debe estar en estado rojo y todos los índices deben tener las réplicas configuradas.

Uso de consultas directas OpenSearch de Amazon Service con Amazon S3 (versión preliminar)

⚠ Esta es una documentación preliminar para las consultas directas de Amazon OpenSearch Service con Amazon S3, que se encuentra en versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio deAWS.

Puede utilizar las consultas directas OpenSearch de Amazon Service para consultar datos en Amazon S3. Amazon OpenSearch Service proporciona una integración de consultas directas con Amazon S3 para analizar los registros operativos en Amazon S3 y los lagos de datos basados en Amazon S3 sin tener que cambiar de servicio. Ahora puede analizar los datos en almacenes de objetos en la nube y, al mismo tiempo, utilizar los análisis operativos y las visualizaciones de Service. OpenSearch

Con las consultas directas con Amazon S3, ya no necesita crear canalizaciones de ETL complejas ni incurrir en el gasto de duplicar datos tanto en el almacenamiento de Amazon S3 como en el de OpenSearch Service. También puede instalar integraciones de plantillas de tipo registro populares que incluyen paneles predefinidos y configurar aceleraciones de datos adaptadas a ese tipo de registro. Las plantillas incluyen registros de flujo de VPC, registros deAWS CloudTrail y registros de Amazon S3. Las aceleraciones incluyen la omisión de índices, las vistas materializadas y los índices cubiertos.

Temas

- Eliminar una fuente OpenSearch de datos de Amazon Service con Amazon S3

Precios

Usted paga por los recursos de Amazon S3 y OpenSearch Service existentes que se utilizan para crear y procesar consultas directas. Las consultas que se envían a Amazon S3 utilizan cómputo facturable y se muestran como unidades de OpenSearch cómputo (OCU) por hora.

Las consultas directas con Amazon S3 son de dos tipos: interactivas y de mantenimiento de índices. Las consultas interactivas realizan análisis de sus datos en Amazon S3. Cuando ejecuta una consulta nueva, OpenSearch Service inicia una nueva sesión que dura un mínimo de diez minutos. OpenSearch El servicio mantiene la sesión activa para garantizar que las consultas posteriores se ejecuten rápidamente. Las consultas de mantenimiento de índices utilizan la computación para mantener los índices en el OpenSearch Servicio. Estas consultas suelen tardar más porque incorporan una cantidad de datos configurable al OpenSearch Servicio para que las consultas interactivas se ejecuten más rápido.

Para obtener más información, consulta los precios OpenSearch de Amazon Service.

Limitaciones

Las siguientes limitaciones se aplican a las consultas directas del OpenSearch servicio con Amazon S3.

- Su OpenSearch dominio debe ser de la versión 2.11 o posterior para admitir las consultas directas OpenSearch del Servicio.
- OpenSearch Las consultas directas de servicio con Amazon S3 solo admiten las tablas de Spark incluidas en AWS Glue Data Catalog. Las tablas de Hive no admiten la transmisión de Spark, que es necesaria para mantener los índices actualizados.
- Algunos tipos de datos no son compatibles. Los tipos de datos admitidos se limitan a Parquet, CSV y JSON.
- AWS CloudFormation las plantillas no se admiten en la versión preliminar de las consultas directas.
- Tu OpenSearch dominio y AWS Glue Data Catalog deben estar en el mismo dominio Cuenta de AWS. Sus tablas de Amazon S3 pueden estar en una cuenta diferente, pero deben estar en la misma Región de AWS que su dominio.

- Las estructuras anidadas de Spark no son compatibles. Si los datos de origen utilizan estructuras anidadas, debe dividirlas en filas.
- No se admiten las tablas creadas a través de Athena.
- Las columnas que faltan pueden requerir el uso de la función `COALESCE` SQL para devolver los resultados.
- No está disponible en OpenSearch Serverless
- Los datos se deben aplanar antes de realizar la consulta o se debe utilizar SQL in OpenSearch Service para convertir las columnas anidadas en columnas dedicadas.

Cuotas

Su cuenta tiene las siguientes cuotas relacionadas con las consultas directas del OpenSearch servicio con Amazon S3. Cada vez que inicia una consulta, OpenSearch Service abre una sesión y la mantiene activa durante al menos diez minutos. Esto reduce la latencia de las consultas al eliminar el tiempo de inicio de la sesión en las consultas posteriores.

Descripción	Máximo
Conexiones por dominio	20
Origen de datos por dominio	20
Índices por dominio	50
Sesiones simultáneas por origen de datos	100

Regiones admitidas

Las siguientes regiones están disponibles para consultas directas de OpenSearch servicio con Amazon S3: Asia-Pacífico (Tokio), Europa (Fráncfort), Europa (Irlanda), EE.UU. Este (Norte de Virginia), EE.UU. Este (Ohio) y EE.UU. Oeste (Oregón).

Creación de integraciones de fuentes de datos de Amazon OpenSearch Service con Amazon S3

⚠ Esta es una documentación preliminar para las consultas directas de Amazon OpenSearch Service con Amazon S3, que se encuentra en versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio deAWS.

Puede crear una nueva fuente de datos de consulta directa de Amazon S3 para OpenSearch Service a través de la API AWS Management Console o la API. Cada nueva fuente de datos la utiliza AWS Glue Data Catalog para administrar las tablas que representan los buckets de Amazon S3.

Temas

Requisitos previos

Antes de crear un origen de datos, debe tener lo siguiente:

- Un OpenSearch dominio con la versión 2.11 o posterior

Para obtener instrucciones sobre cómo configurarlos, consulte the section called “ Creación de dominios OpenSearch de servicio” e Introducción al AWS Glue Data Catalog.

Permisos necesarios

Para crear un origen de datos, su usuario o rol debe tener adjunta una política basada en identidades con los permisos de IAM adecuados. El siguiente ejemplo de política muestra los permisos con

privilegios mínimos necesarios para crear y administrar un origen de datos. Tenga en cuenta que si tiene permisos más generales, como `s3:*` o la política de `AdministratorAccess`, estos engloban los permisos con privilegios mínimos de la política de ejemplo.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "es:ESHttp*",
                "es:AddDataSource",
                "es:DeleteDataSource",
                "es:GetDataSource",
                "es:ListDataSource",
                "es:UpdateDataSource",
                "s3:Get*",
                "s3:List*",
                "s3:Put*",
                "s3:Describe*",
                "glue:*"
            ],
            "Resource": [
                "arn:aws:s3:::bucket-name",
                "arn:aws:s3:::bucket-name/*",
                "arn:aws:glue:us-east-1:{aws-account-id}:database/*"
            ]
        },
        {
            "Sid": "GlueCreateAndReadDataCatalog",
            "Effect": "Allow",
            "Action": [
                "glue:GetDatabase",
                "glue:CreateDatabase",
                "glue:GetDatabases",
                "glue:CreateTable",
                "glue:GetTable",
                "glue:UpdateTable",
                "glue:DeleteTable",
                "glue:GetTables",
                "glue:GetPartition",
                "glue:GetPartitions",
                "glue:CreatePartition",
```

```
                "glue:BatchCreatePartition",
                "glue:GetUserDefinedFunctions"
            ],
            "Resource": "*"
        }
    ]
}
```

El rol debe tener la siguiente política de confianza, que especifica el ID de destino.

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

Para obtener instrucciones sobre cómo crear los roles, consulte Creación de un rol mediante políticas de confianza personalizadas.

Si ha activado el control de acceso detallado, se creará automáticamente un nuevo rol de control OpenSearch de acceso detallado para la fuente de datos. <name of data source>El nombre de la nueva función de control de acceso detallada será _. AWSOpenSearchDirectQuery

De forma predeterminada, el rol solo tiene acceso a los índices de fuentes de datos de consulta directa. Si bien puede configurar el rol para limitar o conceder el acceso a su fuente de datos, se recomienda no ajustar el acceso de este rol. Si elimina la fuente de datos, se eliminará este rol. Esto eliminará el acceso de los demás usuarios si están asignados al rol.

Asigne el AWS Glue Data Catalog rol (si el control de acceso detallado está habilitado después de crear la fuente de datos)

Si ha habilitado un control de acceso detallado después de crear una fuente de datos, debe asignar a los usuarios que no sean administradores a una función de IAM con AWS Glue Data Catalog acceso

para poder ejecutar consultas directas. Para crear manualmente un rol de `glue_access` backend que pueda asignar al rol de IAM, siga estos pasos:

> **Note**
>
> Los índices se utilizan para cualquier consulta realizada en el origen de datos. Un usuario con acceso de lectura al índice de solicitudes de un origen de datos determinado puede leer todas las consultas realizadas en ese origen de datos. Un usuario con acceso de lectura al índice de resultados puede leer los resultados de todas las consultas realizadas en ese origen de datos.

1. En el menú principal de los OpenSearch paneles, seleccione Seguridad, Funciones y Crear funciones.
2. Asigne el rol glue_access.
3. En Permisos de clúster, seleccione `indices:data/write/bulk*`, `indices:data/read/scroll`, `indices:data/read/scroll/clear`.
4. En Índice, introduzca los siguientes índices a los que quiere conceder acceso al usuario con el rol:
   - `.query_execution_request_`*`<name of data source>`*
   - `query_execution_result_`*`<name of data source>`*
   - `flint_*`
5. En Permisos de índice, seleccione `indices_all`.
6. Seleccione Crear.
7. Seleccione Usuarios asignados, Administrar mapeo.
8. En Roles de backend, agregue el ARN del rol de AWS Glue que necesita permiso para llamar a su dominio.

   ```
   arn:aws:iam::account-id:role/role-name
   ```
9. Seleccione Asignar y confirme que el rol aparece en Usuarios asignados.

Para obtener más información sobre la asignación de roles, consulte the section called “Mapear roles a usuarios”.

Configuración de un nuevo origen de datos de consulta directa

Puede configurar una fuente de datos de consulta directa en un dominio con la API de servicio AWS Management Console o con la OpenSearch API.

AWS Management Console

1. Dirígete a la consola OpenSearch de Amazon Service enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios.
3. Seleccione el dominio para el que desea configurar un nuevo origen de datos. Se abrirá la página de detalles del dominio. Seleccione la pestaña Conexiones que aparece debajo de los detalles generales del dominio y busque la sección Consulta directa.
4. Seleccione Crear.
5. En la página de creación del origen de datos, introduzca un nombre para el nuevo origen de datos. En Tipo de origen de datos, elija Amazon S3. Elija un rol de IAM existente que tenga limitaciones en cuanto a lo que se puede acceder en Amazon S3 AWS Glue Data Catalog y en Amazon S3.
6. Seleccione Crear. Esto abre la pantalla de detalles de la fuente de datos con una URL de OpenSearch Dashboards. Puede navegar hasta esta URL para completar los siguientes pasos.

OpenSearch API de servicio

Utilice la operación de la AddDataSourceAPI para crear una nueva fuente de datos en su dominio.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource

{
   "DataSourceType": {
        "s3GlueDataCatalog": {
            "RoleArn": "arn:aws:iam::account-id:role/Admin"
        }
    }
   "Description": "data-source-description",
   "Name": "my-data-source"
}
```

Siguientes pasos

Después de crear una fuente de datos, OpenSearch Service le proporciona una URL de OpenSearch Dashboards. Se usa para configurar el control de acceso, definir tablas, configurar paneles basados en tipos de registro para los tipos de registro más populares y consultar sus datos.

Configurar la fuente de datos en Dashboards OpenSearch

⚠ Esta es una documentación preliminar para las consultas directas de Amazon OpenSearch Service con Amazon S3, que se encuentra en versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio deAWS.

Ahora que ha creado su origen de datos, puede configurar los ajustes de seguridad, definir las tablas de Amazon S3 o configurar la indexación acelerada de datos. En esta sección, se explican varios casos de uso de la fuente de datos en los OpenSearch paneles de control antes de realizar consultas sobre los datos.

Para configurar las siguientes secciones, primero debe navegar hasta su fuente de datos en los OpenSearch paneles. En el menú de navegación izquierdo, en Administración, elija Origen de datos. En Administrar orígenes de datos, seleccione el nombre del origen de datos que creó en la consola.

Configurar el control de acceso

En la página de detalles de su origen de datos, busque la sección Controles de acceso y elija Editar. Si tiene el complemento de seguridad instalado, elija Restringido y seleccione los grupos basados en roles a los que desea proporcionar acceso al nuevo origen de datos. También puede elegir Solo administrador si solo quiere que el administrador tenga acceso al origen de datos.

⚠ Important

Tenga en cuenta que los índices se utilizan para cualquier consulta sobre el origen de datos, por lo que un usuario con acceso de lectura al índice de solicitudes de un origen de datos determinado puede leer todas las consultas sobre ese origen de datos, y un usuario con

acceso de lectura al índice de resultados puede leer los resultados de todas las consultas sobre ese origen de datos.

Defina tablas AWS Glue Data Catalog

Las consultas directas de OpenSearch Service a Amazon S3 utilizan las tablas de Spark incluidas en AWS Glue Data Catalog. Puedes usar una Rastreador de AWS Glue para rastrear tus datos, lo que creará una tabla para ti. Como alternativa, puede crear tablas manualmente desde Query Workbench.

Para administrar las bases de datos y tablas existentes en el origen de datos, o para crear tablas nuevas en las que desee utilizar consultas directas, elija la opción Definir tablas en la página de detalles del origen de datos. Esto lo dirigirá a la página del complemento Query Workbench.

Para configurar una tabla con datos de ejemplo que pueda explorar y usar para las aceleraciones en la siguiente sección, ejecute la siguiente consulta:

```
CREATE EXTERNAL TABLE IF NOT EXISTS datasourcename.gluedatabasename.gluetablename (
   `@timestamp` TIMESTAMP,
    clientip STRING,
    request STRING,
    status INT,
    size INT,
    year INT,
    month INT,
    day INT)
USING json PARTITIONED BY(year, month, day) OPTIONS (path 's3://my-bucket/data/
http_log', compression 'bzip2')
```

Tras crear la tabla, ejecute la siguiente consulta para asegurarse de que es compatible con las consultas directas:

```
MSCK REPAIR TABLE datasourcename.databasename.tablename
```

Aceleración de sus consultas

En la página de detalles de su origen de datos, elija la opción Acelerar el rendimiento. Para garantizar una experiencia rápida con sus datos en Amazon S3, hay tres tipos diferentes de

aceleraciones que puede configurar para OpenSearch indexar los datos en el servicio: omite los índices, las vistas materializadas y cubre los índices.

Índices de omisión

Con un índice de omisión, puede indexar solo los metadatos de los datos almacenados en Amazon S3. Cuando consulta una tabla con un índice de omisión, el planificador de consultas hace referencia al índice y vuelve a escribir la consulta para localizar los datos de manera eficiente, en lugar de escanear todas las particiones y archivos. Esto permite que el índice de omisión reduzca rápidamente la ubicación específica de los datos almacenados.

Cuando configure las tablas de Spark que utilizará desde AWS Glue Data Catalog, OpenSearch Dashboards le preguntará si desea crear índices de omisión en sus tablas. Ahí puede crear un índice de omisión o puede crear uno con el caso práctico de Acelerar el rendimiento cuando termine de configurar la tabla.

```
CREATE SKIPPING INDEX
ON datasourcename.gluedatabasename.gluetablename
(
    year PARTITION,
    month PARTITION,
    day PARTITION,
    hour PARTITION
)
```

Vistas materializadas

Con las vistas materializadas, puede utilizar consultas complejas, como las agregaciones, para alimentar las visualizaciones del panel. Las vistas materializadas incorporan una pequeña cantidad de sus datos al almacenamiento del Servicio. OpenSearch OpenSearch Luego, Service forma un índice a partir de los datos ingeridos que puede usar para las visualizaciones. Puede gestionar el índice de vistas materializadas con élthe section called “Index State Management”, del mismo modo que lo haría con cualquier otro índice. OpenSearch

Utilice la siguiente consulta para crear una nueva vista materializada para la tabla `http_logs` que creó en the section called “Defina tablas AWS Glue Data Catalog”:

```
CREATE MATERIALIZED VIEW datasourcename.gluedatabasename.viewname_view
AS
  SELECT
```

```
    window.start AS `start.time`,
    COUNT(*) AS count
  FROM datasourcename.gluedatabasename.gluetablename
  WHERE status != 200
  GROUP BY TUMBLE(`@timestamp`, '1 Minutes')
WITH (
  auto_refresh = true,
  refresh_interval = '1 Minutes',
  checkpoint_location = 's3://my-bucket/data/http_log/checkpoint_http_count_view',
  watermark_delay = '10 Minutes'
);
```

Índices de cobertura

Con un índice de cobertura, puede incorporar datos de una columna especificada en una tabla. Este es el más eficaz de los tres tipos de indexación. Como OpenSearch Service ingiere todos los datos de la columna deseada, usted obtiene un mejor rendimiento y puede realizar análisis avanzados.

Al igual que con las vistas materializadas, OpenSearch Service crea un nuevo índice a partir de los datos del índice de cobertura. Puede usar este nuevo índice para las visualizaciones del panel de control y otras funciones del OpenSearch Servicio, como la detección de anomalías o las capacidades geoespaciales. Puede gestionar el índice de vistas de portada con élthe section called "Index State Management", del mismo modo que lo haría con cualquier otro índice. OpenSearch

Utilice la siguiente consulta para crear un nuevo índice de cobertura para la tabla `http_logs` que creó en the section called "Defina tablas AWS Glue Data Catalog":

```
CREATE INDEX status_clientip_and_day
ON datasourcename.gluedatabasename.gluetablename ( status, day, clientip )
WITH (
  auto_refresh = true,
  refresh_interval = '5 minute',
  checkpoint_location = 's3://my-bucket/data/http_log/checkpoint_status_and_day'
)
```

Consulta de datos en los paneles OpenSearch

> ⚠ Esta es una documentación preliminar para las consultas directas de Amazon OpenSearch Service con Amazon S3, que se encuentra en versión preliminar. Tanto la documentación

como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio deAWS.

Después de configurar las tablas y configurar la aceleración de consultas opcional deseada, ya puede empezar a realizar el análisis de sus datos. Para consultar sus datos, seleccione la fuente de datos en el menú desplegable de la página de descubrimiento o de la página de observabilidad en los paneles de control. OpenSearch

Si utiliza un índice de omisión o no ha creado uno, puede utilizar SQL o el lenguaje de procesamiento de canalizaciones (PPL) para consultar los datos. Si ha configurado una vista materializada o un índice de cobertura, ya tiene un índice y puede usar el lenguaje de consultas de Dashboards (DQL) en todo Dashboards. También puede usar PPL con el complemento Observabilidad y SQL con el complemento Query Workbench. Actualmente, solo los complementos Observabilidad y Query Workbench admiten PPL y SQL.

SQL

Utilice la siguiente consulta para ejecutar una consulta de SQL de ejemplo para la tabla `http_logs` que creó en the section called “Defina tablas AWS Glue Data Catalog”:

```
SELECT
    FIRST(day) AS day,
    status,
    COUNT(status) AS status_count_by_day
FROM datasourcename.gluedatabasename.gluetablename
WHERE status >= 400
GROUP BY day, status
ORDER BY day, status
LIMIT 20;
```

PPL

Utilice la siguiente consulta para ejecutar una consulta de PPL de ejemplo para la tabla `http_logs` que creó en the section called “Defina tablas AWS Glue Data Catalog”:

```
source = datasourcename.gluedatabasename.gluetablename |
```

```
where status = 500 | sort - clientip, @timestamp | head 20
```

Eliminar una fuente OpenSearch de datos de Amazon Service con Amazon S3

> ⚠ Esta es una documentación preliminar para las consultas directas de Amazon OpenSearch Service con Amazon S3, que se encuentra en versión preliminar. Tanto la documentación como la característica quedan sujetas a cambios. Se recomienda utilizar esta característica solo en entornos de prueba y no en entornos de producción. Para conocer los términos y condiciones de las versiones preliminares, consulte Betas y versiones preliminares en Términos de servicio deAWS.

Cuando eliminas una fuente de datos, Amazon OpenSearch Service la elimina de tu dominio. OpenSearch El servicio también elimina los índices asociados a la fuente de datos. Sus datos transaccionales no se eliminan de Amazon S3, pero Amazon S3 no envía nuevos datos a OpenSearch Service.

Puede eliminar la integración de una fuente de datos mediante la API AWS Management Console o la API del OpenSearch servicio.

AWS Management Console

Eliminación de un origen de datos

1. Dirígete a la consola OpenSearch de Amazon Service enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios.
3. Seleccione el dominio del que desea eliminar un origen de datos. Se abrirá la página de detalles del dominio. Elija la pestaña Conexiones que se encuentra debajo de la información general, y busque la sección Consulta directa.
4. Seleccione el origen de datos que desea eliminar, elija Eliminar y confirme la eliminación.

OpenSearch API de servicio

Utilice la operación DeleteDataSourceAPI para eliminar una fuente de datos existente en su dominio.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/domain/domain-name/
dataSource/data-source-name
```

Supervisión de dominios Amazon OpenSearch Service

El monitoreo es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de Amazon OpenSearch Service y de las demás soluciones de AWS. AWS proporciona las siguientes herramientas para monitorear sus recursos de OpenSearch Service, informar de los problemas y tomar acciones automáticas cuando sea necesario:

Amazon CloudWatch

Amazon CloudWatch monitorea los recursos de OpenSearch Service en tiempo real. Puede recopilar métricas y realizar un seguimiento de ellas, crear paneles personalizados y definir alarmas que realizan advertencias o acciones cuando una métrica alcanza el umbral que se especifique. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Registros de Amazon CloudWatch

Amazon CloudWatch Logs permite monitorear, almacenar y acceder a sus archivos de registro de OpenSearch. CloudWatch Logs monitorea la información de los archivos de registro y puede notificarlo cuando se alcanzan ciertos umbrales. Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch Logs.

Amazon EventBridge

Amazon EventBridge ofrece un flujo casi en tiempo real de eventos del sistema que describen los cambios en sus dominios de OpenSearch Service. Puede crear reglas que vigilen determinados eventos y desencadenen acciones automatizadas en otros servicios de AWS cuando estos eventos se produzcan. Para obtener más información, consulte la Guía del usuario de Amazon EventBridge.

AWS CloudTrail

AWS CloudTrail captura las llamadas de la API de configuración realizadas a OpenSearch Service como eventos. Puede entregar estos eventos al bucket de Amazon S3 que se especifique. Mediante esta información, puede identificar qué usuarios y cuentas realizaron solicitudes, la dirección IP fuente desde la que se realizaron las solicitudes y cuándo se produjeron. Para obtener más información, consulte la Guía del usuario de AWS CloudTrail.

Temas

- Monitoreo de registros de OpenSearch con Registros de Amazon CloudWatch
- Supervisión de los registros de auditoría en Amazon OpenSearch Service
- Monitorización OpenSearch de eventos del servicio con Amazon EventBridge
- Monitoreo de las llamadas a la API de Amazon OpenSearch Service con AWS CloudTrail

Monitoreo de métricas del clúster de OpenSearch con Amazon CloudWatch

Amazon OpenSearch Service publica datos de sus dominios en Amazon CloudWatch. CloudWatch permite recuperar las estadísticas sobre estos puntos de datos como un conjunto ordenado de datos de serie temporal denominado métricas. OpenSearch Service envía la mayoría de las métricas a CloudWatch en intervalos de 60 segundos. Si utiliza los volúmenes de EBS magnéticos o de uso general, las métricas de volumen de EBS solo se actualizan cada cinco minutos. Para obtener más información sobre Amazon CloudWatch, consulte la Guía del usuario de Amazon CloudWatch.

La consola de OpenSearch Service muestra una serie de gráficos basados en los datos sin procesar de CloudWatch. En función de sus necesidades, es posible que prefiera ver los datos del clúster en CloudWatch en lugar de los gráficos que se muestran en la consola. El servicio archiva las métricas durante dos semanas antes de eliminarlas. Las métricas se proporcionan sin cargo adicional, pero CloudWatch sigue cobrando por la creación de paneles y alarmas. Para más información, consulte los precios de Amazon CloudWatch.

OpenSearch Service publica las siguientes métricas en CloudWatch:

- the section called “Métricas de clúster”
- the section called “Métricas de nodo maestro dedicado”
- the section called “Métricas de volumen de EBS”
- the section called “Métricas de la instancia”
- the section called “Métricas de UltraWarm”
- the section called “Métricas de almacenamiento en frío”
- the section called “Métricas de alertas”
- the section called “Métricas de detección de anomalías”
- the section called “Métricas de búsqueda asíncrona”

- the section called “Métricas de SQL”
- the section called “Métricas k-NN”
- the section called “Métricas de búsqueda entre clústeres”
- the section called “Métricas de replicación entre clústeres”
- the section called “Aprender a clasificar métricas”
- the section called “Métricas del lenguaje de procesamiento de canalizaciones”

Ver métricas con CloudWatch

Las métricas de CloudWatch se agrupan por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

Para ver las métricas a través de la consola de CloudWatch

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, busque Métricas y elija, Todas las métricas. Seleccione el espacio de nombres ES/OpenSearchService.
3. Elija una dimensión para ver las métricas correspondientes. Las métricas de los nodos individuales se encuentran en la dimensión `ClientId, DomainName, NodeId`. Las métricas de clúster se encuentran en la dimensión `Per-Domain, Per-Client Metrics`. Algunas métricas de nodos se agregan a nivel de clúster y, por lo tanto, se incluyen en ambas dimensiones. Las métricas de particiones se encuentran en la dimensión `ClientId, DomainName, NodeId, ShardRole`.

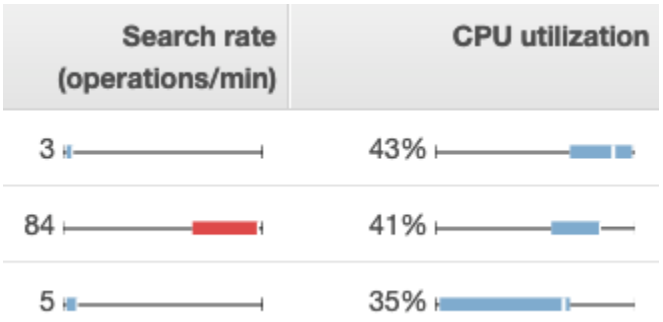
Visualización de una lista de métricas con la AWS CLI

Ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/ES"
```

Interpretación de gráficos de estado en OpenSearch Service

Para ver métricas en OpenSearch Service, utilice las pestañas Estado del clúster e Estado de la instancia. La pestaña Estado de la instancia utiliza gráficos de caja para proporcionar una visibilidad a simple vista del estado de cada nodo de OpenSearch:



- Cada cuadro de color muestra el rango de valores correspondiente al nodo durante el periodo de tiempo especificado.
- Los cuadros azules representan valores que son coherentes con otros nodos. Los cuadros rojos representan los valores atípicos.
- La línea blanca en cada cuadro muestra el valor actual del nodo.
- Los "bigotes" a cada lado del cuadro muestran los valores mínimo y máximo de todas las instancias a lo largo del periodo de tiempo.

Cuando se realizan cambios de configuración en el dominio, a menudo la lista de instancias individuales de las pestañas Estado del clúster e Estado de instancia duplica su tamaño durante un breve periodo antes de volver al número correcto. Para obtener una explicación de este comportamiento, consulte the section called “Cambios de configuración”.

Métricas de clúster

Amazon OpenSearch Service ofrece las siguientes métricas para clústeres.

Métrica	Descripción
`ClusterStatus.green`	Un valor de 1 indica que todas las particiones de índice se han asignado a los nodos del clúster. Estadísticas pertinentes: máximo
`ClusterStatus.yellow`	El valor 1 indica que las particiones principales de todos los índices se han asignado a nodos del clúster, pero las particiones de réplica de al menos un índice están sin asignar. Para más información, consulte the section called “Estado amarillo del clúster”.

Métrica	Descripción
	Estadísticas pertinentes: Máximo
`ClusterStatus.red`	Un valor de 1 indica que las particiones principal y replicada de al menos un índice no se han asignado a los nodos del clúster. Para más información, consulte the section called “Estado rojo del clúster”. Estadísticas pertinentes: Máximo
`Shards.active`	El número total de particiones primarias y de réplicas activas. Estadísticas relevantes: Máximo, Suma
`Shards.unassigned`	El número de particiones que no se asignaron a los nodos del clúster. Estadísticas relevantes: Máximo, Suma
`Shards.delayedUnassigned`	El número de particiones cuya asignación de nodos se retrasó por la configuración de tiempo de espera. Estadísticas relevantes: Máximo, Suma
`Shards.activePrimary`	El número de particiones primarias activas. Estadísticas relevantes: Máximo, Suma
`Shards.initializing`	El número de particiones que se encuentran en inicialización. Estadísticas pertinentes: Suma
`Shards.relocating`	El número de particiones que se encuentran en reubicación. Estadísticas pertinentes: suma

Métrica	Descripción
`Nodes`	La cantidad de nodos en el clúster de OpenSearch Service, incluidos los nodos maestros dedicados y los nodos UltraWarm . Para más información, consulte the section called “Cambios de configuración”. Estadísticas pertinentes: Máximo
`SearchableDocuments`	El número total de documentos que admiten búsquedas para todos los nodos de datos del clúster. Estadísticas pertinentes: mínimo, máximo, promedio
`DeletedDocuments`	El número total de documentos marcados para su eliminación en todos los nodos de datos del clúster. Estos documentos ya no aparecerán en los resultados de búsqueda, pero OpenSearch solo borra los documentos eliminados del disco durante las combinaciones de segmentos. Esta métrica aumenta después de las solicitudes de eliminación y disminuye después de las combinaciones de segmentos. Estadísticas pertinentes: mínimo, máximo, promedio
`CPUUtilization`	El porcentaje de uso de CPU para los nodos de datos del clúster. Máximo muestra el nodo con el mayor uso de CPU. Promedio representa todos los nodos del clúster. Esta métrica también está disponible para los nodos individuales. Estadísticas relevantes: máximo, promedio

Métrica	Descripción
`FreeStorageSpace`	El espacio libre para los nodos de datos del clúster. `Sum` muestra el espacio libre total del clúster, pero debe dejar el periodo en un minuto para recibir un valor preciso. `Minimum` y `Maximum` muestran los nodos con el mínimo y máximo espacio libre, respectivamente. Esta métrica también está disponible para los nodos individuales. OpenSearch Service muestra una `ClusterBlockException` cuando esta métrica alcanza `0`. Para efectuar la recuperación, debe eliminar índices, agregar instancias de mayor tamaño o bien agregar almacenamiento basado en EBS a las instancias existentes. Para más información, consulte the section called “Falta de espacio de almacenamiento disponible”. La consola de OpenSearch Service muestra este valor en GiB. La consola de Amazon CloudWatch lo muestra en MiB. **Note** `FreeStorageSpace` siempre será menor que los valores que el valor que proporcionan las API `_cluster/stats` y `_cat/allocation` de OpenSearch. OpenSearch Service reserva un porcentaje del espacio de almacenamiento de cada instancia para operaciones internas. Para más información, consulte Cálculo de requisitos de almacenamiento. Estadísticas pertinentes: mínimo, máximo, promedio, suma
`ClusterUsedSpace`	El espacio utilizado total para el clúster. Debe dejar el periodo en un minuto para obtener un valor preciso. La consola de OpenSearch Service muestra este valor en GiB. La consola de Amazon CloudWatch lo muestra en MiB. Estadísticas pertinentes: mínimo, máximo

Métrica	Descripción
`ClusterIndexWritesBlocked`	Indica si el clúster acepta o bloquea las solicitudes de escritura entrantes. Un valor de 0 indica que el clúster acepta solicitudes. Un valor de 1 indica que el clúster bloquea las solicitudes. Algunos factores comunes son los siguientes: `FreeStorageSpace` es demasiado bajo o `JVMMemoryPressure` demasiado alta. Para solucionar este problema, considere la posibilidad de añadir más espacio de disco o de ampliar el clúster. Estadísticas pertinentes: máximo
`JVMMemoryPressure`	El porcentaje máximo del montón de Java que se emplea para todos los nodos de datos del clúster. OpenSearch Service utiliza la mitad de la RAM de una instancia para la pila de Java, hasta un tamaño de 32 GiB. Puede escalar las instancias verticalmente hasta 64 GiB de RAM y después escalarlas horizontalmente mediante el agregado de instancias. Consulte the section called “CloudWatch Alarmas recomendadas”. Estadísticas pertinentes: máximo **Note** La lógica de esta métrica cambió en el software del servicio R20220323. Para más información, consulte las notas de la versión.
`OldGenJVMMemoryPressure`	El porcentaje máximo de la pila de Java que se emplea para la “anterior generación” en todos los nodos de datos del clúster. Esta métrica también está disponible a nivel de nodo. Estadísticas pertinentes: máximo

Métrica	Descripción
AutomatedSnapshotFailure	El número de instantáneas automatizadas que han producido un error para el clúster. Un valor de 1 indica que no se ha tomado ninguna instantánea automatizada del dominio en las últimas 36 horas. Estadísticas pertinentes: mínimo, máximo
CPUCreditBalance	Los créditos de CPU restantes que están disponibles para los nodos de datos del clúster. Un crédito de CPU proporciona el desempeño de un núcleo de CPU completo durante un minuto. Para más información, consulte Créditos CPU en la Guía para desarrolladores de Amazon EC2. Esta métrica solo está disponible para el tipo de instancias T2. Estadísticas pertinentes: mínimo
OpenSearchDashboardsHealthyNodes	Una comprobación de estado de OpenSearch Dashboards. Si el mínimo, el máximo y el promedio son todos iguales a 1, Dashboards se comporta con normalidad. Si tiene 10 nodos con un máximo de 1, mínimo de 0 y promedio de 0,7, esto significa que 7 nodos (70 %) están en buen estado y 3 nodos (30 %) no lo están. Estadísticas pertinentes: mínimo, máximo, promedio
OpensearchDashboardsReportingFailedRequestSysErrCount	El número de solicitudes para generar informes de OpenSearch Dashboards que tuvieron errores debido a problemas del servidor o a limitaciones de los recursos. Estadísticas pertinentes: suma
OpensearchDashboardsReportingFailedRequestUserErrCount	El número de solicitudes para generar informes de OpenSearch Dashboards que no se realizaron de forma correcta debido a problemas del cliente. Estadísticas pertinentes: suma

Métrica	Descripción
`OpensearchDashboardsReportingRequestCount`	El número total de solicitudes para generar informes de OpenSearch Dashboards. Estadísticas pertinentes: suma
`OpensearchDashboardsReportingSuccessCount`	El número de solicitudes realizadas de forma correcta para generar informes de OpenSearch Dashboards. Estadísticas pertinentes: suma
`KMSKeyError`	Un valor igual a 1 indica que la clave de AWS KMS utilizada para cifrar los datos en reposo se deshabilitó. Para restablecer el dominio a operaciones normales, rehabilita la clave. La consola solo muestra esta métrica para los dominios que encriptan los datos en reposo. Estadísticas pertinentes: mínimo, máximo
`KMSKeyInaccessible`	Un valor igual a 1 indica que la clave de AWS KMS utilizada para cifrar los datos en reposo se eliminó o se revocaron sus permisos a OpenSearch Service. No puede recuperar los dominios que están en este estado. Sin embargo, si tiene una instantánea manual, puede utilizarla para migrar los datos del dominio a un nuevo dominio. La consola solo muestra esta métrica para los dominios que encriptan los datos en reposo. Estadísticas pertinentes: mínimo, máximo

Métrica	Descripción
`InvalidHostHeaderRequests`	El número de solicitudes HTTP realizadas al clúster de OpenSearch que incluía un encabezado de host no válido (o faltante). Las solicitudes válidas incluyen el nombre de host del dominio como valor de encabezado de host. OpenSearch Service rechaza las solicitudes no válidas para dominios de acceso público que no tienen una política de acceso restrictiva. Es recomendable que aplique una política de acceso restrictiva a todos los dominios. Si se muestran valores altos para esta métrica, confirme que sus clientes de OpenSearch incluyen el nombre de host del dominio (y no, por ejemplo, su dirección IP) en sus solicitudes. Estadísticas pertinentes: suma
`OpenSearchRequests (previously ElasticsearchRequests)`	El número de solicitudes realizadas al clúster de OpenSearch. Estadísticas pertinentes: suma
`2xx, 3xx, 4xx, 5xx`	El número de solicitudes para el dominio que produjeron el código de respuesta HTTP especificado (2xx, 3xx, 4xx, 5xx). Estadísticas pertinentes: suma

Métrica	Descripción
`ThroughputThrottle`	Indica si los discos se han limitado o no. La limitación se produce cuando el rendimiento combinado de `ReadThroughputMicroBursting` y `WriteThroughputMicroBursting` es superior al rendimiento máximo, `MaxProvisionedThroughput`. `MaxProvisionedThroughput` es el valor más bajo del rendimiento de la instancia o del volumen aprovisionado. Un valor de 1 indica que los discos se han limitado. Un valor de 0 indica un comportamiento normal. Para obtener más información sobre el rendimiento de la instancia, consulte Instancias optimizadas para Amazon EBS. Para obtener información sobre el rendimiento del volumen, consulte los tipos de volumen de Amazon EBS. Estadísticas pertinentes: mínimo, máximo

Métricas de nodo maestro dedicado

Amazon OpenSearch Service ofrece las siguientes métricas para nodos maestros dedicados.

Métrica	Descripción
`MasterCPUUtilization`	El porcentaje máximo de recursos de CPU que se utilizan en los nodos maestros dedicados. Recomendamos aumentar el tamaño del tipo de instancia cuando esta métrica alcance el 60 por ciento. Estadísticas pertinentes: máximo
`MasterFreeStorageSpace`	Esta métrica no es pertinente y puede pasarse por alto. El servicio no usa los nodos maestros como nodos de datos.
`MasterJVMMemoryPressure`	El porcentaje máximo del montón de Java que se emplea para todos los nodos maestros dedicados del clúster. Recomendamos cambiar a un tipo de instancia mayor cuando esta métrica alcance el 85 por ciento.

Métrica	Descripción
	Estadísticas pertinentes: máximo **Note** La lógica de esta métrica cambió en el software del servicio R20220323. Para más información, consulte las notas de la versión.
`MasterOldGenJVMMemoryPressure`	El porcentaje máximo de la pila de Java que se emplea para la “anterior generación” según el nodo maestro. Estadísticas pertinentes: máximo
`MasterCPUCreditBalance`	Los créditos de CPU restantes que están disponibles para los nodos maestros dedicados del clúster. Un crédito de CPU proporciona el desempeño de un núcleo de CPU completo durante un minuto. Para más información, consulte Créditos CPU en la Guía para desarrolladores de Amazon EC2. Esta métrica solo está disponible para el tipo de instancias T2. Estadísticas pertinentes: mínimo
`MasterReachableFromNode`	Comprobación de estado de las excepciones `MasterNotDiscovered` . Un valor de 1 indica un comportamiento normal. Un valor de 0 indica que `/_cluster/health/` ha dado error. Los errores significan que no se puede acceder al nodo maestro desde el nodo de origen. Suelen ser el resultado de un problema de conectividad de red o de dependencia de AWS. Estadísticas pertinentes: máximo
`MasterSysMemoryUtilization`	El porcentaje de memoria del nodo maestro que está en uso. Estadísticas pertinentes: máximo

Métricas de volumen de EBS

Amazon OpenSearch Service ofrece las siguientes métricas para volúmenes de EBS.

Métrica	Descripción
`ReadLatency`	La latencia en segundos para las operaciones de lectura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio
`WriteLatency`	La latencia en segundos para las operaciones de escritura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio
`ReadThroughput`	El rendimiento en bytes por segundo para las operaciones de lectura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio
`ReadThroughputMicroBursting`	Se tiene en cuenta el rendimiento, en bytes por segundo, de las operaciones de lectura en volúmenes de EBS cuando se tiene en cuenta la microrráfaga. Esta métrica también está disponible para los nodos individuales. La microrráfaga se produce cuando un volumen de EBS alcanza niveles altos de IOPS o rendimiento durante períodos de tiempo significativamente más cortos (menos de un minuto). Estadísticas pertinentes: mínimo, máximo, promedio
`WriteThroughput`	El rendimiento en bytes por segundo para las operaciones de escritura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio

Métrica	Descripción
`WriteThroughputMicroBursting`	Se tiene en cuenta el rendimiento, en bytes por segundo, de las operaciones de escritura en volúmenes de EBS cuando se tiene en cuenta la microrráfaga. Esta métrica también está disponible para los nodos individuales. La microrráfaga se produce cuando un volumen de EBS alcanza niveles altos de IOPS o rendimiento durante períodos de tiempo significativamente más cortos (menos de un minuto). Estadísticas pertinentes: mínimo, máximo, promedio
`DiskQueueDepth`	El número de solicitudes de entrada y salida (E/S) pendientes de un volumen de EBS. Estadísticas pertinentes: mínimo, máximo, promedio
`ReadIOPS`	El número de operaciones de entrada y salida (E/S) por segundo para las operaciones de lectura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio
`ReadIOPSMicroBursting`	El número de operaciones de entrada y salida (E/S) por segundo para las operaciones de lectura en los volúmenes de EBS cuando se tiene en cuenta la microrráfaga. Esta métrica también está disponible para los nodos individuales. La microrráfaga se produce cuando un volumen de EBS alcanza niveles altos de IOPS o rendimiento durante períodos de tiempo significativamente más cortos (menos de un minuto). Estadísticas pertinentes: mínimo, máximo, promedio
`WriteIOPS`	El número de operaciones de entrada y salida (E/S) por segundo para las operaciones de escritura en los volúmenes de EBS. Esta métrica también está disponible para los nodos individuales. Estadísticas pertinentes: mínimo, máximo, promedio

Métrica	Descripción
`WriteIOPS MicroBursting`	El número de operaciones de entrada y salida (E/S) por segundo para las operaciones de escritura en los volúmenes de EBS cuando se tiene en cuenta la microrráfaga. Esta métrica también está disponible para los nodos individuales. La microrráfaga se produce cuando un volumen de EBS alcanza niveles altos de IOPS o rendimiento durante períodos de tiempo significativamente más cortos (menos de un minuto). Estadísticas pertinentes: mínimo, máximo, promedio
`BurstBalance`	El porcentaje de los créditos de entrada y salida (E/S) que quedan en el bucket de ráfaga para un volumen de EBS. Un valor de 100 significa que el volumen ha acumulado el número máximo de créditos. Si este porcentaje cae por debajo del 70 %, consulte the section called “Bajo balance de ráfaga EBS”. El balance de ráfagas se mantiene en 0 para los dominios con tipos de volúmenes gp3, así como para los dominios con volúmenes gp2 que tengan un tamaño de volumen superior a 1000 GiB. Estadísticas pertinentes: mínimo, máximo, promedio

Métricas de la instancia

Amazon OpenSearch Service proporciona las siguientes métricas para cada instancia de un dominio. OpenSearch Service también acumula estas métricas de instancia para proporcionar información sobre el estado general del clúster. Puede verificar este comportamiento mediante la estadística Recuento de muestras en la consola. Tenga en cuenta que las métricas de la tabla siguiente disponen de estadísticas relevantes para el nodo y el clúster.

> **Important**
>
> Las diferentes versiones de Elasticsearch utilizan diferentes grupos de subprocesos para procesar las llamadas a la API `_index`. Elasticsearch 1.5 y 2.3 utilizan el grupo de subprocesos de indexación. Elasticsearch 5.x, 6.0 y 6.2 utilizan el grupo de subprocesos por lotes. OpenSearch y Elasticsearch 6.3 y posteriores utilizan el grupo de subprocesos de

escritura. Actualmente, la consola de OpenSearch Service no incluye un gráfico para el grupo de subprocesos masivos.
Utilice `GET _cluster/settings?include_defaults=true` para verificar el tamaño del grupo de subprocesos y las colas para el clúster.

Métrica	Descripción
`IndexingLatency`	La diferencia en el tiempo total, en milisegundos, calculada por todas las operaciones de indexación en un nodo entre el minuto N y el minuto (N-1). Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo
`IndexingRate`	El número de operaciones de indexación por minuto. Una sola llamada a la API `_bulk` que añade dos documentos y actualiza dos recuentos como cuatro operaciones, que podrían propagarse por uno o varios nodos. Si dicho índice tiene una o varias réplicas, otros nodos del clúster también registran un total de cuatro operaciones de indexación. Las eliminaciones de documentos no se tienen en cuenta en esta métrica. Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo, suma
`SearchLatency`	La diferencia en el tiempo total, en milisegundos, calculada por todas las búsquedas en un nodo entre el minuto N y el minuto (N-1). Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo
`SearchRate`	El número total de peticiones de búsqueda por minuto de todas las particiones de un nodo de datos. Una sola llamada a la API `_search` podría devolver resultados de muchas particiones

Métrica	Descripción
	diferentes. Si cinco de estas particiones se encuentran en un nodo, este notificaría el valor 5 para la métrica, incluso aunque el cliente solo realizara una solicitud. Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo, suma
`SegmentCount`	El número de segmentos de un nodo de datos. Cuantos más segmentos tenga, más tiempo tardará cada búsqueda. OpenSearch de vez en cuando combina segmentos más pequeños en uno más grande. Estadísticas de nodo pertinentes: máximo, promedio Estadísticas de clúster pertinentes: suma, máximo, promedio
`SysMemoryUtilization`	El porcentaje de memoria de la instancia que está en uso. Es normal obtener valores altos para esta métrica y, por lo general, no representan un problema con el clúster. Para obtener un mejor indicador de posibles problemas de rendimiento y estabilidad, consulte la métrica `JVMMemoryPressure` . Estadísticas de nodo pertinentes: mínimo, máximo, promedio Estadísticas de clúster pertinentes: mínimo, máximo, promedio
`JVMGCYoungCollectionCount`	Número de veces que se ha ejecutado la recopilación de elementos no utilizados "nueva generación". Un número grande y en continuo crecimiento de ejecuciones es normal para las operaciones de clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio

Métrica	Descripción
JVMGCYoungCollectionTime	La cantidad de tiempo en milisegundos que el clúster ha empleado en realizar la recopilación de elementos no utilizados "nueva generación". Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
JVMGCOldCollectionCount	Número de veces que se ha ejecutado la recopilación de elementos no utilizados "generación anterior". En un clúster con suficientes recursos, este número debe ser pequeño y crecer con poca frecuencia. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
JVMGCOldCollectionTime	La cantidad de tiempo en milisegundos que el clúster ha empleado en realizar la recopilación de elementos no utilizados "generación anterior". Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
OpenSearchDashboardsConcurrentConnections	El número de conexiones simultáneas activas a OpenSearch Dashboards. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio

Métrica	Descripción
OpenSearchDashboardsHealthyNode	Comprobación de estado del nodo individual de OpenSearch Dashboards. Un valor de 1 indica un comportamiento normal. Un valor de 0 indica que Dashboards es inaccesible. Estadísticas de nodo pertinentes: mínimo Estadísticas de clúster pertinentes: mínimo, máximo, promedio
OpenSearchDashboardsHeapTotal	La cantidad de memoria de pila asignada a OpenSearch Dashboards en MiB. Los diferentes tipos de instancias EC2 pueden afectar a la asignación exacta de memoria. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
OpenSearchDashboardsHeapUsed	La cantidad absoluta de memoria de la pila utilizada por OpenSearch Dashboards en MiB. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
OpenSearchDashboardsHeapUtilization	El porcentaje máximo de memoria de la pila disponible que utiliza OpenSearch Dashboards. Si este valor aumenta por encima del 80 %, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: mínimo, máximo, promedio

Métrica	Descripción
`OpenSearchDashboardsOS1MinuteLoad`	El promedio de carga de CPU de un minuto para OpenSearch Dashboards. La carga de la CPU idealmente debería permanecer por debajo de 1,00. Aunque los picos temporales están bien, se recomienda aumentar el tamaño del tipo de instancias si esta métrica está constantemente por encima de 1,00. Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo
`OpenSearchDashboardsRequestTotal`	El recuento total de solicitudes HTTP realizadas a OpenSearch Dashboards. Si su sistema es lento o ve un número elevado de solicitudes de Dashboards, considere aumentar el tamaño del tipo de instancias. Estadísticas de nodos pertinentes: suma Estadísticas de clúster pertinentes: suma
`OpenSearchDashboardsResponseTimesMaxInMillis`	El tiempo máximo, en milisegundos, que OpenSearch Dashboards tarda en responder a una solicitud. Si las solicitudes tardan mucho tiempo en devolver resultados, considere aumentar el tamaño del tipo de instancias. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: máximo, promedio
`SearchTaskCancelled`	El número de cancelaciones del nodo coordinador. Estadísticas de nodos pertinentes: suma Estadísticas de clúster pertinentes: suma
`SearchShardTaskCancelled`	El número de cancelaciones del nodo de datos. Estadísticas de nodos pertinentes: suma Estadísticas de clúster pertinentes: suma,

Métrica	Descripción
ThreadpoolForce_mergeQueue	El número de tareas en cola en el grupo de subprocesos de combinación forzada. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
ThreadpoolForce_mergeRejected	El número de tareas rechazadas en el grupo de subprocesos de combinación forzada. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma
ThreadpoolForce_mergeThreads	El tamaño del grupo de subprocesos de combinación forzada. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
ThreadpoolIndexQueue	El número de tareas en cola en el grupo de subprocesos de indexación. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. El tamaño de la cola de indexación máximo es 200. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
ThreadpoolIndexRejected	El número de tareas rechazadas en el grupo de subprocesos de indexación. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma

Métrica	Descripción
`ThreadpoolIndexThreads`	El tamaño del grupo de subprocesos de indexación. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`ThreadpoolSearchQueue`	El número de tareas en cola en el grupo de subprocesos de búsqueda. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. El tamaño máximo de la cola de búsqueda es 1000. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
`ThreadpoolSearchRejected`	El número de tareas rechazadas en el grupo de subprocesos de búsqueda. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma
`ThreadpoolSearchThreads`	El tamaño del grupo de subprocesos de búsqueda. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`Threadpoolsql-workerQueue`	El número de tareas en cola en el grupo de subprocesos de búsqueda de SQL. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio

Métrica	Descripción
`Threadpoolsql-workerRejected`	El número de tareas rechazadas en el grupo de subprocesos de búsqueda de SQL. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma
`Threadpoolsql-workerThreads`	El tamaño del grupo de subprocesos de búsqueda de SQL. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`ThreadpoolBulkQueue`	El número de tareas en cola en el grupo de subprocesos por lotes. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
`ThreadpoolBulkRejected`	El número de tareas rechazadas en el grupo de subprocesos por lotes. Si este número crece continuamente, considere la posibilidad de escalar el clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma
`ThreadpoolBulkThreads`	El tamaño del grupo de subprocesos por lotes. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma

Métrica	Descripción
`ThreadpoolWriteThreads`	El tamaño del grupo de subprocesos de escritura. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`ThreadpoolWriteQueue`	El número de tareas en cola en el grupo de subprocesos de escritura. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`ThreadpoolWriteRejected`	El número de tareas rechazadas en el grupo de subprocesos de escritura. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma **Note** Debido a que el tamaño predeterminado de la cola de escritura aumentó de 200 a 10 000 en la versión 7.1, esta métrica ya no es el único indicador de rechazos de OpenSearch Service. Utilice las métricas `CoordinatingWriteRejected`, `PrimaryWriteRejected` y `ReplicaWriteRejected` para monitorear los rechazos en las versiones 7.1 y posteriores.

Métrica	Descripción
`CoordinatingWriteRejected`	El número total de rechazos se produjo en el nodo de coordinación debido a la presión de indexación desde el último inicio del proceso de OpenSearch Service. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma Esta métrica está disponible en la versión 7.1 y posteriores.
`PrimaryWriteRejected`	El número total de rechazos se produjo en las particiones principales debido a la presión de indexación desde el último inicio del proceso de OpenSearch Service. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma Esta métrica está disponible en la versión 7.1 y posteriores.
`ReplicaWriteRejected`	El número total de rechazos se produjo en las particiones de réplica debido a la presión de indexación desde el último inicio del proceso de OpenSearch Service. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma Esta métrica está disponible en la versión 7.1 y posteriores.

Métricas de UltraWarm

Amazon OpenSearch Service ofrece las siguientes métricas para nodos de UltraWarm.

Métrica	Descripción
`WarmCPUUtilization`	El porcentaje de uso de CPU para los nodos UltraWarm del clúster. Máximo muestra el nodo con el mayor uso de CPU. Promedio represent

Métrica	Descripción
	a todos los nodos UltraWarm del clúster. Esta métrica también está disponible para nodos UltraWarm individuales. Estadísticas relevantes: máximo, promedio
`WarmFreeStorageSpace`	La cantidad de espacio de almacenamiento en caliente libre en MiB. Debido a que UltraWarm utiliza Amazon S3 en lugar de discos adjuntos, `Sum` es la única estadística pertinente. Debe dejar el periodo en un minuto para obtener un valor preciso. Estadísticas pertinentes: suma
`WarmSearchableDocuments`	Número total de documentos en los que se pueden realizar búsquedas de todos los índices templados del clúster. Debe dejar el periodo en un minuto para obtener un valor preciso. Estadísticas pertinentes: suma
`WarmSearchLatency`	La diferencia en el tiempo total, en milisegundos, calculada por todas las búsquedas en UltraWarm entre el minuto N y el minuto (N-1). Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo
`WarmSearchRate`	El número total de peticiones de búsqueda por minuto de todas las particiones de un nodo UltraWarm. Una sola llamada a la API `_search` podría devolver resultados de muchas particiones diferentes. Si cinco de estas particiones se encuentran en un nodo, este notificaría el valor 5 para la métrica, incluso aunque el cliente solo realizara una solicitud. Estadísticas de nodo pertinentes: promedio Estadísticas de clúster pertinentes: promedio, máximo, suma
`WarmStorageSpaceUtilization`	Cantidad total del espacio de almacenamiento templado, en MiB, que utiliza el clúster. Estadísticas pertinentes: máximo

Métrica	Descripción
`HotStorageSpaceUtilization`	Cantidad total del espacio de almacenamiento en caliente que utiliza el clúster. Estadísticas pertinentes: máximo
`WarmSysMemoryUtilization`	Porcentaje de la memoria del nodo maestro que está en uso. Estadísticas pertinentes: máximo
`HotToWarmMigrationQueueSize`	Número de índices a la espera actualmente para migrar del almacenamiento caliente al almacenamiento templado. Estadísticas pertinentes: máximo
`WarmToHotMigrationQueueSize`	Número de índices a la espera actualmente para migrar del almacenamiento templado al almacenamiento caliente. Estadísticas pertinentes: máximo
`HotToWarmMigrationFailureCount`	El número total de errores de migración del almacenamiento en caliente al almacenamiento templado. Estadísticas pertinentes: suma
`HotToWarmMigrationForceMergeLatency`	Latencia media de la etapa de fusión de fuerzas del proceso de migración. Si esta etapa lleva demasiado tiempo, considere aumentar `index.ultrawarm.migration.force_merge.max_num_segments` . Estadísticas pertinentes: promedio
`HotToWarmMigrationSnapshotLatency`	Latencia media de la etapa de instantánea del proceso de migración. Si esta etapa tarda demasiado tiempo, asegúrese de que las particiones estén correctamente dimensionadas y distribuidas por todo el clúster. Estadísticas pertinentes: promedio

Métrica	Descripción
`HotToWarmMigrationProcessingLatency`	La latencia media de migraciones exitosas del almacenamiento en caliente al almacenamiento templado, sin incluir el tiempo que estuvo en la cola. Este valor es la suma de la cantidad de tiempo que se tarda en completar las etapas de fusión de fuerza, instantánea y reubicación de particiones del proceso de migración. Estadísticas pertinentes: promedio
`HotToWarmMigrationSuccessCount`	El número total de migraciones exitosas del almacenamiento en caliente al almacenamiento templado. Estadísticas pertinentes: suma
`HotToWarmMigrationSuccessLatency`	La latencia media de migraciones exitosas del almacenamiento en caliente al almacenamiento templado, incluido el tiempo que estuvo en la cola. Estadísticas pertinentes: promedio
`WarmThreadpoolSearchThreads`	El tamaño del grupo de subprocesos de búsqueda de UltraWarm. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: promedio, suma
`WarmThreadpoolSearchRejected`	El número de tareas rechazadas en el grupo de subprocesos de búsqueda de UltraWarm. Si este número crece, considere la posibilidad de agregar más nodos de UltraWarm. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma

Métrica	Descripción
`WarmThreadpoolSearchQueue`	El número de tareas en cola en el grupo de subprocesos de búsqueda de UltraWarm. Si el tamaño de la cola es elevado, considere la posibilidad de agregar más nodos de UltraWarm. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
`WarmJVMMemoryPressure`	Porcentaje máximo del montón de Java que se emplea con los nodos de UltraWarm. Estadísticas pertinentes: máximo **Note** La lógica de esta métrica cambió en el software del servicio R20220323. Para más información, consulte las notas de la versión.
`WarmOldGenJVMMemoryPressure`	El porcentaje máximo de la pila de Java que se emplea para la “anterior generación” según el nodo UltraWarm. Estadísticas pertinentes: máximo
`WarmJVMGCYoungCollectionCount`	Número de veces que se ejecutó la recolección de basura de la “nueva generación” en los nodos de UltraWarm. Un número grande y en continuo crecimiento de ejecuciones es normal para las operaciones de clúster. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio

Métrica	Descripción
`WarmJVMGCYoungCollectionTime`	La cantidad de tiempo en milisegundos que el clúster empleó en realizar la recolección de basura de la “nueva generación” en los nodos de UltraWarm. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio
`WarmJVMGCOldCollectionCount`	Número de veces que se ejecutó la recolección de basura de la “generación anterior” en los nodos de UltraWarm. En un clúster con suficientes recursos, este número debe ser pequeño y crecer con poca frecuencia. Estadísticas de nodo pertinentes: máximo Estadísticas de clúster pertinentes: suma, máximo, promedio

Métricas de almacenamiento en frío

Amazon OpenSearch Service ofrece las siguientes métricas para el almacenamiento frío.

Métrica	Descripción
`ColdStorageSpaceUtilization`	La cantidad total de espacio de almacenamiento en frío, en MiB, que el clúster utiliza. Estadísticas pertinentes: máximo
`ColdToWarmMigrationFailureCount`	El número total de errores de migración del almacenamiento en frío al almacenamiento templado. Estadísticas pertinentes: suma
`ColdToWarmMigrationLatency`	Cantidad de tiempo para que se completen de forma correcta las migraciones del almacenamiento en frío al almacenamiento templado.

Métrica	Descripción
	Estadísticas pertinentes: promedio
`ColdToWarmMigrationQueueSize`	Número de índices a la espera actualmente para migrar del almacenamiento frío al almacenamiento templado. Estadísticas pertinentes: máximo
`ColdToWarmMigrationSuccessCount`	El número total de migraciones exitosas del almacenamiento en frío al almacenamiento templado. Estadísticas pertinentes: suma
`WarmToColdMigrationFailureCount`	El número total de errores de migración del almacenamiento templado al almacenamiento en frío. Estadísticas pertinentes: suma
`WarmToColdMigrationLatency`	Cantidad de tiempo para que se completen de forma correcta las migraciones del almacenamiento templado al almacenamiento en frío. Estadísticas pertinentes: promedio
`WarmToColdMigrationQueueSize`	Número de índices a la espera actualmente para migrar del almacenamiento templado al almacenamiento frío. Estadísticas pertinentes: máximo
`WarmToColdMigrationSuccessCount`	El número total de migraciones exitosas del almacenamiento templado al almacenamiento en frío. Estadísticas pertinentes: suma

Métricas de OR1

Amazon OpenSearch Service ofrece las siguientes métricas para las instancias OR1.

Métrica	Descripción
`RemoteStorageUsedSpace`	Cantidad total del espacio de Amazon S3, en MiB, que utiliza el clúster. Estadísticas pertinentes: suma
`RemoteStorageWriteRejected`	El número total de solicitudes rechazadas en las particiones principales debido a la presión de replicación y almacenamiento remoto. Se calcula a partir del último inicio del proceso de OpenSearch Service. Estadísticas pertinentes: suma

Métricas de alertas

Amazon OpenSearch Service ofrece las siguientes métricas para alertas.

Métrica	Descripción
`AlertingDegraded`	Un valor de 1 significa que el índice de alerta es rojo o que uno o más nodos no van según lo programado. Un valor de 0 indica un comportamiento normal. Estadísticas pertinentes: máximo
`AlertingIndexExists`	Un valor de 1 significa que el índice `.opensearch-alerting-config` existe. Un valor de 0 significa que no existe. Hasta que utilice la función de alerta por primera vez, este valor sigue siendo 0. Estadísticas pertinentes: máximo
`AlertingIndexStatus.green`	El estado de salud del índice. Un valor de 1 significa verde. Un valor de 0 significa que el índice no existe o no es verde. Estadísticas pertinentes: máximo
`AlertingIndexStatus.red`	El estado de salud del índice. Un valor de 1 significa rojo. Un valor de 0 significa que el índice no existe o no es rojo.

Métrica	Descripción
	Estadísticas pertinentes: máximo
`AlertingIndexStatus.yellow`	El estado de salud del índice. Un valor de 1 significa amarillo. Un valor de 0 significa que el índice no existe o no es amarillo. Estadísticas pertinentes: máximo
`AlertingNodesNotOnSchedule`	Un valor de 1 significa que algunos trabajos no se están ejecutando según lo programado. Un valor de 0 significa que todos los trabajos de alerta se están ejecutando según lo programado (o que no hay trabajos de alerta). Verifique la consola de OpenSearch Service o realice una solicitud `_nodes/stats` para saber si algún nodo muestra un alto consumo de recursos. Estadísticas pertinentes: máximo
`AlertingNodesOnSchedule`	Un valor de 1 significa que todos los trabajos de alerta se están ejecutando según lo programado (o que no hay trabajos de alerta). Un valor de 0 significa que algunos trabajos no se están ejecutando según lo programado. Estadísticas pertinentes: máximo
`AlertingScheduledJobEnabled`	Un valor de 1 significa que la configuración del clúster `opensearch.scheduled_jobs.enabled` es verdadera. Un valor de 0 significa que es falsa y que los trabajos programados están deshabilitados. Estadísticas pertinentes: máximo

Métricas de detección de anomalías

Amazon OpenSearch Service ofrece las siguientes métricas para la detección de anomalías.

Métrica	Descripción
`ADPluginUnhealthy`	El valor 1 significa que el complemento de detección de anomalías no funciona correctamente, bien debido a un gran número de errores o bien porque uno de los índices que utiliza es rojo. Un valor de 0 indica que el complemento funciona como se esperaba. Estadísticas pertinentes: máximo
`ADExecuteRequestCount`	El número de solicitudes para detectar anomalías. Estadísticas pertinentes: suma
`ADExecuteFailureCount`	El número de solicitudes erróneas para detectar anomalías. Estadísticas pertinentes: suma
`ADHCExecuteFailureCount`	El número de errores de solicitud al detectar anomalías para los detectores de alta cardinalidad. Estadísticas pertinentes: suma
`ADHCExecuteRequestCount`	El número de solicitudes al detectar anomalías para detectores de alta cardinalidad. Estadísticas pertinentes: suma
`ADAnomalyResultsIndexStatusIndexExists`	Un valor de 1 significa que existe el índice al que apunta el alias `.opensearch-anomaly-results`. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo
`ADAnomalyResultsIndexStatus.red`	Un valor de 1 significa que el índice al que apunta el alias `.opensearch-anomaly-results` es rojo. Un valor de 0 significa que no lo es. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo

Métrica	Descripción
`ADAnomaly Detectors IndexStat usIndexExists`	Un valor de 1 significa que el índice `.opensearch-anomaly-detectors` existe. Un valor de 0 significa que no existe. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo
`ADAnomaly Detectors IndexStat us.red`	Un valor de 1 significa que el índice `.opensearch-anomaly-detectors` es rojo. Un valor de 0 significa que no lo es. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo
`ADModelsC heckpoint IndexStat usIndexExists`	Un valor de 1 significa que el índice `.opensearch-anomaly-checkpoints` existe. Un valor de 0 significa que no existe. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo
`ADModelsC heckpoint IndexStat us.red`	Un valor de 1 significa que el índice `.opensearch-anomaly-checkpoints` es rojo. Un valor de 0 significa que no lo es. Hasta que no se utilice la detección de anomalías por primera vez, este valor permanece en 0. Estadísticas pertinentes: máximo

Métricas de búsqueda asíncrona

Amazon OpenSearch Service ofrece las siguientes métricas para la búsqueda asíncrona.

Estadísticas del nodo coordinador de búsqueda asíncrona (por nodo coordinador)

Métrica	Descripción
`AsynchronousSearchSubmissionRate`	El número de búsquedas asíncronas enviadas en el último minuto.
`AsynchronousSearchInitializedRate`	El número de búsquedas asíncronas inicializadas en el último minuto.
`AsynchronousSearchRunningCurrent`	El número de búsquedas asíncronas que se ejecutan actualmente.
`AsynchronousSearchCompletionRate`	El número de búsquedas asíncronas realizadas correctamente en el último minuto.
`AsynchronousSearchFailureRate`	El número de búsquedas asíncronas que se completaron y fallaron en el último minuto.
`AsynchronousSearchPersistRate`	El número de búsquedas asíncronas que persistieron en el último minuto.
`AsynchronousSearchPersistFailedRate`	El número de búsquedas asíncronas que no pudieron persistir en el último minuto.
`AsynchronousSearchRejected`	El número total de búsquedas asíncronas rechazadas desde el tiempo de actividad del nodo.

Métrica	Descripción
`AsynchronousSearchCancelled`	El número total de búsquedas asíncronas canceladas desde el tiempo de actividad del nodo.
`AsynchronousSearchMaxRunningTime`	Duración de la búsqueda asíncrona de ejecución más larga en un nodo en el último minuto.

Estadísticas del clúster de búsqueda asíncrona

Métrica	Descripción
`AsynchronousSearchStoreHealth`	El estado de la tienda en el índice persistente (ROJO/no ROJO) en el último minuto.
`AsynchronousSearchStoreSize`	El tamaño del índice del sistema en todas las particiones en el último minuto.
`AsynchronousSearchStoredResponseCount`	El número de respuestas almacenadas en el índice del sistema en el último minuto.

Métricas de ajuste automático

Amazon OpenSearch Service ofrece las siguientes métricas de ajuste automático.

Métrica	Descripción
`AutoTuneChangesHistoryHeapSize`	El historial de cambios en MiB para los valores de ajuste del tamaño del montón.

Métrica	Descripción
`AutoTuneChangesHistoryJVMYoungGenArgs`	El historial de cambios de los argumentos de JVM YongGen.
`AutoTuneFailed`	Un valor booleano que indica si el cambio de ajuste automático produjo un error.
`AutoTuneSucceeded`	Un valor booleano que indica si el cambio de ajuste automático se realizó correctamente.
`AutoTuneValue`	El historial de cambios de cola (recuento) y el historial de cambios de ajustes de caché (en MiB) para los cambios no disruptivos.

Métricas de Multi-AZ con modo de espera

Amazon OpenSearch Service ofrece las siguientes métricas para Multi-AZ con modo de espera.

Métricas a nivel de nodo para los nodos de datos en zonas de disponibilidad activas

Métrica	Descripción
`CPUUtilization`	El porcentaje de uso de CPU para los nodos de datos del clúster. Máximo muestra el nodo con el mayor uso de CPU. Promedio represent a todos los nodos del clúster. Esta métrica también está disponible para los nodos individuales.
`FreeStorageSpace`	El espacio libre para los nodos de datos del clúster. `Sum` muestra el espacio libre total del clúster, pero debe dejar el periodo en un minuto para recibir un valor preciso. `Minimum` y `Maximum` muestran los nodos con el mínimo y máximo espacio libre, respectivamente. Esta métrica también está disponible para los nodos individuales. OpenSearch Service muestra una `ClusterBlockException` cuando esta métrica alcanza `0`. Para efectuar la recuperación, debe eliminar índices, agregar instancias de mayor tamaño o bien agregar almacenamiento basado en EBS a las instancias existentes. Para más información,

Métrica	Descripción
	consulte the section called “Falta de espacio de almacenamiento disponible”. La consola de OpenSearch Service muestra este valor en GiB. La consola de Amazon CloudWatch lo muestra en MiB.
`JVMMemory Pressure`	El porcentaje máximo del montón de Java que se emplea para todos los nodos de datos del clúster. OpenSearch Service utiliza la mitad de la RAM de una instancia para la pila de Java, hasta un tamaño de 32 GiB. Puede escalar las instancias verticalmente hasta 64 GiB de RAM y después escalarlas horizontalmente mediante el agregado de instancias. Consulte the section called “ CloudWatch Alarmas recomendadas”.
`SysMemory Utilization`	El porcentaje de memoria de la instancia que está en uso. Es normal obtener valores altos para esta métrica y, por lo general, no representan un problema con el clúster. Para obtener un mejor indicador de posibles problemas de rendimiento y estabilidad, consulte la métrica `JVMMemory Pressure` .
`IndexingLatency`	La diferencia en el tiempo total, en milisegundos, calculada por todas las operaciones de indexación en un nodo entre el minuto N y el minuto (N-1).
`IndexingRate`	El número de operaciones de indexación por minuto.
`SearchLatency`	La diferencia en el tiempo total, en milisegundos, calculada por todas las búsquedas en un nodo entre el minuto N y el minuto (N-1).
`SearchRate`	El número total de peticiones de búsqueda por minuto de todas las particiones de un nodo de datos.
`Threadpool SearchQueue`	El número de tareas en cola en el grupo de subprocesos de búsqueda. Si el tamaño de la cola es sistemáticamente elevado, considere la posibilidad de escalar el clúster. El tamaño máximo de la cola de búsqueda es 1000.

Métrica	Descripción
`ThreadpoolWriteQueue`	El número de tareas en cola en el grupo de subprocesos de escritura.
`ThreadpoolSearchRejected`	El número de tareas rechazadas en el grupo de subprocesos de búsqueda. Si este número crece continuamente, considere la posibilidad de escalar el clúster.
`ThreadpoolWriteRejected`	El número de tareas rechazadas en el grupo de subprocesos de escritura.

Métricas de nivel de clúster para clústeres en zonas de disponibilidad activas

Métrica	Descripción
`DataNodes`	El número total de particiones activas y en espera.
`DataNodesShards.active`	El número total de particiones primarias y de réplicas activas.
`DataNodesShards.unassigned`	El número de particiones que no se asignaron a los nodos del clúster.
`DataNodesShards.initializing`	El número de particiones que se encuentran en inicialización.
`DataNodesShards.relocating`	El número de particiones que se encuentran en reubicación.

Métricas de rotación de zonas de disponibilidad

Si `ActiveReads.`*`Availability-Zone`*` = 1`, entonces la zona está activa. Si `ActiveReads.`*`Availability-Zone`*` = 0`, entonces la zona está en espera.

Métricas de un momento dado

Amazon OpenSearch Service ofrece las siguientes métricas para la búsqueda en un momento dado (PIT).

Estadísticas del nodo coordinador de PIT (por nodo coordinador)

Métrica	Descripción
`CurrentPointInTime`	El número de contextos de búsqueda PIT activos en el nodo.
`TotalPointInTime`	El número de contextos de búsqueda PIT caducados desde el tiempo de actividad del nodo.
`AvgPointInTimeAliveTime`	El keep-alive promedio de los contextos de búsqueda PIT desde el tiempo de actividad del nodo.
`HasActivePointInTime`	Un valor de 1 indica que hay contextos PIT activos en los nodos desde el tiempo de actividad del nodo. Un valor de 0 indica que no hay.
`HasUsedPointInTime`	Un valor de 1 indica que hay contextos PIT vencidos en los nodos desde el tiempo de actividad del nodo. Un valor de 0 indica que no hay.

Métricas de SQL

Amazon OpenSearch Service ofrece las siguientes métricas para la compatibilidad con SQL.

Métrica	Descripción
`SQLFailedRequestCountByCusErr`	El número de solicitudes a la API `_sql` que no se han realizado correctamente debido a un problema del cliente. Por ejemplo, una solicitud podría devolver el código de estado HTTP 400 debido a una excepción `IndexNotFoundException` . Estadísticas pertinentes: suma

Métrica	Descripción
`SQLFailedRequestCountBySysErr`	El número de solicitudes a la API `_sql` que no se han realizado correctamente debido a un problema del servidor o a una limitación de características. Por ejemplo, una solicitud podría devolver el código de estado HTTP 503 debido a una excepción `VerificationException` . Estadísticas pertinentes: suma
`SQLRequestCount`	El número de solicitudes a la API `_sql`. Estadísticas pertinentes: suma
`SQLDefaultCursorRequestCount`	Similar a `SQLRequestCount` , pero solo cuenta las solicitudes de paginación. Estadísticas pertinentes: suma
`SQLUnhealthy`	Un valor de 1 indica que, en respuesta a ciertas solicitudes, el complemento SQL devuelve códigos de respuesta 5xx o pasa DSL de consulta no válida a OpenSearch. Las demás solicitudes deberían realizarse correctamente. Un valor de 0 indica que no hay errores recientes. Si aparece sistemáticamente un valor de 1, solucione los problemas en las solicitudes que sus clientes están realizando al complemento. Estadísticas pertinentes: máximo

Métricas k-NN

Amazon OpenSearch Service incluye las siguientes métricas para el complemento k-nearest neighbor (k-NN).

Métrica	Descripción
KNNCacheCapacityReached	Métrica por nodo para saber si se alcanzó la capacidad de caché. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: máximo
KNNCircuitBreakerTriggered	Métrica por clúster para saber si se activa el disyuntor. Si algún nodo devuelve un valor de 1 para KNNCacheCapacityReached , este valor también devolverá 1. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: máximo
KNNEvictionCount	Métrica por nodo para el número de gráficos que se expulsaron de la caché debido a limitaciones de memoria o tiempo de inactividad. Las expulsiones explícitas que se producen debido a la eliminación de indexación no se cuentan. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma
KNNGraphIndexErrors	Métrica por nodo para el número de solicitudes para agregar el campo knn_vector de un documento a un gráfico que produjo un error. Estadísticas pertinentes: suma
KNNGraphIndexRequests	Métrica por nodo para el número de solicitudes para agregar el campo knn_vector de un documento a un gráfico. Estadísticas pertinentes: suma
KNNGraphMemoryUsage	Métrica por nodo para el tamaño actual de caché (tamaño total de todos los gráficos en memoria) en kilobytes. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: promedio

Métrica	Descripción
KNNGraphQueryErrors	Métrica por nodo para el número de consultas de gráficos que produjeron un error. Estadísticas pertinentes: suma
KNNGraphQueryRequests	Métrica por nodo para el número de consultas de gráficos. Estadísticas pertinentes: suma
KNNHitCount	Métrica por nodo para el número de aciertos de caché. Un acierto de caché se produce cuando un usuario consulta un gráfico que ya está cargado en la memoria. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma
KNNLoadExceptionCount	Métrica por nodo para el número de veces que se produjo una excepción al intentar cargar un gráfico en la caché. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma
KNNLoadSuccessCount	Métrica por nodo para el número de veces que el complemento cargó correctamente un gráfico en la caché. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma
KNNMissCount	Métrica por nodo para el número de errores de caché. Un error de caché se produce cuando un usuario consulta un gráfico que aún no está cargado en la memoria. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma

Métrica	Descripción
KNNQueryRequests	Métrica por nodo para el número de solicitudes de consulta que recibió el complemento k-NN. Estadísticas pertinentes: suma
KNNScriptCompilationErrors	Métrica por nodo para el número de errores durante la compilación del script. Esta estadística solo es relevante para la búsqueda de scripts de puntuación k-NN. Estadísticas pertinentes: suma
KNNScriptCompilations	Métrica por nodo para el número de veces que se ha compilado el script k-NN. Por lo general, este valor debe ser 1 o 0, pero si se llena la caché que contiene los scripts compilados, el script k-NN podría ser recompilado. Esta estadística solo es relevante para la búsqueda de scripts de puntuación k-NN. Estadísticas pertinentes: suma
KNNScriptQueryErrors	Métrica por nodo para el número de errores durante las consultas de scripts. Esta estadística solo es relevante para la búsqueda de scripts de puntuación k-NN. Estadísticas pertinentes: suma
KNNScriptQueryRequests	Métrica por nodo para el número total de consultas de script. Esta estadística solo es relevante para la búsqueda de scripts de puntuación k-NN. Estadísticas pertinentes: suma
KNNTotalLoadTime	El tiempo en nanosegundos que k-NN tardó en cargar gráficos en la caché. Esta métrica solo es pertinente para la búsqueda aproximada de k-NN. Estadísticas pertinentes: suma

Métricas de búsqueda entre clústeres

Amazon OpenSearch Service ofrece las siguientes métricas para la búsqueda entre clústeres.

Métricas de dominio de origen

Métrica	Dimensión	Descripción
`CrossClusterOutboundConnections`	`ConnectionId`	Número de nodos conectados. Si la respuesta incluye uno o más dominios omitidos, utilice esta métrica para rastrear las conexiones que no estén en buen estado. Si este número cae a 0, entonces la conexión no está en buen estado.
`CrossClusterOutboundRequests`	`ConnectionId`	El número de peticiones de búsqueda enviadas al dominio de destino. Utilícelo para comprobar si la carga de peticiones de búsqueda en clústeres está sobrecargando su dominio, correlacione cualquier pico en esta métrica con cualquier pico JVM/CPU.

Métrica de dominio de destino

Métrica	Dimensión	Descripción
`CrossClusterInboundRequests`	`ConnectionId`	El número de solicitudes de conexión entrantes recibidas desde el dominio de origen.

Agregue una alarma de CloudWatch en caso de que pierda una conexión de forma inesperada. Para ver los pasos para crear una alarma, consulte Crear una alarma de CloudWatch basada en un umbral estático.

Métricas de replicación entre clústeres

Amazon OpenSearch Service ofrece las siguientes métricas para la replicación entre clústeres.

Métrica	Descripción
`ReplicationRate`	La tasa media de operaciones de replicación por segundo. Esta métrica es similar a `IndexingRate` .
`LeaderCheckPoint`	Para lograr una conexión específica, la suma de los valores de punto de control líder entre todos los índices de replicación. Puede utilizar esta métrica para medir la latencia de replicación.
`FollowerCheckPoint`	Para lograr una conexión específica, la suma de los valores de punto de control seguidor entre todos los índices de replicación. Puede utilizar esta métrica para medir la latencia de replicación.
`ReplicationNumSyncingIndices`	El número de índices que tienen un estado de replicación de `SYNCING`.
`ReplicationNumBootstrappingIndices`	El número de índices que tienen un estado de replicación de `BOOTSTRAPPING` .
`ReplicationNumPausedIndices`	El número de índices que tienen un estado de replicación de `PAUSED`.
`ReplicationNumFailedIndices`	El número de índices que tienen un estado de replicación de `FAILED`.
`CrossClusterOutboundReplicationRequests`	El número de solicitudes de transporte de replicación en el dominio seguidor. Las solicitudes de transporte son internas y se producen cada vez que se llama una operación de la API de replicación. También se producen cuando el dominio seguidor sondea los cambios con respecto al dominio líder.

Métrica	Descripción
`CrossClusterInboundReplicationRequests`	El número de solicitudes de transporte de replicación en el dominio principal. Las solicitudes de transporte son internas y se producen cada vez que se llama una operación de API de replicación.
`AutoFollowNumSuccessStartReplication`	El número de índices de seguidores que ha creado correctamente una regla de replicación para una conexión específica.
`AutoFollowNumFailedStartReplication`	El número de índices de seguidores que no pudo crear una regla de replicación cuando había un patrón coincidente. Este problema puede deberse a un problema de red en el clúster remoto o a un problema de seguridad (es decir, el rol asociado no tiene permiso para iniciar la replicación).
`AutoFollowLeaderCallFailure`	Si ha habido alguna consulta fallida del índice de seguidores al índice de líderes para obtener nuevos datos. Un valor de 1 significa que ha habido 1 o más llamadas fallidas en el último minuto.

Aprender a clasificar métricas

Amazon OpenSearch Service ofrece las siguientes métricas para aprender a clasificar.

Métrica	Descripción
`LTRRequestTotalCount`	Recuento total de solicitudes de clasificación.
`LTRRequestErrorCount`	Recuento total de solicitudes fallidas.
`LTRStatus.red`	Comprueba si uno de los índices necesarios para ejecutar el complemento es rojo.

Métrica	Descripción
`LTRMemoryUsage`	Memoria total utilizada por el complemento.
`LTRFeaturMemoryUsageInBytes`	La cantidad de memoria, en bytes, utilizada por los campos de características de Learning to Rank (Aprender a clasificar).
`LTRFeaturesetMemoryUsageInBytes`	La cantidad de memoria, en bytes, que utiliza todos los conjuntos de características de Learning to Rank (Aprender a clasificar).
`LTRModelMemoryUsageInBytes`	La cantidad de memoria, en bytes, utilizada por todos los modelos Learning to Rank (Aprender a clasificar).

Métricas del lenguaje de procesamiento de canalizaciones

Amazon OpenSearch Service ofrece las siguientes métricas para el lenguaje de procesamiento de canalizaciones.

Métrica	Descripción
`PPLFailedRequestCountByCusErr`	El número de solicitudes a la API `_ppl` que no se han realizado correctamente debido a un problema del cliente. Por ejemplo, una solicitud podría devolver el código de estado HTTP 400 debido a una excepción `IndexNotFoundException` .
`PPLFailedRequestCountBySysErr`	El número de solicitudes a la API `_ppl` que no se han realizado correctamente debido a un problema del servidor o a una limitación de características. Por ejemplo, una solicitud podría devolver el código de estado HTTP 503 debido a una excepción `VerificationException` .
`PPLRequestCount`	El número de solicitudes a la API `_ppl`.

Monitoreo de registros de OpenSearch con Registros de Amazon CloudWatch

Amazon OpenSearch Service expone los siguientes registros de OpenSearch a través de Registros de Amazon CloudWatch:

- Registros de errores
- Registros lentos
- Registros de auditoría

Los registros lentos de búsqueda, los registros lentos de índice y los registros de errores son útiles para la resolución de problemas de rendimiento y estabilidad. Los registros de auditoría realizan un seguimiento de la actividad de los usuarios con fines de conformidad. Todos los registros están deshabilitados de forma predeterminada. Si están habilitados, se aplica el precio estándar de CloudWatch.

> **Note**
>
> Los registros de errores solo están disponibles para la versión 5.1 de OpenSearch y Elasticsearch y posteriores. Los registros lentos están disponibles en todas las versiones de OpenSearch y Elasticsearch.

Para los registros, OpenSearch utiliza Apache Log4j 2 y sus niveles de registro integrados (de menor a mayor gravedad) `TRACE`, `DEBUG`, `INFO`, `WARN`, `ERROR` y `FATAL`.

Si habilita registros de errores, OpenSearch Service publica líneas de registro de `WARN`, `ERROR` y `FATAL` en CloudWatch. OpenSearch Service también publica varias excepciones del nivel `DEBUG`, incluido lo siguiente:

- `org.opensearch.index.mapper.MapperParsingException`
- `org.opensearch.index.query.QueryShardException`
- `org.opensearch.action.search.SearchPhaseExecutionException`
- `org.opensearch.common.util.concurrent.OpenSearchRejectedExecutionException`
- `java.lang.IllegalArgumentException`

Los registros de errores ayudan a solucionar problemas en muchas situaciones, entre las que se incluyen las siguientes:

- Problemas de compilación de script Painless
- Consultas no válidas
- Problemas de indexación
- Errores de instantáneas
- Fallas de migración de la administración de estados de índice

Temas

Habilitación de la publicación de registros (consola)

La consola de OpenSearch Service es la manera más sencilla de habilitar la publicación de registros en CloudWatch.

Para habilitar la publicación de registros en CloudWatch (consola)

1. Visite https://aws.amazon.com y elija Iniciar sesión en la consola.
2. En Análisis, elija Amazon OpenSearch Service.
3. Elija el dominio que desea actualizar.
4. En la pestaña Registros, seleccione un tipo de registro y luego elija Habilitar.
5. Cree un grupo de registros de CloudWatch o elija uno existente.

> **Note**
>
> Si prevé habilitar varios registros, recomendamos publicar cada uno en su propio grupo de registros. Esta separación hace que los registros sean más fáciles de analizar.

6. Elija una política de acceso que contenga los permisos adecuados o cree una política mediante el JSON que proporciona la consola:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn:*"
    }
  ]
}
```

Le recomendamos que agregue las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra la política problema del suplente confuso. La cuenta de origen es la propietaria del dominio y el ARN de origen es el ARN del dominio. Su dominio debe estar en el software de servicio R20211203 o posterior para agregar estas claves de condición.

Por ejemplo, podría agregar el siguiente bloque de condición a la política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

> **Important**
>
> CloudWatch Logs admite 10 políticas de recursos por región. Si planea habilitar los registros para varios dominios de OpenSearch Service, debe crear y reutilizar una política más amplia que incluya varios grupos de registros para evitar alcanzar este

límite. Para obtener información sobre los pasos para actualizar la política, consulte the section called “Habilitación de la publicación de registros (AWS CLI)”.

7. Elija Habilitar.

   El estado del dominio cambia de Activo a En proceso. El estado debe volver a Activo antes de que la publicación de registro esté habilitada. Este cambio suele tardar 30 minutos, pero puede tardar más en función de la configuración del dominio.

Si habilita uno de los registros lentos, consulte the section called “Configuración de umbrales de registro de OpenSearch para registros lentos”. Si habilitó registros de auditorías, consulte the section called “Paso 2: Activa los registros de auditoría en los OpenSearch paneles”. Si habilitó únicamente los registros de errores, no tiene que realizar ningún paso de configuración adicional.

Habilitación de la publicación de registros (AWS CLI)

Para poder habilitar la publicación de registros, necesita un grupo de registros de CloudWatch Logs. Si aún no lo tiene, puede crear uno mediante el siguiente comando:

```
aws logs create-log-group --log-group-name my-log-group
```

Introduzca el siguiente comando para encontrar el ARN del grupo de registros y, a continuación, anótelo:

```
aws logs describe-log-groups --log-group-name my-log-group
```

Ahora puede dar permisos a OpenSearch Service para escribir en el grupo de registros. Debe proporcionar el ARN del grupo de registros cerca del final del comando:

```
aws logs put-resource-policy \
  --policy-name my-policy \
  --policy-document '{ "Version": "2012-10-17", "Statement": [{ "Sid": "",
 "Effect": "Allow", "Principal": { "Service": "es.amazonaws.com"}, "Action":
[ "logs:PutLogEvents","logs:CreateLogStream"],"Resource": "cw_log_group_arn:*"}]}'
```

> **Important**
>
> CloudWatch Logs admite 10 políticas de recursos por región. Si planea habilitar registros lentos para varios dominios de OpenSearch Service, debe crear y reutilizar una política más amplia que incluya varios grupos de registros para evitar alcanzar este límite.

Si tiene que revisar esta política más adelante, utilice el comando `aws logs describe-resource-policies`. Para actualizar la política, ejecute el mismo comando `aws logs put-resource-policy` con un nuevo documento de política.

Finalmente, puede utilizar la opción `--log-publishing-options` para habilitar la publicación. La sintaxis de la opción es la misma para los comandos `create-domain` y `update-domain-config`.

Parámetro	Valores válidos
`--log-publishing-options`	`SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`ES_APPLICATION_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`
	`AUDIT_LOGS={CloudWatchLogsLogGroupArn= cw_log_group_arn ,Enabled=true|false}`

> **Note**
>
> Si prevé habilitar varios registros, recomendamos publicar cada uno en su propio grupo de registros. Esta separación hace que los registros sean más fáciles de analizar.

Ejemplo

En el siguiente ejemplo se habilita la publicación de los registros lentos de búsqueda e índice para el dominio especificado:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --log-publishing-options
 "SEARCH_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-
group,Enabled=true},INDEX_SLOW_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-
east-1:123456789012:log-group:my-other-log-group,Enabled=true}"
```

Para deshabilitar la publicación en CloudWatch, ejecute el mismo comando con `Enabled=false`.

Si habilita uno de los registros lentos, consulte the section called “Configuración de umbrales de registro de OpenSearch para registros lentos”. Si habilitó registros de auditorías, consulte the section called “Paso 2: Activa los registros de auditoría en los OpenSearch paneles”. Si habilitó únicamente los registros de errores, no tiene que realizar ningún paso de configuración adicional.

Habilitación de la publicación de registros (SDK de AWS)

Para habilitar la publicación de registros, primero debe crear un grupo de registros de CloudWatch, obtener su ARN y otorgar permisos a OpenSearch Service para escribir en ella. Las operaciones pertinentes se documentan en la Referencia de la API de Amazon CloudWatch Logs:

- `CreateLogGroup`
- `DescribeLogGroup`
- `PutResourcePolicy`

Puede obtener acceso a estas operaciones mediante los SDK de AWS.

Los AWS SDK (excepto los de Android e iOS SDK) admiten todas las operaciones definidas en la Referencia de la API de Amazon OpenSearch Service, incluida la opción `--log-publishing-options` para `CreateDomain` y `UpdateDomainConfig`.

Si habilita uno de los registros lentos, consulte the section called “Configuración de umbrales de registro de OpenSearch para registros lentos”. Si habilitó únicamente los registros de errores, no tiene que realizar ningún paso de configuración adicional.

Habilitar publicación de registros (CloudFormation)

En este ejemplo, se utiliza CloudFormation para crear un grupo de registros llamado `opensearch-logs`, se asignan los permisos adecuados y, a continuación, se crea un dominio con la publicación

de registros habilitada para registros de aplicaciones, registros lentos de búsqueda y registros lentos de índice.

Para poder habilitar la publicación de registros, hay que crear un grupo de registros de CloudWatch:

```
Resources:
  OpenSearchLogGroup:
    Type: AWS::Logs::LogGroup
    Properties:
      LogGroupName: opensearch-logs
Outputs:
  Arn:
    Value:
      'Fn::GetAtt':
        - OpenSearchLogGroup
        - Arn
```

La plantilla genera el ARN del grupo de registros. En este caso, el ARN es `arn:aws:logs:us-east-1:123456789012:log-group:opensearch-logs`.

Mediante el ARN, cree una política de recursos que dé permisos a OpenSearch Service para escribir en el grupo de registros:

```
Resources:
 OpenSearchLogPolicy:
   Type: AWS::Logs::ResourcePolicy
   Properties:
     PolicyName: my-policy
     PolicyDocument: "{ \"Version\": \"2012-10-17\", \"Statement\": [{ \"Sid\": \"\",
 \"Effect\": \"Allow\", \"Principal\": { \"Service\": \"es.amazonaws.com\"}, \"Action
\":[ \"logs:PutLogEvents\",\"logs:CreateLogStream\"],\"Resource\": \"arn:aws:logs:us-
east-1:123456789012:log-group:opensearch-logs:*\"}]}"
```

Por último, cree la siguiente pila de CloudFormation, que genera un dominio de OpenSearch Service con publicación de registros. La política de acceso permite al usuario de la Cuenta de AWS realizar todas las solicitudes HTTP al dominio.

```
Resources:
  OpenSearchServiceDomain:
    Type: "AWS::OpenSearchService::Domain"
    Properties:
```

```
      DomainName: my-domain
      EngineVersion: "OpenSearch_1.0"
      ClusterConfig:
        InstanceCount: 2
        InstanceType: "r6g.xlarge.search"
        DedicatedMasterEnabled: true
        DedicatedMasterCount: 3
        DedicatedMasterType: "r6g.xlarge.search"
      EBSOptions:
        EBSEnabled: true
        VolumeSize: 10
        VolumeType: "gp2"
      AccessPolicies:
        Version: "2012-10-17"
        Statement:
            Effect: "Allow"
            Principal:
                AWS: "arn:aws:iam::123456789012:user/es-user"
            Action: "es:*"
            Resource: "arn:aws:es:us-east-1:123456789012:domain/my-domain/*"
      LogPublishingOptions:
        ES_APPLICATION_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        SEARCH_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
        INDEX_SLOW_LOGS:
          CloudWatchLogsLogGroupArn: "arn:aws:logs:us-east-1:123456789012:log-
group:opensearch-logs"
          Enabled: true
```

Para obtener información detallada sobre la sintaxis, consulte las opciones de publicación de registros en la Guía del usuario de AWS CloudFormation.

Configuración de umbrales de registro de OpenSearch para registros lentos

OpenSearch deshabilita los registros lentos de forma predeterminada. Después de habilitar la publicación de registros lentos en CloudWatch, aún necesita especificar los umbrales de registro para cada índice de OpenSearch. Estos umbrales definen exactamente lo que se debe registrar y el nivel de registro.

Debe especificar esta configuración a través de la API de REST de OpenSearch:

```
PUT domain-endpoint/index/_settings
{
  "index.search.slowlog.threshold.query.warn": "5s",
  "index.search.slowlog.threshold.query.info": "2s"
}
```

Para verificar que los registros lentos se publican correctamente, considere empezar con valores muy bajos para verificar que los registros aparecen en CloudWatch y, a continuación, aumente los umbrales a niveles más útiles.

Si los registros no aparecen, verifique lo siguiente:

- ¿Existe el grupo de registros de CloudWatch? Verifique la consola de CloudWatch.
- ¿OpenSearch Service tiene permisos para escribir en el grupo de registros? Verifique la consola de OpenSearch Service.
- ¿El dominio de OpenSearch Service está configurado para publicar en el grupo de registros? Verifique la consola de OpenSearch Service, utilice la opción AWS CLI de `describe-domain-config` o llame a `DescribeDomainConfig` mediante uno de los SDK.
- ¿Los umbrales de registro de OpenSearch son tan bajos que las solicitudes los superan? Para revisar los umbrales de un índice, utilice el siguiente comando:

  ```
  GET domain-endpoint/index/_settings?pretty
  ```

Si desea deshabilitar los registros lentos de un índice, devuelva los umbrales que ha cambiado a sus valores predeterminados de `-1`.

Deshabilitar la publicación en CloudWatch mediante la consola de OpenSearch Service o AWS CLI no impide la generación de registros por parte de OpenSearch; solo se detiene la publicación de esos registros. Asegúrese de verificar la configuración de su índice si ya no necesita registros lentos.

Visualización de registros

La visualización de la aplicación y de los registros lentos en CloudWatch es exactamente igual que la visualización de cualquier otro registro de CloudWatch. Para más información, consulte Visualización de datos de registro en la Guía del usuario de Registros de Amazon CloudWatch.

Aquí tiene algunas consideraciones para visualizar los registros:

- OpenSearch Service publica solo los primeros 255 000 caracteres de cada línea en CloudWatch. El contenido restante está truncado. Para los registros de auditoría, son 10 000 caracteres por mensaje.
- En CloudWatch, los nombres del flujo de registro tienen los sufijos `-index-slow-logs`, `-search-slow-logs`, `-application-logs` y `-audit-logs` para ayudar a identificar su contenido.

Supervisión de los registros de auditoría en Amazon OpenSearch Service

Si tu dominio de Amazon OpenSearch Service utiliza un control de acceso detallado, puedes habilitar los registros de auditoría para tus datos. Los registros de auditoría son altamente personalizables y te permiten realizar un seguimiento de la actividad de los usuarios en tus OpenSearch clústeres, incluidas las autenticaciones correctas y fallidas, las solicitudes, los cambios de indexación y las consultas de búsqueda entrantes. OpenSearch La configuración predeterminada realiza un seguimiento de un conjunto común de acciones de usuario, pero recomendamos adaptar la configuración a las necesidades exactas.

Al igual que los registros de OpenSearch aplicaciones y los registros lentos, OpenSearch Service publica los registros de auditoría en CloudWatch Logs. Si está activado, se aplica el CloudWatch precio estándar.

> **Note**
>
> Para habilitar los registros de auditoría, su rol de usuario debe estar asignado al `security_manager` rol, lo que le da acceso a la API OpenSearch `plugins/_security` REST. Para obtener más información, consulte the section called “Modificar el usuario maestro”.

Temas

- Limitaciones
- Habilitación de los registros de auditoría
- Habilite el registro de auditorías mediante AWS CLI

- Habilite el registro de auditoría con la API de configuración
- Categorías y capas de registro de auditoría
- Configuración de registros de auditoría
- Ejemplo de registro de auditoría
- Configuración de registros de auditoría mediante la API REST

Limitaciones

Los registros de auditoría presentan las siguientes limitaciones:

- Los registros de auditoría no incluyen peticiones de búsqueda entre clústeres rechazadas por la política de acceso al dominio de destino.
- El tamaño máximo de cada mensaje de registro de auditoría es de 10 000 caracteres. El mensaje del registro de auditoría se trunca si se supera este límite.

Habilitación de los registros de auditoría

La habilitación de registros de auditoría es un proceso de dos pasos. En primer lugar, debe configurar su dominio para publicar los registros de auditoría en CloudWatch Logs. A continuación, habilita los registros de auditoría en los OpenSearch paneles de control y los configura para que se adapten a sus necesidades.

> **Important**
>
> Si encuentra un error al seguir estos pasos, consulte the section called “No se pueden habilitar los registros de auditoría” para obtener información para la resolución de problemas.

Paso 1: Habilitar los registros de auditoría y configurar una política de acceso

En estos pasos se describe cómo habilitar los registros de auditoría con la consola. También puede habilitarlos mediante la AWS CLI API de servicio o la API de OpenSearch servicio.

Para habilitar los registros de auditoría para un dominio de OpenSearch servicio (consola)

1. Seleccione el dominio para abrir su configuración y, a continuación, vaya a la pestaña Registros.

2. Seleccione Registros de auditoría y, luego Habilitar.
3. Cree un grupo de CloudWatch registros o elija uno existente.
4. Seleccione una política de acceso que contenga los permisos adecuados o cree una política mediante el JSON que proporciona la consola:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "es.amazonaws.com"
      },
      "Action": [
        "logs:PutLogEvents",
        "logs:CreateLogStream"
      ],
      "Resource": "cw_log_group_arn"
    }
  ]
}
```

Le recomendamos que agregue las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra la política problema del suplente confuso. La cuenta de origen es la propietaria del dominio y el ARN de origen es el ARN del dominio. Su dominio debe estar en el software de servicio R20211203 o posterior para agregar estas claves de condición.

Por ejemplo, podría agregar el siguiente bloque de condición a la política:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

5. Seleccione Habilitar.

Paso 2: Activa los registros de auditoría en los OpenSearch paneles

Después de habilitar los registros de auditoría en la consola de OpenSearch servicio, también debe habilitarlos en los OpenSearch paneles y configurarlos para que se adapten a sus necesidades.

1. Abre los OpenSearch paneles de control y selecciona Seguridad en el menú de la izquierda.
2. Seleccione Registros de auditoría.
3. Seleccione Habilitar registro de auditoría.

La interfaz de usuario de Dashboards ofrece un control total de la configuración del registro de auditoría en Configuración general y en Configuración de la conformidad. Para obtener una descripción de todas las opciones de configuración, consulte Configuración del registro de auditoría.

Habilite el registro de auditorías mediante AWS CLI

El siguiente AWS CLI comando habilita los registros de auditoría en un dominio existente:

```
aws opensearch update-domain-config --domain-name my-domain --log-publishing-options
 "AUDIT_LOGS={CloudWatchLogsLogGroupArn=arn:aws:logs:us-east-1:123456789012:log-
group:my-log-group,Enabled=true}"
```

También puede habilitar registros de auditoría al crear un dominio. Para obtener más información, consulte la Referencia de comandos de laAWS CLI.

Habilite el registro de auditoría con la API de configuración

La siguiente solicitud a la API de configuración habilita los registros de auditoría en un dominio existente:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "LogPublishingOptions": {
    "AUDIT_LOGS": {
      "CloudWatchLogsLogGroupArn":"arn:aws:logs:us-east-1:123456789012:log-
group1:sample-domain",
      "Enabled":true
    }
  }
```

```
}
```

Para obtener más información, consulta la referencia de la API OpenSearch de Amazon Service.

Categorías y capas de registro de auditoría

La comunicación del clúster se produce a través de dos capas independientes: la capa REST y la capa de transporte.

- La capa REST cubre la comunicación con clientes HTTP como curl, Logstash, OpenSearch Dashboards, el cliente REST de alto nivel de Java y la biblioteca de solicitudes de Python, todas las solicitudes HTTP que llegan al clúster.
- La capa de transporte se encarga de la comunicación entre nodos. Por ejemplo, después de que una petición de búsqueda llega al clúster (en la capa REST), el nodo de coordinación que se encarga de la solicitud envía la consulta a otros nodos, recibe sus respuestas, reúne los documentos necesarios y los reúne en la respuesta final. Las operaciones como la asignación de particiones y el reequilibrio también se producen en la capa de transporte.

Puede habilitar o deshabilitar los registros de auditoría para capas enteras, así como las categorías de auditoría individuales de una capa. La siguiente tabla contiene un resumen de las categorías de auditoría y las capas para las que están disponibles.

Categoría	Descripción	Disponible para REST	Disponible para transporte
FAILED_LOGIN	Una solicitud contenía credenciales no válidas y la autenticación falló.	Sí	Sí
MISSING_PRIVILEGES	Un usuario no poseía los privilegios para realizar la solicitud.	Sí	Sí
GRANTED_PRIVILEGES	Un usuario poseía los privilegios para realizar la solicitud.	Sí	Sí

Categoría	Descripción	Disponible para REST	Disponible para transporte
OPENSEARCH_SECURITY_INDEX_ATTEMPT	Una solicitud intentó modificar el índice `.opendistro_security` .	No	Sí
AUTHENTICATED	Una solicitud contenía credenciales válidas y la autenticación se realizó correctamente.	Sí	Sí
INDEX_EVENT	Una solicitud realizó una operación administrativa con un índice, como crearlo, establecer un alias o realizar una combinación de fuerza. La lista completa de `indices:admin/` acciones que incluye esta categoría está disponible en la documentación. OpenSearch	No	Sí

Además de estas categorías estándar, el control de acceso detallado ofrece varias categorías adicionales diseñadas para cumplir con los requisitos de conformidad de los datos.

Categoría	Descripción
COMPLIANCE_DOC_READ	Una solicitud realizó un evento de lectura en un documento en un índice.

Categoría	Descripción
COMPLIANCE_DOC_WRITE	Una solicitud realizó un evento de escritura en un documento en un índice.
COMPLIANCE_INTERNAL_CONFIG_READ	Una solicitud realizó un evento de lectura en el índice `.opendistro_security` .
COMPLIANCE_INTERNAL_CONFIG_WRITE	Una solicitud realizó un evento de escritura en el índice `.opendistro_security` .

Puede utilizar cualquier combinación de categorías y atributos de mensaje. Por ejemplo, si envía una solicitud REST para indexar un documento, podría ver las siguientes líneas en los registros de auditoría:

- AUTHENTICATED en la capa REST (autenticación)
- GRANTED_PRIVILEGE en la capa de transporte (autorización)
- COMPLIANCE_DOC_WRITE (documento escrito en un índice)

Configuración de registros de auditoría

Los registros de auditoría cuentan con numerosas opciones de configuración.

Configuración general

La configuración general permite habilitar o deshabilitar categorías individuales o capas enteras. Recomendamos encarecidamente mantener GRANTED_PRIVILEGES y AUTHENTICATED como categorías excluidas. De lo contrario, estas categorías se registran en cada solicitud válida al clúster.

Nombre	Configuración del backend	Descripción
Capa REST	enable_rest	Habilite o deshabilite los eventos que se producen en la capa REST.

Nombre	Configuración del backend	Descripción
Categorías REST deshabilitadas	disabled_rest_categories	Especifique las categorías de auditoría que se omitirán en la capa REST. La modificación de estas categorías puede aumentar drásticamente el tamaño de los registros de auditoría.
Capa de transporte	enable_transport	Habilite o deshabilite eventos que ocurren en la capa de transporte.
Categorías de transporte deshabilitadas	disabled_transport_categories	Especifique las categorías de auditoría que deben omitirse en la capa de transporte. La modificación de estas categorías puede aumentar drásticamente el tamaño de los registros de auditoría.

La configuración de atributos permite personalizar la cantidad de detalles en cada línea de registro.

Nombre	Configuración del backend	Descripción
Solicitudes masivas	resolve_bulk_requests	Habilitar esta configuración genera un registro para cada documento de una solicitud masiva, lo que puede aumentar drásticamente el tamaño de los registros de auditoría.
Cuerpo de la solicitud	log_request_body	Incluya el cuerpo de la solicitud de las solicitudes.
Resolver índices	resolve_indices	Resolver alias a índices.

Utilice la configuración de ignorar para excluir un conjunto de usuarios o rutas de API:

Nombre	Configuración del backend	Descripción
Usuarios ignorados	ignore_users	Especifique los usuarios que desea excluir.
Solicitudes ignoradas	ignore_requests	Especifique los patrones de solicitud que desea excluir.

Configuración de la conformidad

La configuración de la conformidad permite ajustar el acceso a nivel del índice, del documento o del campo.

Nombre	Configuración del backend	Descripción
Registro de conformidad	enable_compliance	Para habilitar o deshabilitar el registro de conformidad.

Puede especificar la siguiente configuración para el registro de eventos de lectura y escritura.

Nombre	Configuración del backend	Descripción
Registro de configuración interno	internal_config	Habilite o deshabilite el registro de eventos en el índice `.opendistro_security` .

Puede especificar la siguiente configuración para el registro de eventos de lectura.

Nombre	Configuración del backend	Descripción
Metadatos de lectura	read_metadata_only	Incluya solo metadatos para eventos de lectura. No incluya ningún campo de documento.
Usuarios ignorados	read_ignore_users	No incluya ciertos usuarios para eventos de lectura.
Campos observados	read_watched_fields	Especifique los índices y campos que se van a observar en busca de eventos de lectura. Agregar campos vigilados genera un registro por cada acceso a los documentos, lo que puede aumentar drásticamente el tamaño de los registros de auditoría. Los campos observados admiten patrones de índice y patrones de campo: `{ "index-name-pattern": [ "field-name-pattern" ], "logs*": [ "message" ], "twitter": [ "id", "user*" ] }`

Puede especificar la siguiente configuración para eventos de escritura.

Nombre	Configuración del backend	Descripción
Metadatos de escritura	write_metadata_only	Incluya solo metadatos para eventos de escritura. No incluya ningún campo de documento.

Nombre	Configuración del backend	Descripción
Diferencias de registro	write_log_diffs	Si write_metadata_only es falso, incluya solo las diferencias entre los eventos de escritura.
Usuarios ignorados	write_ignore_users	No incluya ciertos usuarios para eventos de escritura.
Índices de seguimiento	write_watched_indices	Especifique los índices o patrones de índice para observar los eventos de escritura. Agregar campos vigilados genera un registro por cada acceso a los documentos, lo que puede aumentar drásticamente el tamaño de los registros de auditoría.

Ejemplo de registro de auditoría

Esta sección incluye un ejemplo de configuración, una petición de búsqueda y el registro de auditoría resultante para todos los eventos de lectura y escritura de un índice.

Paso 1: configurar los registros de auditoría

Después de habilitar la publicación de los registros de auditoría en un grupo de CloudWatch registros, vaya a la página de registro de auditorías del OpenSearch panel de control y seleccione Habilitar el registro de auditoría.

1. En Configuración general, seleccione Configurar y asegúrese de que la capa REST esté habilitada.
2. En Configuración de la conformidad, seleccione Configurar.
3. En Escritura, en Campos observados, agregue `accounts` para todos los eventos de escritura en este índice.
4. En Lectura, en Campos observados, agregue los campos `ssn` y `id-` del índice`accounts`:

```
{
  "accounts-": [
    "ssn",
    "id-"
  ]
```

```
}
```

Paso 2: realizar eventos de lectura y escritura

1. Diríjase a OpenSearch los paneles, elija Herramientas de desarrollo e indexe un documento de muestra:

```
PUT accounts/_doc/0
{
  "ssn": "123",
  "id-": "456"
}
```

2. Para probar un evento de lectura, envíe la siguiente solicitud:

```
GET accounts/_search
{
  "query": {
    "match_all": {}
  }
}
```

Paso 3: observar los registros

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Grupos de registro.
3. Seleccione el grupo de registros que especificó al habilitar registros de auditoría. Dentro del grupo de registros, OpenSearch Service crea un flujo de registros para cada nodo de su dominio.
4. En Flujos de registros, seleccione Buscar todos.
5. Para los eventos de lectura y escritura, consulte los registros correspondientes. Puede existir una demora de 5 segundos antes de que aparezca el registro.

   Ejemplo de registro de auditoría de escritura

```
{
  "audit_compliance_operation": "CREATE",
  "audit_cluster_name": "824471164578:audit-test",
```

```
  "audit_node_name": "be217225a0b77c2bd76147d3ed3ff83c",
  "audit_category": "COMPLIANCE_DOC_WRITE",
  "audit_request_origin": "REST",
  "audit_compliance_doc_version": 1,
  "audit_node_id": "3xNJhm4XS_yTzEgDWcGRjA",
  "@timestamp": "2020-08-23T05:28:02.285+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "3.236.145.227",
  "audit_trace_doc_id": "lxnJGXQBqZSlDB91r_uZ",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 8,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

Ejemplo de registro de auditoría de lectura

```
{
  "audit_cluster_name": "824471164578:audit-docs",
  "audit_node_name": "806f6050cb45437e2401b07534a1452f",
  "audit_category": "COMPLIANCE_DOC_READ",
  "audit_request_origin": "REST",
  "audit_node_id": "saSevm9ASte0-pjAtYi2UA",
  "@timestamp": "2020-08-31T17:57:05.015+00:00",
  "audit_format_version": 4,
  "audit_request_remote_address": "54.240.197.228",
  "audit_trace_doc_id": "config:7.7.0",
  "audit_request_effective_user": "admin",
  "audit_trace_shard_id": 0,
  "audit_trace_indices": [
    "accounts"
  ],
  "audit_trace_resolved_indices": [
    "accounts"
  ]
}
```

Para incluir el cuerpo de la solicitud, vuelva a la configuración de conformidad en los OpenSearch paneles y desactive Escribir metadatos. Para excluir eventos de un usuario específico, agregue el usuario a Usuarios ignorados.

Para obtener una descripción de cada campo de registro de auditoría, consulte la Referencia de campo del registro de auditoría. Para obtener información sobre la búsqueda y el análisis de los datos del registro de auditoría, consulte Análisis de los datos de registro con CloudWatch Logs Insights en la Guía del usuario de Amazon CloudWatch Logs.

Configuración de registros de auditoría mediante la API REST

Recomendamos usar OpenSearch paneles de control para configurar los registros de auditoría, pero también puede usar la API REST de control de acceso detallada. Esta sección contiene una solicitud de ejemplo. La documentación completa sobre la API REST está disponible en la documentación. OpenSearch

```
PUT _plugins/_security/api/audit/config
{
  "enabled": true,
  "audit": {
    "enable_rest": true,
    "disabled_rest_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "enable_transport": true,
    "disabled_transport_categories": [
      "GRANTED_PRIVILEGES",
      "AUTHENTICATED"
    ],
    "resolve_bulk_requests": true,
    "log_request_body": true,
    "resolve_indices": true,
    "exclude_sensitive_headers": true,
    "ignore_users": [
      "kibanaserver"
    ],
    "ignore_requests": [
      "SearchRequest",
      "indices:data/read/*",
      "/_cluster/health"
    ]
```

```
  },
  "compliance": {
    "enabled": true,
    "internal_config": true,
    "external_config": false,
    "read_metadata_only": true,
    "read_watched_fields": {
      "read-index-1": [
        "field-1",
        "field-2"
      ],
      "read-index-2": [
        "field-3"
      ]
    },
    "read_ignore_users": [
      "read-ignore-1"
    ],
    "write_metadata_only": true,
    "write_log_diffs": false,
    "write_watched_indices": [
      "write-index-1",
      "write-index-2",
      "log-*",
      "*"
    ],
    "write_ignore_users": [
      "write-ignore-1"
    ]
  }
}
```

Monitorización OpenSearch de eventos del servicio con Amazon EventBridge

Amazon OpenSearch Service se integra con Amazon EventBridge para notificarte determinados eventos que afectan a tus dominios. Los eventos de AWS los servicios se envían casi EventBridge en tiempo real. Los mismos eventos también se envían a Amazon CloudWatch Events, la predecesora de Amazon EventBridge. 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. Entre las acciones que se pueden activar automáticamente se incluyen las siguientes:

- Invocar una función AWS Lambda
- Invocar un Run Command de Amazon EC2
- Desviar el evento a Amazon Kinesis Data Streams
- Activación de una máquina de estados AWS Step Functions
- Notificar un tema de Amazon SNS o una cola de Amazon SQS

Para obtener más información, consulta Cómo empezar con Amazon EventBridge en la Guía del EventBridge usuario de Amazon.

Temas

- Eventos de actualización del software de servicio
- Eventos de ajuste automático
- Eventos del estado del clúster
- Eventos del punto de conexión de VPC
- Eventos de retirada de nodos
- Eventos de error de dominio
- Tutorial: Cómo escuchar los EventBridge eventos OpenSearch de Amazon Service
- Tutorial: Sending Amazon SNS alerts for available software updates

Eventos de actualización del software de servicio

OpenSearch El servicio envía los eventos EventBridge cuando se produce uno de los siguientes eventos de actualización del software del servicio.

Actualización del software de servicio disponible

OpenSearch El servicio envía este evento cuando hay disponible una actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Available",
    "severity": "Informational",
    "description": "Service software update R20220928 available. Service Software
 Deployment Mechanism:
                   Blue/Green. For more information on deployment configuration,
 please
                   see: https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Actualización del software de servicio programada

OpenSearch El servicio envía este evento cuando se ha programado una actualización del software del servicio. En el caso de las actualizaciones opcionales, recibirá la notificación en la fecha programada y tendrá la opción de volver a programarla en cualquier momento. En el caso de las actualizaciones obligatorias, recibirá la notificación tres días antes de la fecha programada y tendrá la opción de reprogramarla dentro del plazo obligatorio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
```

```
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Scheduled",
    "severity": "High",
    "description": "A new service software update [R20200330-p1] has been scheduled at
 [21st May 2023 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Actualización del software de servicio reprogramada

OpenSearch El servicio envía este evento cuando se ha reprogramado una actualización opcional del software del servicio. Para obtener más información, consulte the section called “Actualizaciones opcionales frente a actualizaciones obligatorias”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Rescheduled",
    "severity": "High",
    "description": "The service software update [R20200330-p1], which was originally
 scheduled for
                    [21st May 2023 12:40 GMT], has been rescheduled to [23rd May 2023
 12:40 GMT].
                    Please see documentation for more information on scheduling
 software updates:
```

```
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/service-software.html."
  }
}
```

Actualización del software de servicio comenzada

OpenSearch El servicio envía este evento cuando se inicia una actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Started",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] started.
  }
}
```

Actualización del software de servicio finalizada

OpenSearch El servicio envía este evento cuando se completa la actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
```

```
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Completed",
    "severity": "Informational",
    "description": "Service software update [R20200330-p1] completed."
  }
}
```

Actualización del software de servicio cancelada

OpenSearch El servicio envía este evento cuando se cancela una actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled as a
                    newer update is available. Please schedule the latest update."
  }
}
```

Actualización programada del software de servicio cancelada

OpenSearch El servicio envía este evento cuando se cancela una actualización del software del servicio que estaba programada previamente para el dominio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Cancelled",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] has been
 cancelled."
  }
}
```

Actualización del software de servicio no ejecutada

OpenSearch El servicio envía este evento cuando no puede iniciar una actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
```

```
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Unexecuted",
    "severity": "Informational",
    "description": "The scheduled service software update [R20200330-p1] cannot be
 started. Reason: [reason]"
  }
}
```

Error al actualizar el software del servicio

OpenSearch El servicio envía este evento cuando se produce un error en la actualización del software del servicio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Failed",
    "severity": "High",
    "description": "Installation of service software update [R20200330-p1] failed.
 [reason].
  }
}
```

Se requiere actualización del software de servicio

OpenSearch El servicio envía este evento cuando se requiere una actualización del software del servicio. Para obtener más información, consulte the section called “Actualizaciones opcionales frente a actualizaciones obligatorias”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Software Update Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2016-11-01T13:12:22Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Service Software Update",
    "status": "Required",
    "severity": "High",
    "description": "Service software update [R20200330-p1] available. Update
                    will be automatically installed after [21st May 2023] if no
                    action is taken. Service Software Deployment Mechanism: Blue/Green.
                    For more information on deployment configuration, please see:
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/managedomains-configuration-changes.html"
  }
}
```

Eventos de ajuste automático

OpenSearch El servicio envía los eventos EventBridge cuando se produce uno de los siguientes eventos de Auto-Tune.

Ajuste automático pendiente

OpenSearch El servicio envía este evento cuando Auto-Tune ha identificado recomendaciones de ajuste para mejorar el rendimiento y la disponibilidad del clúster. Solo verá este evento para dominios con el ajuste automático deshabilitado.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
```

```
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Pending",
    "description": "Auto-Tune recommends the following new settings for your
 domain: { JVM Heap size : 60%}. Enable Auto-Tune to improve cluster stability and
 performance.",
    "scheduleTime": "{iso8601-timestamp}"
  }
}
```

Ajuste automático iniciado

OpenSearch El servicio envía este evento cuando Auto-Tune comienza a aplicar nuevas configuraciones a su dominio.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Started",
    "scheduleTime": "{iso8601-timestamp}",
    "startTime": "{iso8601-timestamp}",
```

```
    "description" : "Auto-Tune is applying the following settings to your domain: { JVM
 Heap size : 60%}."
  }
}
```

El ajuste automático requiere una implementación azul/verde programada

OpenSearch El servicio envía este evento cuando Auto-Tune ha identificado recomendaciones de ajuste que requieren una implementación programada en azul o verde.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Pending",
    "startTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has identified the following settings for your domain
 that require a blue/green deployment: { JVM Heap size : 60%}.
                   You can schedule the deployment for your preferred time."
  }
}
```

Ajuste automático cancelado

OpenSearch El servicio envía este evento cuando se cancela la programación de Auto-Tune porque no hay recomendaciones de ajuste pendientes.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Low",
    "status": "Cancelled",
    "scheduleTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has cancelled the upcoming blue/green deployment."
  }
}
```

Ajuste automático completado

OpenSearch El servicio envía este evento cuando Auto-Tune ha completado la implementación azul/verde y el clúster está operativo con la nueva configuración de la JVM instalada.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "completionTime": "{iso8601-timestamp}",
    "description": "Auto-Tune has completed the blue/green deployment and successfully
 applied the following settings: { JVM Heap size : 60%}."
```

```
  }
}
```

Ajuste automático deshabilitado y cambios revertidos

OpenSearch El servicio envía este evento cuando se ha desactivado el ajuste automático y se han revertido los cambios aplicados.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": [ "arn:aws:es:us-east-1:123456789012:domain/test-domain" ],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. All settings have been reverted. Auto-
Tune will continue to evaluate
                    cluster performance and provide recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Ajuste automático deshabilitado y cambios conservados

OpenSearch El servicio envía este evento cuando se ha desactivado el ajuste automático y se han conservado los cambios aplicados.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
```

```
  "id": "3acb26c8-397c-4c89-a80a-ce672a864c55",
  "detail-type": "Amazon OpenSearch Service Auto-Tune Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2020-10-30T22:06:31Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Auto-Tune Event",
    "severity": "Informational",
    "status": "Completed",
    "description": "Auto-Tune is now disabled. The most-recent settings by Auto-Tune
 have been retained.
                   Auto-Tune will continue to evaluate cluster performance and provide
 recommendations.",
    "completionTime": "{iso8601-timestamp}"
  }
}
```

Eventos del estado del clúster

OpenSearch El servicio envía ciertos eventos EventBridge cuando el estado del clúster se ve comprometido.

Red cluster recovery started (Recuperación de clúster en rojo iniciada)

OpenSearch El servicio envía este evento después de que el estado del clúster haya estado en rojo de forma continua durante más de una hora. Intenta restaurar automáticamente uno o varios índices en rojo a partir de una instantánea para corregir el estado del clúster.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
```

```
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Started",
      "severity":"High",
      "description":"Your cluster status is red. We have started automatic snapshot
 restore for the red indices.
                    No action is needed from your side. Red indices [red-index-0, red-
index-1]"
   }
}
```

Red cluster recovery partially completed (Recuperación de clúster en rojo completada parcialmente)

OpenSearch El servicio envía este evento cuando solo pudo restaurar un subconjunto de índices rojos a partir de una instantánea mientras intentaba corregir el estado de un clúster rojo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Partially Restored",
      "severity":"High",
      "description":"Your cluster status is red. We were able to restore the following
 Red indices from
                   snapshot: [red-index-0]. Indices not restored: [red-index-1].
 Please refer https://docs.aws.amazon.com/opensearch-service/latest/developerguide/
handling-errors.html#handling-errors-red-cluster-status for troubleshooting steps."
```

```
   }
}
```

Red cluster recovery failed (Error de recuperación de clúster en rojo)

OpenSearch El servicio envía este evento cuando no puede restaurar ningún índice mientras intenta corregir el estado de un clúster rojo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Failed",
      "severity":"High",
      "description":"Your cluster status is red. We were unable to restore the Red
 indices automatically.
                   Indices not restored: [red-index-0, red-index-1]. Please refer
 https://docs.aws.amazon.com/opensearch-service/latest/developerguide/handling-
errors.html#handling-errors-red-cluster-status for troubleshooting steps."
   }
}
```

Shards to be deleted (Se deben eliminar particiones)

OpenSearch El servicio envía este evento cuando intenta corregir automáticamente el estado del clúster rojo después de haber estado rojo de forma continua durante 14 días, pero uno o más índices permanecen en rojo. Transcurridos 7 días más (21 días en total si el número está en rojo de forma continua), el OpenSearch Servicio procederá a eliminar los fragmentos no asignados de todos los índices rojos.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:36:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"Medium",
      "description":"Your cluster status is red. Please fix the red indices as soon as
 possible.
                    If not fixed by 2022-04-12 01:51:47+00:00, we will delete all
 unassigned shards,
                    the unit of storage and compute, for these red indices to recover
 your domain and make it green.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.
                    test_data, test_data1",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) to be deleted"
   }
}
```

Shards deleted (Particiones eliminadas)

OpenSearch El servicio envía este evento después de que el estado del clúster haya estado en rojo de forma continua durante 21 días. Procede a eliminar las particiones no asignadas (almacenamiento y computación) de todos los índices en rojo. Para más información, consulte the section called “Corrección automática de clústeres en rojo”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Cluster Status Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2022-04-09T10:54:48Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "severity":"High",
      "description":"We have deleted unassinged shards, the unit of storage and
 compute, in
                    red indices: index-1, index-2 because these indices were red for
 more than
                    21 days and could not be restored with the automated restore
 process.
                    Please refer to https://docs.aws.amazon.com/opensearch-service/
latest/developerguide/handling-errors.html#handling-errors-red-cluster-status for
 troubleshooting steps.",
      "event":"Automatic Snapshot Restore for Red Indices",
      "status":"Shard(s) deleted"
   }
}
```

Advertencia de alto recuento de particiones

OpenSearch El servicio envía este evento cuando el número medio de fragmentos en los nodos de datos activos supera el 90% del límite predeterminado recomendado de 1000. Si bien las versiones posteriores de Elasticsearch OpenSearch admiten un límite máximo configurable de particiones por nodo, le recomendamos que no tenga más de 1000 particiones por nodo. Consulte Elección del número de particiones.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
```

```
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Low",
     "description":"One or more data nodes have close to 1000 shards. To ensure optimum
 performance and stability of your
                   cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

Límite de recuento de particiones superado

OpenSearch El servicio envía este evento cuando el número medio de particiones en los nodos de datos activos supera el límite predeterminado recomendado de 1000. Si bien las versiones posteriores de Elasticsearch OpenSearch admiten un límite máximo configurable de particiones por nodo, le recomendamos que no tenga más de 1000 particiones por nodo. Consulte Elección del número de particiones.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High Shard Count",
     "status":"Warning",
     "severity":"Medium",
```

```
     "description":"One or more data nodes have more than 1000 shards. To ensure
 optimum performance and stability of your
                    cluster, please refer to the best practice guidelines - https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/sizing-domains.html#bp-
sharding."
  }
}
```

Espacio en disco reducido

OpenSearch El servicio envía este evento cuando uno o más nodos del clúster tienen menos del 25% del espacio de almacenamiento disponible o menos de 25 GB.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Space",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more data nodes in your cluster has less than 25% of storage
 space or less than 25GB.
                   Your cluster will be blocked for writes at 20% or 20GB. Please refer
 to the documentation for more information - https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/handling-errors.html#troubleshooting-cluster-block"
  }
}
```

Vulneración del límite de espacio en disco mínimo

OpenSearch El servicio envía este evento cuando todos los nodos del clúster tienen menos del 10% del espacio de almacenamiento disponible o menos de 10 GB. Si todos los nodos superan el límite

de disco bajo, cualquier índice nuevo da como resultado un clúster amarillo, y si todos los nodos se sitúan por debajo del límite de disco alto, aparece un clúster rojo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Low Disk Watermark Breach",
     "status":"Warning",
     "severity":"Medium",
     "description":"Low Disk Watermark threshold is about to be breached. Once the
 threshold is breached, new index creation will be blocked on all
                   nodes to prevent the cluster status from turning red. Please
 increase disk size to suit your storage needs. For more information,
                   see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#troubleshooting-cluster-block".
  }
}
```

Balance de ráfaga de EBS por debajo del 70 %

OpenSearch El servicio envía este evento cuando el saldo de ráfagas de EBS en uno o más nodos de datos cae por debajo del 70%. El agotamiento del balance de ráfaga de EBS puede provocar una falta de disponibilidad generalizada del clúster y una limitación de las solicitudes de E/S, lo que puede provocar altas latencias y tiempos de espera en las solicitudes de indexación y búsqueda. Para conocer los pasos para solucionar este problema, consulte the section called “Bajo balance de ráfaga EBS”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
```

```
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
     "status":"Warning",
     "severity":"Medium",
     "description":"EBS burst balance on one or more data nodes is below 70%.
                    Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                    to fix this issue."
  }
}
```

Balance de ráfaga de EBS por debajo del 20 %

OpenSearch El servicio envía este evento cuando el saldo de ráfagas de EBS en uno o más nodos de datos cae por debajo del 20%. El agotamiento del balance de ráfaga de EBS puede provocar una falta de disponibilidad generalizada del clúster y una limitación de las solicitudes de E/S, lo que puede provocar altas latencias y tiempos de espera en las solicitudes de indexación y búsqueda. Para conocer los pasos para solucionar este problema, consulte the section called “Bajo balance de ráfaga EBS”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"EBS Burst Balance",
```

```
    "status":"Warning",
    "severity":"High",
    "description":"EBS burst balance on one or more data nodes is below 20%.
                   Follow https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/handling-errors.html#handling-errors-low-ebs-burst
                   to fix this issue.
  }
}
```

Limitación de rendimiento de disco

OpenSearch El servicio envía este evento cuando las solicitudes de lectura y escritura en su dominio están siendo limitadas debido a las limitaciones de rendimiento de sus volúmenes de EBS o de su instancia EC2. Si recibe esta notificación, considere la posibilidad de ampliar sus volúmenes o instancias siguiendo las prácticas recomendadas. AWS Si su tipo de volumen es gp2, aumente el tamaño del volumen. Si su tipo de volumen es gp3, aprovisione más rendimiento. También puede comprobar que la base de instancias y el rendimiento máximo de EBS sean superiores o iguales al rendimiento del volumen aprovisionado, y puede escalar verticalmente en consecuencia.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Disk Throughput Throttle",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is experiencing throttling due to instance or volume
 throughput limitations.
                   Please consider scaling your domain to suit your throughput needs.
 In July 2023, we improved
                   the accuracy of throughput throttle calculation by replacing ‘Max
 volume throughput’ with
```

```
                    'Provisioned volume throughput'. Please refer to the documentation
 for more information."
  }
}
```

Tamaño de partición grande

OpenSearch El servicio envía este evento cuando uno o más fragmentos del clúster superan los 50 GiB o los 65 GiB. Para garantizar un rendimiento y una estabilidad óptimos del clúster, reduzca el tamaño de las particiones.

Para obtener más información, consulte las prácticas recomendadas de fragmentación.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Large Shard Size",
     "status":"Warning",
     "severity":"Medium",
     "description":"One or more shards are larger than 65GiB. To ensure optimum cluster
 performance and stability, reduce shard sizes.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-large-shard-
size."
  }
}
```

Alto uso de JVM

OpenSearch El servicio envía este evento cuando la `JVMMemoryPressure` métrica de tu dominio supera el 80%. Si supera el 92 % durante 30 minutos, se bloquearán todas las operaciones de

escritura en el clúster. Para garantizar una estabilidad óptima del clúster, reduzca el tráfico al clúster o escale su dominio para proporcionar memoria suficiente para su carga de trabajo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"High JVM Usage",
     "status":"Warning",
     "severity":"High",
     "description":"JVM memory pressure has exceeded 80%. If it exceeds 92% for 30
 minutes, all write operations to your cluster
                    will be blocked. To ensure optimum cluster stability, reduce
 traffic to the cluster or use larger instance types.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-high-jvm."
  }
}
```

GC insuficiente

OpenSearch El servicio envía este evento cuando la JVM máxima es superior al 70% y la diferencia entre el máximo y el mínimo es inferior al 30%. Esto puede indicar que la JVM no puede recuperar suficiente memoria para la carga de trabajo durante los ciclos de recopilación de elementos no utilizados. Esto puede provocar respuestas cada vez más lentas y latencias más altas y, en algunos casos, incluso la caída de nodos debido a que se ha agotado el tiempo de espera de las comprobaciones de estado. Para garantizar una estabilidad óptima del clúster, reduzca el tráfico al clúster o escale su dominio para proporcionar memoria suficiente para su carga de trabajo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Insufficient GC",
     "status":"Warning",
     "severity":"Medium",
     "description":"Maximum JVM is above 70% and JVM range is less than 30%. This may
 indicate insufficient garbage collection for your workload.
                   For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-insufficient-
gc."
  }
}
```

Advertencia de enrutamiento indexado personalizada

OpenSearch El servicio envía este evento cuando el dominio está en proceso y contiene índices con una configuración personalizada de index.routing.location, lo que puede provocar que las implementaciones de color azul-verde se bloqueen. Compruebe que la configuración se aplique correctamente.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
```

```
     "event":"Custom Index Routing Warning",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is in processing state and contains indice(s) with
 custom index.routing.allocation
                    settings which can cause blue-green deployments to get stuck.
 Verify settings are applied properly.
                    For more information, see https://docs.aws.amazon.com/opensearch-
service/latest/developerguide/monitoring-events.html#monitoring-events-index-routing."
   }
}
```

Fallo en el bloqueo de partición

OpenSearch El servicio envía este evento cuando tu dominio está en mal estado debido a fragmentos no asignados. `[ShardLockObtainFailedException]` Para obtener más información, consulta ¿Cómo resuelvo la excepción de bloqueo de fragmentos en memoria en Amazon OpenSearch Service?

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2017-12-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Failed Shard Lock",
     "status":"Warning",
     "severity":"Medium",
     "description":"Your domain is unhealthy due to unassigned shards with
 [ShardLockObtainFailedException]. For more information,
                    see https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html#monitoring-events-failed-shard-lock."
}
```

Eventos del punto de conexión de VPC

OpenSearch El servicio envía ciertos eventos EventBridge relacionados con los puntos finales de la AWS PrivateLink interfaz.

Error al crear el punto de conexión de VPC

OpenSearch El servicio envía este evento cuando no puede crear un punto final de VPC solicitado. Este error puede ocurrir porque alcanzó el límite de la cantidad de puntos de conexión de VPC permitidos dentro de una región. También verá este error si no existe una subred ni un grupo de seguridad especificados.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Create Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to create VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: You've reached the limit on the
                     number of VPC endpoints that you can create in the AWS Region."
   }
}
```

Error al actualizar el punto de conexión de VPC

OpenSearch El servicio envía este evento cuando no puede eliminar un punto final de VPC solicitado.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Update Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to update VPC endpoint aos-0d4c74c0342343 for domain
                     arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: <failure message>."
    }
}
```

Error al eliminar el punto de conexión de VPC

OpenSearch El servicio envía este evento cuando no puede eliminar un punto final de VPC solicitado.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service VPC Endpoint Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
```

```
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"VPC Endpoint Delete Validation",
      "status":"Failed",
      "severity":"High",
      "description":"Unable to delete VPC endpoint aos-0d4c74c0342343 for domain
                  arn:aws:es:eu-south-1:123456789012:domain/my-domain due to the
 following validation failures: Specified subnet doesn't exist."
   }
}
```

Eventos de retirada de nodos

OpenSearch El servicio envía los eventos EventBridge cuando se produce uno de los siguientes eventos de retirada de nodos.

Retirada de nodos programada

OpenSearch El servicio envía este evento cuando se ha programado la retirada de un nodo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Scheduled",
    "severity": "Medium",
    "description": "An automated action to retire and replace a node has been scheduled
 on your domain.
                    The node will be replaced in the next off-peak window. For more
 information, see
```

```
                    https://docs.aws.amazon.com/opensearch-service/latest/
developerguide/monitoring-events.html."
  }
}
```

Se completó la retirada del nodo

OpenSearch El servicio envía este evento cuando se ha completado la retirada de un nodo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Completed",
    "severity": "Medium",
    "description": "The node has been retired and replaced with a new node."
  }
}
```

Error al retirar el nodo

OpenSearch El servicio envía este evento cuando se produce un error al retirar un nodo.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version": "0",
  "id": "01234567-0123-0123-0123-012345678901",
  "detail-type": "Amazon OpenSearch Service Notification",
  "source": "aws.es",
```

```
  "account": "123456789012",
  "time": "2023-04-07T10:07:33Z",
  "region": "us-east-1",
  "resources": ["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail": {
    "event": "Node Retirement Notification",
    "status": "Failed",
    "severity": "Medium",
    "description": "Node retirement failed. No actions are required from your end. We
 will automatically
                    retry replacing the node."
  }
}
```

Eventos de error de dominio

OpenSearch El servicio envía los eventos EventBridge cuando se produce uno de los siguientes errores de dominio.

Error en la validación de la actualización del dominio

OpenSearch El servicio envía este evento si detecta uno o más errores de validación al intentar actualizar o realizar un cambio de configuración en un dominio. Para conocer los pasos para solucionar estos errores, consulte the section called “Solución de errores de validación”.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
   "version":"0",
   "id":"01234567-0123-0123-0123-012345678901",
   "detail-type":"Amazon OpenSearch Service Domain Update Notification",
   "source":"aws.es",
   "account":"123456789012",
   "time":"2016-11-01T13:12:22Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:es:us-east-1:123456789012:domain/test-domain"
   ],
   "detail":{
      "event":"Domain Update Validation",
```

```
      "status":"Failed",
      "severity":"High",
      "description":"Unable to perform updates to your domain due to the following
 validation failures: <failures>
                    Please see the documentation for more information https://
docs.aws.amazon.com/opensearch-service/latest/developerguide/managedomains-
configuration-changes.html#validation"
   }
}
```

Clave KMS inaccesible

OpenSearch El servicio envía este evento cuando no puede acceder a tu AWS KMS clave.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Domain Error Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2016-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"KMS Key Inaccessible",
     "status":"Error",
     "severity":"High",
     "description":"The KMS key associated with this domain is inaccessible. You are at
 risk of losing access to your domain.
                    For more information, please refer to https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

Aislamiento de dominios

OpenSearch El servicio envía este evento cuando tu dominio queda aislado y no puede recibir, leer ni escribir solicitudes porque la red no puede acceder a él.

Ejemplo

A continuación se muestra un ejemplo de este evento:

```
{
  "version":"0",
  "id":"01234567-0123-0123-0123-012345678901",
  "detail-type":"Amazon OpenSearch Service Notification",
  "source":"aws.es",
  "account":"123456789012",
  "time":"2023-11-01T13:12:22Z",
  "region":"us-east-1",
  "resources":["arn:aws:es:us-east-1:123456789012:domain/test-domain"],
  "detail":{
     "event":"Domain Isolation Notification",
     "status":"Error",
     "severity":"High",
     "description":"Your OpenSearch Service domain has been isolated. An isolated
 domain is unreachable by network and cannot receive, read, or write requests. For more
 information and assistance, please contact AWS Support at https://docs.aws.amazon.com/
opensearch-service/latest/developerguide/encryption-at-rest.html#disabled-key."
  }
}
```

Tutorial: Cómo escuchar los EventBridge eventos OpenSearch de Amazon Service

En este tutorial, configuras una AWS Lambda función sencilla que escucha los eventos de Amazon OpenSearch Service y los escribe en un flujo de registro de CloudWatch Logs.

Requisitos previos

En este tutorial se presupone que ya tienes un dominio OpenSearch de servicio. Si no creó un dominio, siga los pasos de Creación y administración de dominios para crear uno.

Paso 1: crear la función Lambda

En este procedimiento, se crea una función Lambda sencilla que sirva de destino para los mensajes de eventos de OpenSearch servicio.

Para crear una función de Lambda de destino

1. Abra la AWS Lambda consola en https://console.aws.amazon.com/lambda/.
2. Seleccione Crear función y Crear desde cero.
3. En Nombre de la función, ingrese event-handler.
4. En Tiempo de ejecución, seleccione Python 3.8.
5. Seleccione Crear función.
6. En la sección Código de función, edite el código de muestra de tal modo que coincida con el siguiente ejemplo:

```
import json

def lambda_handler(event, context):
    if event["source"] != "aws.es":
        raise ValueError("Function only supports input from events with a source
 type of: aws.es")

    print(json.dumps(event))
```

   Esta es una función simple de Python 3.8 que imprime los eventos enviados por OpenSearch Service. Si todo está configurado correctamente, al final de este tutorial, los detalles del evento aparecen en el flujo de registro de CloudWatch Logs asociado a esta función de Lambda.
7. Seleccione Implementar.

Paso 2: registrar una regla de eventos

En este paso, creará una EventBridge regla que capture los eventos de sus dominios de OpenSearch servicio. Esta regla captura todos los eventos dentro de la cuenta, en la cual se define. Los propios mensajes de eventos contienen información acerca de la fuente del evento, incluido el dominio desde el que se originó. Puede utilizar esta información para filtrar y ordenar eventos de manera programática.

Para crear una EventBridge regla

1. Abra la EventBridge consola en https://console.aws.amazon.com/events/.
2. Seleccione Crear regla.
3. Nombre la regla event-rule.
4. Seleccione Siguiente.

5. Para el patrón de eventos, selecciona AWS services, Amazon OpenSearch Service y All Events. Este patrón se aplica a todos los dominios de tu OpenSearch Servicio y a todos los eventos del OpenSearch Servicio. También puede crear un patrón más específico para filtrar algunos resultados.
6. Pulse Siguiente.
7. Para el destino, seleccione Función de Lambda. En el menú desplegable de funciones, elija event-handler.
8. Pulse Siguiente.
9. Omita las etiquetas y vuelva a pulsar Siguiente.
10. Revise la configuración y elija Crear regla.

Paso 3: probar la configuración

La próxima vez que reciba una notificación en la sección Notificaciones de la consola de OpenSearch servicio, si todo está configurado correctamente, se activará la función Lambda y escribirá los datos del evento en un flujo de registro de CloudWatch Logs para la función.

Para probar la configuración

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Registros y, a continuación, seleccione el grupo de registro de la función de Lambda (por ejemplo, /aws/lambda/event-handler).
3. Seleccione una secuencia de registro para ver los datos de los eventos.

Tutorial: Sending Amazon SNS alerts for available software updates

En este tutorial, configuras una regla de EventBridge eventos de Amazon que captura las notificaciones de las actualizaciones de software de servicio disponibles en Amazon OpenSearch Service y te envía una notificación por correo electrónico a través de Amazon Simple Notification Service (Amazon SNS).

Requisitos previos

En este tutorial se presupone que ya tiene un dominio OpenSearch de servicio. Si no creó un dominio, siga los pasos de Creación y administración de dominios para crear uno.

Paso 1: crear y suscribirse a un tema de Amazon SNS

Configure un tema de Amazon SNS para servir como destino de eventos para la nueva regla de eventos.

Para crear un destino de Amazon SNS

1. Abra la consola de Amazon SNS en https://console.aws.amazon.com/sns/v3/home.
2. Seleccione Temas y Crear tema.
3. Para el tipo de tarea, seleccione Estándar y nombre el trabajo software-update.
4. Seleccione Crear nuevo tema.
5. Una vez creado el tema, seleccione Crear suscripción.
6. En Protocolo, seleccione Correo electrónico. En Punto de conexión, ingrese una dirección de email a la que actualmente tenga acceso y elija Crear suscripción.
7. Consulte su cuenta de email y espere para recibir un mensaje de correo electrónico de confirmación de la suscripción. Cuando lo reciba, seleccione Confirmar suscripción.

Paso 2: registrar una regla de eventos

A continuación, registre una regla de eventos que solo capture los eventos de actualización del software de servicio.

Para crear una regla de eventos

1. Abra la EventBridge consola en https://console.aws.amazon.com/events/.
2. Seleccione Crear regla.
3. Nombre la regla softwareupdate-rule.
4. Seleccione Siguiente.
5. Para el patrón de eventos, selecciona AWS servicios, Amazon OpenSearch Service y Amazon OpenSearch Service Software Update Notification. Este patrón coincide con cualquier evento de actualización del software del OpenSearch servicio realizado por Service. Para obtener más información sobre los patrones de eventos, consulta los patrones de EventBridge eventos de Amazon en la Guía del EventBridge usuario de Amazon.
6. Si lo desea, puede filtrar solo por gravedades específicas. Para conocer las gravedades de cada evento, consulte the section called “Eventos de actualización del software de servicio”.

7. Seleccione Siguiente.
8. Para el destino, seleccione Tema de SNS y seleccione software-update.
9. Seleccione Siguiente.
10. Omita las etiquetas y elija Siguiente.
11. Revise la configuración de la regla y elija Crear regla.

La próxima vez que reciba una notificación del OpenSearch Servicio sobre una actualización de software de servicio disponible, si todo está configurado correctamente, Amazon SNS debería enviarle una alerta por correo electrónico sobre la actualización.

Monitoreo de las llamadas a la API de Amazon OpenSearch Service con AWS CloudTrail

Amazon OpenSearch Service se integra con AWS CloudTrail, un servicio que proporciona un registro de las medidas adoptadas por un usuario, un rol o un servicio AWS en OpenSearch Service. CloudTrail captura todas las llamadas de la API de configuración para OpenSearch Service como eventos.

> **Note**
>
> CloudTrail solo captura las llamadas a la API de configuración, como `CreateDomain` y `GetUpgradeStatus`. CloudTrail no captura llamadas a la API de OpenSearch, como `_search` y `_bulk`. Para estas llamadas, consulte the section called “Monitoreo de registros de auditoría”.

Entre las llamadas capturadas se incluyen las que se realizan desde la consola de OpenSearch Service, la AWS CLI o un SDK de AWS. Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos para OpenSearch Service. Si no configura un registro de seguimiento, puede ver los eventos más recientes en la consola de CloudTrail en el Historial de eventos. Mediante la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a OpenSearch Service, la dirección IP desde la cual se realizó, quién la realizó y cuándo, etc.

Para obtener más información acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

Información de Amazon OpenSearch Service en CloudTrail

CloudTrail se habilita en Cuenta de AWS cuando crea la cuenta. Cuando se produce una actividad en OpenSearch Service, esa actividad se registra en un evento de CloudTrail junto con otros eventos de servicio de AWS en el Event history (Historial de eventos). Puede ver, buscar y descargar los últimos eventos de la cuenta de Cuenta de AWS. Para obtener más información, consulte Visualización de eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de los eventos de la cuenta de Cuenta de AWS, incluidos los eventos de OpenSearch Service, cree un registro de seguimiento. Un registro de seguimiento habilita a CloudTrail para 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 registra 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:

- Creación de una traza para su Cuenta de AWS
- Integraciones de servicios de AWS con registros de CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las acciones de la API de configuración de OpenSearch Service que se documentan en la referencia de API de Amazon OpenSearch Service.

Cada entrada de registro o evento contiene información sobre 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 AWS Identity and Access Management (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 el Elemento userIdentity de CloudTrail.

Descripción de las entradas del archivo de registro de Amazon OpenSearch Service

Un registro de seguimiento es una configuración que habilita 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 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 que sigue se muestra una entrada de registro de CloudTrail que ilustra la operación `CreateDomain`:


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDACKCEVSQ6C2EXAMPLE",
    "arn": "arn:aws:iam::123456789012:user/test-user",
    "accountId": "123456789012",
    "accessKeyId": "access-key",
    "userName": "test-user",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-08-21T21:59:11Z"
      }
    },
    "invokedBy": "signin.amazonaws.com"
  },
  "eventTime": "2018-08-21T22:00:05Z",
  "eventSource": "es.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-1",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "signin.amazonaws.com",
  "requestParameters": {
    "engineVersion": "OpenSearch_1.0",
    "clusterConfig": {
      "instanceType": "m4.large.search",
      "instanceCount": 1
    },
```

```
    "snapshotOptions": {
      "automatedSnapshotStartHour": 0
    },
    "domainName": "test-domain",
    "encryptionAtRestOptions": {},
    "eBSOptions": {
      "eBSEnabled": true,
      "volumeSize": 10,
      "volumeType": "gp2"
    },
    "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}",
    "advancedOptions": {
      "rest.action.multi.allow_explicit_index": "true"
    }
  },
  "responseElements": {
    "domainStatus": {
      "created": true,
      "clusterConfig": {
        "zoneAwarenessEnabled": false,
        "instanceType": "m4.large.search",
        "dedicatedMasterEnabled": false,
        "instanceCount": 1
      },
      "cognitoOptions": {
        "enabled": false
      },
      "encryptionAtRestOptions": {
        "enabled": false
      },
      "advancedOptions": {
        "rest.action.multi.allow_explicit_index": "true"
      },
      "upgradeProcessing": false,
      "snapshotOptions": {
        "automatedSnapshotStartHour": 0
      },
      "eBSOptions": {
        "eBSEnabled": true,
        "volumeSize": 10,
        "volumeType": "gp2"
      },
```

```
      "engineVersion": "OpenSearch_1.0",
      "processing": true,
      "aRN": "arn:aws:es:us-west-1:123456789012:domain/test-domain",
      "domainId": "123456789012/test-domain",
      "deleted": false,
      "domainName": "test-domain",
      "accessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::123456789012:root\"},\"Action\":\"es:*\",
\"Resource\":\"arn:aws:es:us-west-1:123456789012:domain/test-domain/*\"}]}"
    }
  },
  "requestID": "12345678-1234-1234-1234-987654321098",
  "eventID": "87654321-4321-4321-4321-987654321098",
  "eventType": "AwsApiCall",
  "recipientAccountId": "123456789012"
}
```

Seguridad en Amazon OpenSearch Service

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS. Para obtener más información sobre los programas de conformidad que se aplican a Amazon OpenSearch Service, consulta AWS Servicios incluidos en el ámbito de aplicación por programa de conformidad.
- Seguridad en la nube: tu responsabilidad viene determinada por el AWS servicio que utilices. 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.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida al utilizar el OpenSearch Servicio. Los siguientes temas muestran cómo configurar el OpenSearch Servicio para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos OpenSearch del Servicio.

Temas

- Uso de roles vinculados a servicios para Amazon OpenSearch Service.

Protección de datos en Amazon OpenSearch Service

El AWS modelo de se aplica a protección de datos en Amazon OpenSearch Service. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure los usuarios individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos. AWS Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con. AWS CloudTrail
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-2 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con un OpenSearch servicio u otro tipo de servicio Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que

ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Cifrado de datos en reposo para Amazon OpenSearch Service

OpenSearch Los dominios de servicio ofrecen el cifrado de los datos en reposo, una función de seguridad que ayuda a evitar el acceso no autorizado a los datos. La función utiliza AWS Key Management Service (AWS KMS) para almacenar y gestionar las claves de cifrado y el algoritmo del estándar de cifrado avanzado con claves de 256 bits (AES-256) para realizar el cifrado. Si está habilitada, la característica cifra los siguientes aspectos de un dominio:

- Todos los índices (incluidos los que están almacenados) UltraWarm
- OpenSearch registros
- Archivos de intercambio
- Todos los demás datos del directorio de la aplicación
- Instantáneas automatizadas

Los siguientes elementos no se cifran cuando habilita el cifrado de datos en reposo, pero puede realizar pasos adicionales para protegerlos:

- Instantáneas manuales: actualmente no puede utilizar AWS KMS claves para cifrar instantáneas manuales. No obstante, puede utilizar el cifrado del lado del servidor con claves administradas por S3 o claves de KMS para cifrar el bucket que utiliza como repositorio de instantáneas. Para obtener instrucciones, consulte the section called “Registrar un repositorio de instantáneas manuales”.
- Registros lentos y registros de errores: si publica registros y desea cifrarlos, puede cifrar su grupo de CloudWatch registros con la misma AWS KMS clave que el dominio del servicio. OpenSearch Para obtener más información, consulte Cifrar datos de registro en CloudWatch Logs utilizando AWS KMS la Guía del usuario de Amazon CloudWatch Logs.

> **Note**
>
> No puedes habilitar el cifrado en reposo en un dominio existente si UltraWarm el almacenamiento en frío está activado en el dominio. Primero debes deshabilitar UltraWarm

> o almacenar en frío, habilitar el cifrado en reposo y, a continuación, volver a habilitar UltraWarm o almacenar en frío. Si desea conservar los índices UltraWarm o almacenarlos en frío, debe moverlos a un almacenamiento en caliente antes de inhabilitarlos UltraWarm o almacenarlos en frío.

OpenSearch El servicio solo admite claves KMS de cifrado simétrico, no asimétricas. Para conocer cómo crear claves simétricas, consulte Creación de claves en la Guía para desarrolladores de AWS Key Management Service .

Independientemente de si el cifrado en reposo está habilitado, todos los dominios cifran automáticamente los paquetes personalizados mediante AES-256 y claves administradas por el servicio. OpenSearch

Permisos

Para usar la consola de OpenSearch servicio para configurar el cifrado de los datos en reposo, debe tener permisos de lectura AWS KMS, como la siguiente política basada en la identidad:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:List*",
        "kms:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

Si desea utilizar una clave distinta de la AWS clave propia, también debe tener permisos para crear concesiones para la clave. Estos permisos normalmente suelen adoptar la forma de una política con base en recursos que especifica al crear la clave.

Si quieres que tu clave sea exclusiva de OpenSearch Service, puedes añadir la ViaService condición kms: a esa política clave:

```
"Condition": {
```

```
  "StringEquals": {
    "kms:ViaService": "es.us-west-1.amazonaws.com"
  },
  "Bool": {
    "kms:GrantIsForAWSResource": "true"
  }
}
```

Para obtener más información, consulte Uso de políticas clave en AWS KMS en la Guía para AWS Key Management Service desarrolladores.

Habilitar el cifrado de datos en reposo

El cifrado de los datos inactivos en dominios nuevos requiere Elasticsearch 5.1 OpenSearch o una versión posterior. Para habilitarlo en los dominios existentes, se requiere Elasticsearch OpenSearch 6.7 o una versión posterior.

Para habilitar el cifrado de los datos en reposo (consola)

1. Abre el dominio en la AWS consola y, a continuación, selecciona Acciones y Editar la configuración de seguridad.
2. En Cifrado, seleccione Habilitar el cifrado de datos en reposo.
3. Elige la AWS KMS clave que quieras usar y, a continuación, selecciona Guardar cambios.

También puede habilitar el cifrado a través de la API de configuración. La siguiente solicitud permite el cifrado de datos en reposo en un dominio existente:

```
{
   "ClusterConfig":{
      "EncryptionAtRestOptions":{
         "Enabled": true,
         "KmsKeyId":"arn:aws:kms:us-east-1:123456789012:alias/my-key"
      }
   }
}
```

Clave KMS desactivada o eliminada

Si deshabilitas o eliminas la clave que usaste para cifrar un dominio, el dominio deja de estar accesible. OpenSearch El servicio te envía una notificación informándote de que no puede acceder a la clave KMS. Vuelva a habilitar la clave inmediatamente para acceder a su dominio.

El equipo del OpenSearch Servicio no puede ayudarte a recuperar tus datos si se elimina la clave. AWS KMS elimina las claves solo después de un período de espera de al menos siete días. Si su clave está pendiente de eliminación, cancele la eliminación o tome una instantánea manual del dominio para evitar la pérdida de datos.

Deshabilitar el cifrado de datos en reposo

Después de configurar un dominio para cifrar los datos en reposo, no puede desactivar la configuración. En su lugar, puede realizar una instantánea manual del dominio existente, crear otro dominio, migrar los datos y eliminar el dominio antiguo.

Monitorear dominios que cifran los datos en reposo

Los dominios que cifran los datos en reposo tienen dos métricas adicionales: `KMSKeyError` y `KMSKeyInaccessible`. Estas métricas solo aparecen si el dominio se encuentra con un problema con la clave de cifrado. Para obtener una descripción completa de estas métricas, consulte the section called “Métricas de clúster”. Puede verlos mediante la consola de OpenSearch servicio o la consola de Amazon CloudWatch .

> **Tip**
>
> Cada métrica representa un problema importante para un dominio, por lo que te recomendamos que crees CloudWatch alarmas para ambos. Para obtener más información, consulte the section called “ CloudWatch Alarmas recomendadas”.

Otras consideraciones

- La rotación automática de claves preserva las propiedades de AWS KMS las claves, por lo que la rotación no afecta a la capacidad de acceder a OpenSearch los datos. Los dominios del OpenSearch Servicio de Cifrado no admiten la rotación manual de claves, lo que implica crear una clave nueva y actualizar cualquier referencia a la clave anterior. Para obtener más información, consulte Rotación de claves en la Guía para desarrolladores de AWS Key Management Service .

- Algunos tipos de instancias no admiten el cifrado de datos en reposo. Para obtener más información, consulte the section called “Tipos de instancias admitidas”.
- Los dominios que cifran los datos en reposo utilizan otro nombre de repositorio para sus instantáneas automatizadas. Para obtener más información, consulte the section called “Restaurar instantáneas”.
- Si bien recomendamos encarecidamente habilitar el cifrado en reposo, puede agregar sobrecarga de CPU adicional y unos pocos milisegundos de latencia. Sin embargo, la mayoría de los casos de uso no son sensibles a estas diferencias y la magnitud del impacto depende de la configuración del clúster, los clientes y el perfil de uso.

Sin ode-to-node cifrado para Amazon OpenSearch Service

El ode-to-node cifrado N proporciona una capa de seguridad adicional además de las funciones predeterminadas de Amazon OpenSearch Service.

Cada dominio OpenSearch de servicio, independientemente de si el dominio utiliza el acceso a la VPC, reside en su propia VPC dedicada. Esta arquitectura evita que los posibles atacantes intercepten el tráfico entre OpenSearch los nodos y mantiene el clúster seguro. Sin embargo, de forma predeterminada, el tráfico de la VPC está sin cifrar. ode-to-node El cifrado N permite el cifrado TLS 1.2 para todas las comunicaciones dentro de la VPC.

Si envía datos al OpenSearch Servicio a través de HTTPS, el node-to-node cifrado ayuda a garantizar que sus datos permanezcan cifrados a medida que OpenSearch los distribuye (y redistribuye) por todo el clúster. Si los datos llegan sin cifrar a través de HTTP, OpenSearch Service los cifra cuando llegan al clúster. Puedes exigir que todo el tráfico al dominio llegue a través de HTTPS mediante la consola o la API AWS CLI de configuración.

No se requiere ningún ode-to-node cifrado si habilitas un control de acceso detallado.

Habilitar el node-to-node cifrado

ode-to-node El cifrado de los dominios nuevos requiere cualquier versión de OpenSearch Elasticsearch 6.0 o posterior. Para habilitar el node-to-node cifrado en los dominios existentes se requiere cualquier versión de OpenSearch Elasticsearch 6.7 o posterior. Seleccione el dominio existente en la consola de AWS , Acciones y Editar la configuración de seguridad.

Como alternativa, puede usar la API de configuración AWS CLI or. Para obtener más información, consulta la referencia de AWS CLI comandos y la referencia de la API de OpenSearch servicio.

Deshabilitar el cifrado node-to-node

Después de configurar un dominio para que utilice el node-to-node cifrado, no podrá deshabilitar la configuración. En su lugar, puede realizar una instantánea manual del dominio cifrado, crear otro dominio, migrar los datos y eliminar el dominio antiguo.

Identity and Access Management en Amazon OpenSearch Service

Amazon OpenSearch Service ofrece varias formas de controlar el acceso a tus dominios. En este tema, se tratan los diversos tipos de política, la forma en que interactúan entre sí y cómo crear sus propias políticas personalizadas.

> **Important**
>
> La compatibilidad con VPC introduce algunas consideraciones adicionales en el control de acceso al OpenSearch servicio. Para obtener más información, consulte the section called "Acerca de las políticas de acceso en los dominios de VPC".

Tipos de políticas

OpenSearch El servicio admite tres tipos de políticas de acceso:

- the section called "Políticas basadas en recursos"
- the section called "Políticas basadas en identidades"
- the section called "Políticas basadas en IP"

Políticas basadas en recursos

Al crear un dominio, agrega una política basada en recursos, a veces denominada política de acceso al dominio. Estas políticas especifican qué acciones puede realizar una entidad principal en los subrecursos del dominio (con la excepción de la búsqueda entre clústeres). Los subrecursos incluyen OpenSearch índices y API. El elemento Entidad principal especifica las cuentas, los usuarios o los roles que tienen permitido el acceso. El elemento Recurso especifica los subrecursos a los que pueden obtener acceso estos elementos principales.

Por ejemplo, la siguiente política basada en recursos concede a `test-user` acceso completo (`es:*`) a los subrecursos en `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:*"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Dos consideraciones importantes se aplican a esta política:

- Estos privilegios se aplican únicamente a este dominio. A menos que cree políticas similares en otros dominios, `test-user` solo puede acceder a `test-domain`.
- El `/*` final en el elemento `Resource` es significativo e indica que las políticas basadas en recursos solo se aplican a los subrecursos del dominio, no al propio dominio. En las políticas basadas en recursos, la acción `es:*` es equivalente a `es:ESHttp*`.

  Por ejemplo, `test-user` puede realizar solicitudes frente a un índice (`GET https://search-test-domain.us-west-1.es.amazonaws.com/test-index`), pero no puede actualizar la configuración del dominio (`POST https://es.us-west-1.amazonaws.com/2021-01-01/opensearch/domain/test-domain/config`). Observe la diferencia entre los dos puntos de conexión. El acceso a la API de configuración requiere una política basada en identidad.

Puede especificar un nombre de índice parcial agregando un comodín. Este ejemplo identifica cualquier índice que empiecen con `commerce`:

```
arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce*
```

En este caso, el comodín significa que `test-user` puede realizar solicitudes a índices dentro de `test-domain` que tengan nombres que comiencen con `commerce`.

Para restringir aún más `test-user`, puede aplicar la siguiente política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
_search"
    }
  ]
}
```

Ahora `test-user` puede realizar solo una operación: búsquedas del índice `commerce-data`. Todos los demás índices del dominio son inaccesibles y, sin permisos para utilizar las acciones `es:ESHttpPut` o `es:ESHttpPost`, `test-user` no puede agregar ni modificar documentos.

A continuación, podría decidir configurar un rol para usuarios avanzados. Esta política concede a `power-user-role` acceso a los métodos HTTP GET y PUT para todos los URI del índice:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:role/power-user-role"
        ]
      },
      "Action": [
        "es:ESHttpGet",
        "es:ESHttpPut"
      ],
```

```
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/commerce-data/
*"
    }
  ]
}
```

Si el dominio se encuentra en una VPC o utiliza un control de acceso detallado, puede utilizar una política de acceso al dominio abierto. De lo contrario, la política de acceso al dominio debe contener alguna restricción, ya sea por entidad principal o dirección IP.

Para obtener información sobre todas las acciones disponibles, consulte the section called "Referencia de los elementos de las políticas". Para obtener un control mucho más pormenorizado sobre sus datos, utilice una política de acceso al dominio abierto con control de acceso detallado.

Políticas basadas en identidades

A diferencia de las políticas basadas en recursos, que forman parte de cada dominio de OpenSearch servicio, las políticas basadas en la identidad se asocian a los usuarios o roles que utilizan el servicio (IAM). AWS Identity and Access Management Al igual que las políticas basadas en recursos, las políticas basadas en identidad especifican quién puede obtener acceso a un servicio, las acciones que puede realizar y, si corresponde, los recursos en los que se pueden realizar dichas acciones.

Aunque en realidad no tienen por qué serlo, las políticas basadas en identidad suelen ser más genéricas. Normalmente, solo determinan las acciones de la API de configuración que un usuario puede realizar. Una vez implementadas estas políticas, puede usar políticas basadas en recursos (o un control de acceso detallado) en Service para ofrecer a los usuarios acceso a los índices y las OpenSearch API. OpenSearch

> **Note**
>
> Los usuarios con la `AmazonOpenSearchServiceReadOnlyAccess` política AWS gestionada no pueden ver el estado del clúster en la consola. Para que puedan ver el estado del clúster (y otros OpenSearch datos), añada la `es:ESHttpGet` acción a una política de acceso y adjúntela a sus cuentas o funciones.

Dado que las políticas basadas en identidad se adjuntan a usuarios o roles (entidades principales), el JSON no especifica una entidad principal. La siguiente política concede acceso a las acciones que comienzan por `Describe` y `List`. Esta combinación de acciones proporciona acceso de solo lectura a las configuraciones de dominio, pero no a los datos almacenados en el dominio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:Describe*",
        "es:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Un administrador puede tener acceso total al OpenSearch Servicio y a todos los datos almacenados en todos los dominios:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "es:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Las políticas basadas en identidad permiten utilizar etiquetas para controlar el acceso a la API de configuración. La siguiente política, por ejemplo, permite a las entidades principales adjuntas ver y actualizar la configuración de un dominio si el dominio tiene la etiqueta `team:devops`:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:UpdateDomainConfig",
      "es:DescribeDomain",
      "es:DescribeDomainConfig"
    ],
```

```
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/team": [
          "devops"
        ]
      }
    }
  }]
}
```

También puedes usar etiquetas para controlar el acceso a la OpenSearch API. Las políticas basadas en etiquetas para la OpenSearch API solo se aplican a los métodos HTTP. Por ejemplo, la siguiente política permite a los directores adjuntos enviar solicitudes GET y PUT a la OpenSearch API si el dominio tiene la `environment:production` etiqueta:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:ESHttpGet",
      "es:ESHttpPut"
    ],
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
      }
    }
  }]
}
```

Para un control más detallado de la OpenSearch API, considera la posibilidad de utilizar un control de acceso más detallado.

> **Note**
>
> Tras añadir una o más OpenSearch API a cualquier política basada en etiquetas, debe realizar una sola operación de etiquetado (como añadir, eliminar o modificar una etiqueta) para que los cambios surtan efecto en un dominio. Debe utilizar el software de servicio R20211203 o posterior para incluir las operaciones de la OpenSearch API en las políticas basadas en etiquetas.

OpenSearch El servicio admite las claves de condición `TagKeys` globales `RequestTag` y las claves de condición de la API de configuración, no de la API. OpenSearch Estas condiciones solo se aplican a las llamadas a la API que incluyen etiquetas dentro de la solicitud, como `CreateDomain`, `AddTags` y `RemoveTags`. La siguiente política permite a las entidades principales adjuntas crear dominios, pero solo si incluyen la etiqueta `team:it` en la solicitud:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "es:CreateDomain",
      "es:AddTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/team": [
          "it"
        ]
      }
    }
  }
}
```

Para conocer más detalles sobre la utilización de etiquetas para el control de acceso y las diferencias entre las políticas basadas en recursos y las políticas basadas en identidad, consulte la Guía del usuario de IAM.

Políticas basadas en IP

Las políticas basadas en IP restringen el acceso a un dominio a una o más direcciones IP o bloques de CIDR. Técnicamente, las políticas basadas en IP no son un tipo de política distinto. En lugar de ello, son solo políticas basadas en recursos que especifican una entidad principal anónima e incluyen un elemento de Condición especial.

El principal atractivo de las políticas basadas en IP es que permiten realizar solicitudes sin firmar a un dominio de OpenSearch servicio, lo que permite utilizar clientes como curl y OpenSearch Dashboards o acceder al dominio a través de un servidor proxy. Para más información, consulte the section called “Uso de un proxy para acceder al servicio desde los paneles OpenSearch OpenSearch ”.

> **Note**
>
> Si ha habilitado acceso VPC para su dominio, no puede configurar una política basada en IP. En su lugar, puede utilizar grupos de seguridad para controlar qué direcciones IP pueden tener acceso al dominio. Para más información, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”.

La siguiente política concede a todas las solicitudes HTTP que se originan en el intervalo de IP especificado acceso a `test-domain`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
```

```
      },
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    }
  ]
}
```

Si su dominio tiene un punto de conexión público y no utiliza un control de acceso detallado, recomendamos combinar direcciones IP y entidades principales de IAM. Esta política concede acceso HTTP `test-user` únicamente si la solicitud se origina en el intervalo IP especificado:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::987654321098:user/test-user"
      ]
    },
    "Action": [
      "es:ESHttp*"
    ],
    "Condition": {
      "IpAddress": {
        "aws:SourceIp": [
          "192.0.2.0/24"
        ]
      }
    },
    "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
  }]
}
```

Realizar y firmar solicitudes de servicio OpenSearch

Incluso si configura una política de acceso completamente abierta y basada en recursos, todas las solicitudes a la API de configuración del OpenSearch servicio deben estar firmadas. Si sus políticas especifican funciones o usuarios de IAM, las solicitudes a las OpenSearch API también deben firmarse con la versión 4 de AWS Signature. El método de firma difiere en función de la API:

- Para realizar llamadas a la API OpenSearch de configuración del servicio, le recomendamos que utilice uno de los AWS SDK. Los SDK simplifican en gran medida el proceso y pueden ahorrar

mucho tiempo en comparación con la creación y firma de sus propias solicitudes. Los puntos de enlace de la API de configuración utilizan el siguiente formato:

```
es.region.amazonaws.com/2021-01-01/
```

Por ejemplo, la siguiente solicitud introduce un cambio de configuración en el dominio `movies`, pero es preciso identificarse (no recomendado):

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/movies/config
{
  "ClusterConfig": {
    "InstanceType": "c5.xlarge.search"
  }
}
```

Si utiliza uno de los SDK como Boto 3, el SDK se encarga automáticamente de la firma de solicitudes:

```
import boto3

client = boto3.client(es)
response = client.update_domain_config(
  DomainName='movies',
  ClusterConfig={
    'InstanceType': 'c5.xlarge.search'
  }
)
```

Para ver un código de muestra de Java, consulte the section called “Utilizar los SDK de AWS”.

- Para realizar llamadas a las OpenSearch API, debes firmar tus propias solicitudes. Las OpenSearch API utilizan el siguiente formato:

```
domain-id.region.es.amazonaws.com
```

Por ejemplo, la siguiente solicitud busca en el índice `movies` de thor:

```
GET https://my-domain.us-east-1.es.amazonaws.com/movies/_search?q=thor
```

> **Note**
>
> El servicio ignora los parámetros pasados en las direcciones URL de las solicitudes HTTP POST firmadas con Signature Version 4.

Cuando las políticas chocan

Surgen complejidades cuando las políticas están en desacuerdo o no hacen mención explícita a un usuario. Entender cómo funciona IAM en la Guía del usuario de IAM ofrece un breve resumen de la lógica de evaluación de políticas:

- De forma predeterminada, se deniegan todas las solicitudes.
- Un permiso explícito anula esta opción predeterminada.
- Una denegación explícita anula cualquier permiso concedido.

Por ejemplo, si una política basada en recursos le concede acceso a un subrecurso de dominio (un OpenSearch índice o una API), pero una política basada en la identidad le niega el acceso, se le deniega el acceso. Si una política basada en identidad concede acceso y una política basada en recursos no especifica si debe tener acceso o no, tiene permitido el acceso. Consulte la siguiente tabla de políticas que se entrecruzan para acceder a un resumen completo de resultados de subrecursos del dominio.

	Permitido en política basada en recursos	Denegado en política basada en recursos	Ni permitido ni denegado en política basada en recursos
Allowed in identity-based policy	Permitir	Deny	Allow
Denied in identity-based policy	Deny	Deny	Deny
Neither allowed nor denied in identity-based policy	Allow	Deny	Deny

Referencia de los elementos de las políticas

OpenSearch El servicio es compatible con la mayoría de los elementos de política de la Referencia de elementos de política de IAM, con la excepción de. `NotPrincipal` La siguiente tabla muestra los elementos más comunes.

Elemento de política JSON	Resumen
`Version`	La versión actual del idioma de la política es `2012-10-17` . Todas las políticas de acceso deben especificar este valor.
`Effect`	Este elemento especifica si la instrucción permite o deniega el acceso a las acciones especificadas. Los valores válidos son `Allow` o `Deny`.
`Principal`	Este elemento especifica el rol Cuenta de AWS o el usuario de IAM al que se le permite o deniega el acceso a un recurso y puede adoptar varias formas: • AWS cuentas: `"Principal":{"AWS": ["123456789012"]}` o `"Principal":{"AWS": ["arn:aws:iam::123456789012:root"]}` • Usuarios de IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:user/test-user"]}` • Roles de IAM: `"Principal":{"AWS": ["arn:aws:iam::123456789012:role/test-role"]}` **Important** Especificar el comodín * habilita el acceso anónimo al dominio, lo que no se recomienda a menos que agregue una condición basada en IP, utilice la compatibilidad con la VPC o habilite un control de acceso detallado. Además, inspeccione cuidadosa mente las siguientes políticas para confirmar que no otorgan un acceso amplio:

Elemento de política JSON	Resumen
	• Políticas basadas en la identidad asociadas a los AWS direc tores asociados (por ejemplo, las funciones de IAM) • Políticas basadas en recursos asociadas a los AWS recur sos asociados (por ejemplo, claves de KMS) AWS Key Management Service

Elemento de política JSON	Resumen

`Action`	OpenSearch El servicio usa `ESHttp*` acciones para los métodos OpenSearch HTTP. El resto de las acciones se aplican a la API de configuración.
	
	Determinadas acciones `es:` admiten permisos de nivel de recursos. Por ejemplo, puede otorgar a un usuario permisos para eliminar un dominio particular sin dar a dicho usuario permisos para eliminar cualquier dominio. Otras acciones se aplican solo al propio servicio. Por ejemplo, `es:ListDomainNames` no tiene sentido en el contexto de un dominio único y, por lo tanto, requiere un comodín.
	
	Para obtener una lista de todas las acciones disponibles y saber si se aplican a los subrecursos del dominio (`test-domain/*`), a la configuración del dominio (`test-domain`) o solo al servicio (*), consulte Acciones, recursos y claves de condición de Amazon OpenSearch Service en la Referencia de autorización de servicios Las políticas basadas en recursos difieren de los permisos en el nivel de recursos. Las políticas basadas en recursos son políticas JSON completas que se adjuntan a dominios. Los permisos de nivel de recurso permiten restringir acciones a dominios o subrecursos particulares. En la práctica, puede pensar en permisos de nivel de recursos como parte opcional de una política basada en recursos o identidades.
	
	Aunque los permisos de nivel de recurso para `es:CreateDomain` puedan parecer poco intuitivos (después de todo, ¿por qué darle a un usuario permisos para crear un dominio que ya existe?), la utilización de un comodín permite aplicar un esquema de nomenclatura sencillo para sus dominios, por ejemplo `"Resource": "arn:aws:es:us-west-1:987654321098:domain/my-team-name-*"` .
	
	Por supuesto, nada impide que incluya acciones junto a elementos de recursos menos restrictivos, como las siguientes:
	
	`{`
	`"Version": "2012-10-17",`

Elemento de política JSON	Resumen

	<pre>"Statement": [
	  {
	  "Effect": "Allow",
	  "Action": [
	  "es:ESHttpGet",
	  "es:DescribeDomain"
	  ],
	  "Resource": "*"
	  }
	  ]
	}</pre>
	Para obtener más información acerca de las acciones y recursos de emparejamiento, consulte el elemento `Resource` en esta tabla.

`Condition`	OpenSearch El servicio es compatible con la mayoría de las condicion es que se describen en las claves de contexto de condiciones AWS globales de la Guía del usuario de IAM. Entre las excepciones más destacables se incluye la `aws:PrincipalTag` clave, que el OpenSearch servicio no admite.
	
	Al configurar una política basada en IP, debe especificar las direcciones IP o bloque de CIDR como condición, como en el ejemplo siguiente:
	
	<pre>"Condition": {
	  "IpAddress": {
	  "aws:SourceIp": [
	  "192.0.2.0/32"
	  ]
	  }
	}</pre>
	Como se indica en the section called “Políticas basadas en identidades” `aws:ResourceTag` `aws:RequestTag` , las claves de `aws:TagKeys` condición y las claves de condición se aplican tanto a la API de configura ción como a las OpenSearch API.

Elemento de política JSON	Resumen

`Resource`	OpenSearch El servicio utiliza `Resource` los elementos de tres formas básicas:
	
	• Para las acciones que se aplican al propio OpenSearch Servicio, por ejemplo`es:ListDomainNames` , o para permitir el acceso total, utilice la siguiente sintaxis:
	
	`"Resource": "*"`
	
	• Para las acciones que implican la configuración de un dominio, como `es:DescribeDomain` , puede utilizar la siguiente sintaxis:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`"`
	
	• Para las acciones que se aplican a los subrecursos de un dominio, como `es:ESHttpGet` , puede utilizar la siguiente sintaxis:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/*"`
	
	No es necesario utilizar un comodín. OpenSearch El servicio le permite definir una política de acceso diferente para cada OpenSearch índice o API. Por ejemplo, podría limitar los permisos de un usuario al índice `test-index` :
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index"`
	
	En lugar de acceso completo a `test-index` , quizá prefiera limitar la política a solo la API de búsqueda:
	
	`"Resource": "arn:aws:es:` *region*`:`*aws-account-id*`:domain/`*domain-name*`/test-index/_search"`

Elemento de política JSON	Resumen
	Incluso puede controlar el acceso a documentos individuales: `"Resource": "arn:aws:es:  region:aws-account-id:domain/domain-name /test-index/test-type/1"` Básicamente, si OpenSearch expresa el subrecurso como un URI, puede controlar el acceso a él mediante una política de acceso. Para obtener un mayor control sobre los recursos a los que puede obtener acceso un usuario, consulte the section called “Control de acceso detallado”. Para conocer detalles sobre qué acciones admiten los permisos en el nivel de recursos, consulte el elemento `Action` en esta tabla.

Opciones avanzadas y consideraciones de la API

OpenSearch El servicio tiene varias opciones avanzadas, una de las cuales tiene implicaciones en el control de acceso:`rest.action.multi.allow_explicit_index`. En su configuración predeterminada como verdadero, permite a los usuarios omitir los permisos de subrecursos en determinadas circunstancias.

Por ejemplo, tomemos la siguiente política basada en recursos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttp*"
```

```
      ],
      "Resource": [
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/test-index/*",
        "arn:aws:es:us-west-1:987654321098:domain/test-domain/_bulk"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
  ]
}
```

Esta política otorga acceso `test-user` completo a la API OpenSearch masiva `test-index` y a la misma. También permite solicitudes `GET` a `restricted-index`.

La siguiente solicitud de indexación, como cabría esperar, falla debido a un error de permisos:

```
PUT https://search-test-domain.us-west-1.es.amazonaws.com/restricted-index/movie/1
{
  "title": "Your Name",
  "director": "Makoto Shinkai",
  "year": "2016"
}
```

A diferencia de la API index, la API bulk permite crear, actualizar y eliminar muchos documentos en una única llamada. Sin embargo, con frecuencia especifica estas operaciones en el cuerpo de la solicitud, en lugar de la URL de solicitud. Dado que OpenSearch Service utiliza las URL para controlar el acceso a los subrecursos del dominio, `test-user` puede, de hecho, utilizar la API masiva para realizar cambios en ellas. `restricted-index` Aunque el usuario carezca de permisos `POST` en el índice, la siguiente solicitud tiene éxito:

```
POST https://search-test-domain.us-west-1.es.amazonaws.com/_bulk
```

```
{ "index" : { "_index": "restricted-index", "_type" : "movie", "_id" : "1" } }
{ "title": "Your Name", "director": "Makoto Shinkai", "year": "2016" }
```

En esta situación, la política de acceso no consigue cumplir su objetivo. Para evitar que los usuarios omitan este tipo de restricciones, puede cambiar `rest.action.multi.allow_explicit_index` a falso. Si este valor es falso, todas las llamadas a las API bulk, mget y msearch que especifican nombres de índice en el cuerpo de la solicitud dejan de funcionar. En otras palabras, las llamadas a `_bulk` ya no funcionan, pero las llamadas a `test-index/_bulk` sí. Este segundo punto de conexión contiene un nombre de índice, por lo que no es necesario especificar uno en el cuerpo de la solicitud.

OpenSearch Los paneles dependen en gran medida de mget y msearch, por lo que es poco probable que funcionen correctamente después de este cambio. Como remedio parcial, puede dejar `rest.action.multi.allow_explicit_index` como verdadero y denegar a determinados usuarios el acceso a una o varias de estas API.

Para obtener más información acerca de cómo cambiar esta configuración, consulte the section called “Configuración avanzada de clústeres”.

Del mismo modo, la siguiente política basada en recursos contiene dos problemas sutiles:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/*"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/test-user"
      },
      "Action": "es:ESHttp*",
      "Resource": "arn:aws:es:us-west-1:987654321098:domain/test-domain/restricted-
index/*"
    }
```

```
  ]
}
```

- A pesar de la denegación explícita, `test-user` puede seguir realizando llamadas como, por ejemplo, `GET https://search-test-domain.us-west-1.es.amazonaws.com/_all/_search` y `GET https://search-test-domain.us-west-1.es.amazonaws.com/*/_search` para acceder a los documentos en `restricted-index`.
- Dado que el elemento `Resource` hace referencia a `restricted-index/*`, `test-user` no tiene permisos para acceder directamente a los documentos del índice. El usuario, sin embargo, tiene permisos para eliminar todo el índice. Para evitar el acceso y la eliminación, la política debe especificar en su lugar `restricted-index*`.

En lugar de combinar permisos amplios y denegaciones delimitadas, el enfoque más seguro consiste en seguir el principio de privilegio mínimo y conceder solo los permisos requeridos para realizar una tarea. Para obtener más información sobre cómo controlar el acceso a índices u OpenSearch operaciones individuales, consulte. the section called “Control de acceso detallado”

> **Important**
>
> Al especificar el comodín *, se permite el acceso anónimo a su dominio. No se recomienda utilizar el comodín. Además, inspeccione detenidamente las siguientes políticas para confirmar que no conceden un acceso amplio:
>
> - Políticas basadas en la identidad asociadas a los AWS directores asociados (por ejemplo, las funciones de IAM)
> - Políticas basadas en recursos asociadas a los AWS recursos asociados (por ejemplo, claves de KMS) AWS Key Management Service

Configurar políticas de acceso

- Para obtener instrucciones sobre cómo crear o modificar políticas basadas en recursos e IP en OpenSearch Service, consulte. the section called “Configurar políticas de acceso”
- Para obtener instrucciones sobre la creación o modificación de políticas basadas en identidad en IAM, consulte Crear políticas de IAM en la Guía del usuario de IAM.

Políticas de muestra adicionales

Si bien este capítulo incluye muchos ejemplos de políticas, el control de AWS acceso es un tema complejo que se entiende mejor con ejemplos. Para más información, consulte Ejemplos de políticas de IAM basadas en identidad en la Guía del usuario de IAM.

Referencia de permisos OpenSearch de la API de Amazon Service

Cuando configura el control de acceso, escribe políticas de permiso que puede adjuntar a una identidad de IAM (políticas basadas en identidad). Para obtener más información detallada de referencia, consulte los siguientes temas en la Referencia de autorizaciones de servicio:

- Claves de condición, recursos y acciones del servicio. OpenSearch
- Claves de acciones, recursos y condiciones de OpenSearch Ingestion.

Esta referencia contiene información sobre las operaciones de la API que se pueden utilizar en una política de IAM. También incluye el AWS recurso para el que puede conceder los permisos y las claves de condición que puede incluir para un control de acceso detallado.

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 para el OpenSearch Servicio, usa el `es:` prefijo seguido del nombre de la operación de la API (por ejemplo,). `es:CreateDomain` Para especificar una acción para la OpenSearch ingestión, usa el `osis:` prefijo seguido de la operación de API (por ejemplo,). `osis:CreatePipeline`

AWS políticas gestionadas para Amazon OpenSearch Service

Una política AWS gestionada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que

actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AmazonOpenSearchServiceFullAccess

Otorga acceso completo a las operaciones y los recursos de la API de configuración del OpenSearch servicio para un Cuenta de AWS.

Puede encontrar la AmazonOpenSearchServiceFullAccesspolítica en la consola de IAM.

AmazonOpenSearchServiceReadOnlyAccess

Otorga acceso de solo lectura a todos los recursos del OpenSearch Servicio para un. Cuenta de AWS

Puede encontrar la AmazonOpenSearchServiceReadOnlyAccesspolítica en la consola de IAM.

AmazonOpenSearchServiceRolePolicy

No puede asociar `AmazonOpenSearchServiceRolePolicy` a sus entidades IAM. Esta política está asociada a un rol vinculado al servicio que permite al OpenSearch Servicio acceder a los recursos de la cuenta. Para obtener más información, consulte the section called “Permisos”.

Puede encontrar la AmazonOpenSearchServiceRolePolicypolítica en la consola de IAM.

AmazonOpenSearchServiceCognitoAccess

Proporciona los permisos mínimos de Amazon Cognito necesarios para habilitar la autenticación de Cognito.

Puedes encontrar la AmazonOpenSearchServiceCognitoAccesspolítica en la consola de IAM.

AmazonOpenSearchIngestionServiceRolePolicy

No puede asociar `AmazonOpenSearchIngestionServiceRolePolicy` a sus entidades IAM. Esta política se adjunta a una función vinculada a un servicio que permite a OpenSearch Ingestion habilitar el acceso a la VPC para las canalizaciones de ingestión, crear etiquetas y publicar métricas relacionadas con la ingestión en su cuenta. CloudWatch Para obtener más información, consulte the section called “Uso de roles vinculados a servicios”.

Puedes encontrar la política en la consola de IAM. AmazonOpenSearchIngestionServiceRolePolicy

AmazonOpenSearchIngestionFullAccess

Otorga acceso completo a las operaciones y los recursos de la API de OpenSearch ingestión para un. Cuenta de AWS

Puede encontrar la AmazonOpenSearchIngestionFullAccesspolítica en la consola de IAM.

AmazonOpenSearchIngestionReadOnlyAccess

Otorga acceso de solo lectura a todos los recursos de OpenSearch Ingestion durante un. Cuenta de AWS

Puede encontrar la AmazonOpenSearchIngestionReadOnlyAccesspolítica en la consola de IAM.

AmazonOpenSearchServerlessServiceRolePolicy

Proporciona los Amazon CloudWatch permisos mínimos necesarios para enviar datos de métricas OpenSearch sin servidor a. CloudWatch

Puede encontrar la AmazonOpenSearchServerlessServiceRolePolicypolítica en la consola de IAM.

OpenSearch Actualizaciones del servicio para las políticas AWS gestionadas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas del OpenSearch Servicio desde que este servicio comenzó a realizar un seguimiento de los cambios.

Cambio	Descripción	Fecha
Actualización de `AmazonOpenSearchServiceRolePolicy` y `AmazonElasticsearchServiceRolePolicy`	Se añadieron los permisos necesarios para que el rol vinculado al servicio asigne y desasigne direcciones IPv6. La política de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores.	18 de octubre de 2023

Cambio	Descripción	Fecha
Se ha agregado `AmazonOpenSearchIngestionServiceRolePolicy`	Una nueva política que permite a OpenSearch Ingestion habilitar el acceso a la VPC para las canalizaciones de ingestión, crear etiquetas y publicar métricas relacionadas con la CloudWatch ingestión en su cuenta. Para ver la política JSON, consulte la consola de IAM.	26 de abril de 2023
Se ha agregado `AmazonOpenSearchIngestionFullAccess`	Una nueva política que otorga acceso total a las operaciones y los recursos de la API de OpenSearch Ingestion para un. Cuenta de AWS Para ver la política JSON, consulte la consola de IAM.	26 de abril de 2023
Se ha agregado `AmazonOpenSearchIngestionReadOnlyAccess`	Una nueva política que otorga acceso de solo lectura a todos los recursos de OpenSearch Ingestion para un. Cuenta de AWS Para ver la política JSON, consulte la consola de IAM.	26 de abril de 2023

Cambio	Descripción	Fecha
Se ha agregado `AmazonOpenSearchServerlessServiceRolePolicy`	Una nueva política que proporciona los permisos mínimos necesarios para enviar datos de métricas OpenSearch sin servidor a. Amazon CloudWatch Para ver la política JSON, consulte la consola de IAM.	29 de noviembre de 2022
Actualización de `AmazonOpenSearchServiceRolePolicy` y `AmazonElasticsearchServiceRolePolicy`	Se agregaron los permisos necesarios para que la función vinculada al servicio cree puntos de enlace de VPC OpenSearch gestionados por el servicio. Algunas acciones solo se pueden realizar cuando la solicitud contiene la etiqueta `OpenSearchManaged=true` . La política de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores.	7 de noviembre de 2022

Cambio	Descripción	Fecha
Actualización de `AmazonOpenSearchServiceRolePolicy` y `AmazonElasticsearchServiceRolePolicy`	Se agregó soporte para la `PutMetricData` acción, que es necesario para publicar las métricas OpenSearch del clúster en Amazon CloudWatch. La política de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores. Para ver la política JSON, consulte la consola de IAM.	12 de septiembre de 2022
Actualización de `AmazonOpenSearchServiceRolePolicy` y `AmazonElasticsearchServiceRolePolicy`	Se ha agregado compatibilidad con el tipo de recurso `acm`. La política proporciona el permiso mínimo AWS Certificate Manager (ACM) de solo lectura necesario para que el rol vinculado al servicio verifique y valide los recursos de ACM con el fin de crear y actualizar dominios personalizados habilitados para terminales. La política de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores.	28 de julio de 2022

Cambio	Descripción	Fecha
Actualización de `AmazonOpenSearchServiceCognitoAccess` y `AmazonESCognitoAccess`	Se agregó soporte para la `UpdateUserPoolClient` acción, que es necesario para establecer la configuración del grupo de usuarios de Cognito durante la actualización de Elasticsearch a. OpenSearch Se han corregido los permisos de la acción `SetIdentityPoolRoles` para permitir el acceso a todos los recursos. La política de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores.	20 de diciembre de 2021
Se ha actualizado `AmazonOpenSearchServiceRolePolicy`	Se ha agregado compatibilidad con el tipo de recurso `security-group` . La política proporciona los permisos mínimos de Amazon EC2 y Elastic Load Balancing necesarios para el rol vinculado a servicios a fin de habilitar el acceso mediante la VPC.	9 de septiembre de 2021

Cambio	Descripción	Fecha
• Se ha agregado `AmazonOpenSearchServiceFullAccess` • Se ha dado de baja `AmazonESFullAccess`	Esta nueva política tiene por objeto sustituir a la política anterior. Ambas políticas proporcionan acceso completo a la API de configuración del OpenSearch servicio y a todos los métodos HTTP de las API. OpenSearch El control de acceso detallado y las políticas basadas en recursos aún pueden restringir el acceso.	7 de septiembre de 2021
• Se ha agregado `AmazonOpenSearchServiceReadOnlyAccess` • Se ha dado de baja `AmazonESReadOnlyAccess`	Esta nueva política tiene por objeto sustituir a la política anterior. Ambas políticas proporcionan acceso de solo lectura a la API de configuración del OpenSearch servicio (`es:Describe* es:List*`, `yes:Get*`) y no proporcionan acceso a los métodos HTTP de las OpenSearch API.	7 de septiembre de 2021
• Se ha agregado `AmazonOpenSearchServiceCognitoAccess` • Se ha dado de baja `AmazonESCognitoAccess`	Esta nueva política tiene por objeto sustituir a la política anterior. Ambas políticas proporcionan los permisos mínimos de Amazon Cognito necesarios para habilitar la autenticación de Cognito.	7 de septiembre de 2021

Cambio	Descripción	Fecha
• Se ha agregado AmazonOpenSearchServiceRolePolicy • Se ha dado de baja `AmazonElasticsearchServiceRolePolicy`	Esta nueva política tiene por objeto sustituir a la política anterior. Ambas políticas proporcionan los permisos mínimos de Amazon EC2 y Elastic Load Balancing necesarios para el rol vinculado a servicios a fin de habilitar el acceso mediante la VPC.	7 de septiembre de 2021
Comenzó el seguimiento de los cambios	Amazon OpenSearch Service ahora rastrea los cambios en las políticas AWS gestionadas.	7 de septiembre de 2021

Prevención del suplente confuso entre servicios

El problema del suplente confuso es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema del suplente confuso. La suplantación entre servicios puede producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que lo ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Se recomienda utilizar las claves de contexto de condición global `aws:SourceArn` y `aws:SourceAccount` en las políticas de recursos para limitar los permisos que Amazon OpenSearch Service concede a otro servicio para el recurso. Si el valor de `aws:SourceArn` no contiene el ID de cuenta, como un ARN de bucket de Amazon S3, debe utilizar ambas claves de contexto de condición global para limitar los permisos. Si utiliza claves de contexto de condición global y el valor de `aws:SourceArn` contiene el ID de cuenta, el valor de `aws:SourceAccount` y

la cuenta en el valor de `aws:SourceArn` deben utilizar el mismo ID de cuenta cuando se utiliza en la misma instrucción de política. Utilice `aws:SourceArn` si desea que solo se asocie un recurso al acceso entre servicios. Utilice `aws:SourceAccount` si quiere permitir que cualquier recurso de esa cuenta se asocie al uso entre servicios.

El valor de `aws:SourceArn` debe ser el ARN del dominio OpenSearch Service.

La forma más eficaz de protegerse contra el problema del suplente confuso es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utilice la clave de condición de contexto global `aws:SourceArn` con comodines (*) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:es:*:123456789012:*`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en OpenSearch Service para evitar el problema del adjunto confundido.

```
{
   "Version":"2012-10-17",
   "Statement":{
      "Sid":"ConfusedDeputyPreventionExamplePolicy",
      "Effect":"Allow",
      "Principal":{
         "Service":"es.amazonaws.com"
      },
      "Action":"sts:AssumeRole",
      "Condition":{
         "StringEquals":{
            "aws:SourceAccount":"123456789012"
         },
         "ArnLike":{
            "aws:SourceArn":"arn:aws:es:region:123456789012:domain/my-domain"
         }
      }
   }
}
```

Control de acceso detallado en Amazon Service OpenSearch

El control de acceso detallado ofrece formas adicionales de controlar el acceso a tus datos en Amazon Service. OpenSearch Por ejemplo, puede ser conveniente que, según quién realice la

solicitud, una búsqueda devuelva los resultados de un solo índice. Es posible que desee ocultar determinados campos en los documentos o excluir algunos documentos por completo.

El control de acceso detallado ofrece las siguientes características:

- Control de acceso con base en roles
- Seguridad en el nivel de índice, de documento y de campo
- OpenSearch Paneles de mandos: multiusuario
- Autenticación básica HTTP para paneles y paneles OpenSearch OpenSearch

Temas

Un panorama más amplio: control de acceso detallado y seguridad del servicio OpenSearch

La seguridad OpenSearch de Amazon Service consta de tres capas principales:

Red

La primera capa de seguridad es la red, que determina si las solicitudes llegan a un dominio OpenSearch de servicio. Si elige Acceso público al crear un dominio, las solicitudes procedentes de cualquier cliente conectado a Internet pueden llegar al punto de conexión del dominio. Si elige Acceso a la VPC, los clientes deben conectarse a la VPC (y los grupos de seguridad asociados deben permitirlo) para que una solicitud llegue al punto de conexión. Para obtener más información, consulte the section called “Compatibilidad con VPC”.

Política de acceso al dominio

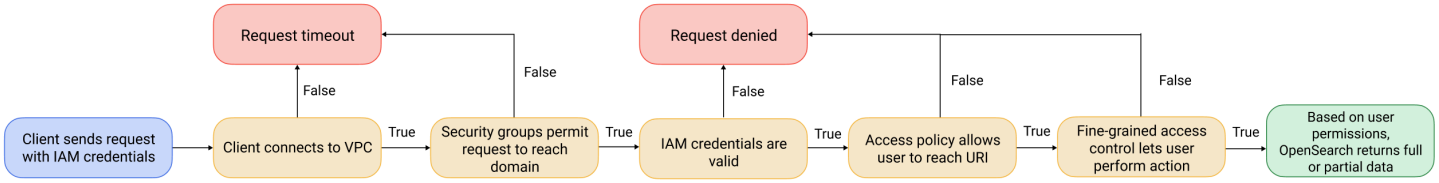
La segunda capa de seguridad es la política de acceso al dominio. Una vez que una solicitud llega a un punto de conexión del dominio, la política de acceso con base en recursos permite o deniega el acceso de la solicitud a un URI determinado. La política de acceso acepta o rechaza las solicitudes en el «límite» del dominio, antes de que lleguen a OpenSearch propiamente dicho.

Control de acceso detallado

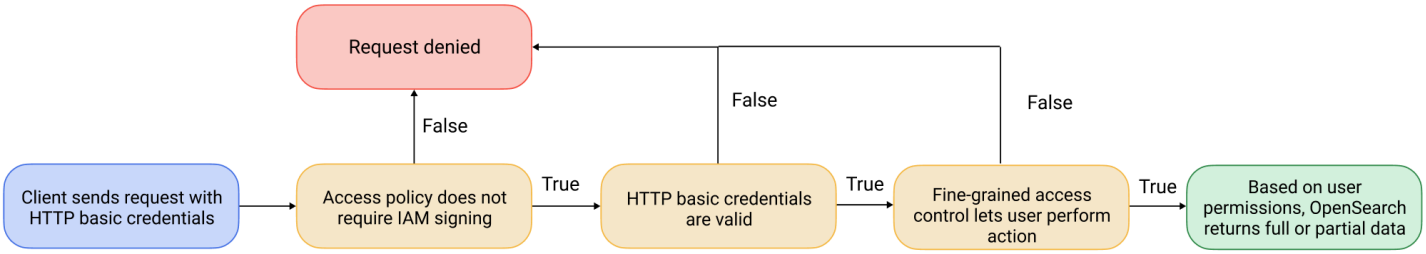
La tercera y última capa de seguridad es el control de acceso detallado. Una vez que una política de acceso con base en recursos ha permitido que una solicitud llegue a un punto de conexión del dominio, el control de acceso detallado evalúa las credenciales del usuario y lo autentica o bien deniega la solicitud. Si el control de acceso detallado autentica al usuario, obtiene todos los roles mapeados a ese usuario y utiliza el conjunto completo de permisos para determinar cómo gestionar la solicitud.

> **Note**
>
> Si una política de acceso basada en recursos contiene funciones o usuarios de IAM, los clientes deben enviar las solicitudes firmadas mediante la versión 4 de AWS Signature. Como tales, las políticas de acceso pueden entrar en conflicto con el control de acceso detallado, sobre todo si se utiliza la base de datos de usuarios interna y la autenticación básica de HTTP. No se puede firmar una solicitud con un nombre de usuario y contraseña y también con credenciales de IAM. En general, si habilita el control de acceso detallado, se recomienda utilizar una política de acceso al dominio que no requiera solicitudes firmadas.

Este primer diagrama ilustra una configuración habitual: un dominio de acceso a la VPC con el control de acceso detallado habilitado, una política de acceso con base en IAM y un usuario maestro de IAM.



Este segundo diagrama ilustra otra configuración habitual: un dominio de acceso público con el control de acceso detallado habilitado, una política de acceso que no utiliza principales de IAM y un usuario maestro en la base de datos de usuarios interna.



Ejemplo

Supongamos que se realiza una solicitud `GET` a `movies/_search?q=thor`. ¿El usuario tiene permisos para buscar en el índice `movies`? En caso afirmativo, ¿el usuario tiene permisos para ver todos los documentos que contiene? ¿La respuesta debería omitir o anonimizar algún campo? Para el usuario maestro, la respuesta podría tener este aspecto:

```
{
  "hits": {
    "total": 7,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "directors": [
            "Kenneth Branagh",
            "Joss Whedon"
          ],
          "release_date": "2011-04-21T00:00:00Z",
```

```
          "genres": [
            "Action",
            "Adventure",
            "Fantasy"
          ],
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor",
          "actors": [
            "Chris Hemsworth",
            "Anthony Hopkins",
            "Natalie Portman"
          ],
          "year": 2011
        }
      },
      ...
    ]
  }
}
```

Si un usuario con permisos más limitados emite exactamente la misma solicitud, la respuesta podría tener el siguiente aspecto:

```
{
  "hits": {
    "total": 2,
    "max_score": 8.772789,
    "hits": [{
        "_index": "movies",
        "_type": "_doc",
        "_id": "tt0800369",
        "_score": 8.772789,
        "_source": {
          "year": 2011,
          "release_date":
 "3812a72c6dd23eef3c750c2d99e205cbd260389461e19d610406847397ecb357",
          "plot": "The powerful but arrogant god Thor is cast out of Asgard to
 live amongst humans in Midgard (Earth), where he soon becomes one of their finest
 defenders.",
          "title": "Thor"
        }
```

```
      },
      ...
    ]
  }
}
```

La respuesta contiene menos aciertos y menos campos para cada acierto. Además, el campo `release_date` está anonimizado. Si un usuario sin permisos realiza la misma solicitud, el clúster devuelve un error:

```
{
  "error": {
    "root_cause": [{
      "type": "security_exception",
      "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
    }],
    "type": "security_exception",
    "reason": "no permissions for [indices:data/read/search] and User [name=limited-
user, roles=[], requestedTenant=null]"
  },
  "status": 403
}
```

Si un usuario proporciona credenciales no válidas, el clúster devuelve una excepción `Unauthorized`.

Conceptos clave

Al comenzar con un control de acceso detallado, tenga en cuenta los siguientes conceptos:

- Funciones: la forma principal de utilizar un control de acceso detallado. En este caso, se trata de roles distintos de los roles de IAM. Los roles contienen cualquier combinación de permisos: para todo el clúster, específicos del índice, en el nivel de documento y en el nivel de campo.
- Mapeo: después de configurar un rol, se asigna a uno o más usuarios. Por ejemplo, puede mapear tres roles a un solo usuario: un rol que proporciona acceso a Dashboards, otro que proporciona acceso de solo lectura a `index1` y otro que proporciona acceso de escritura a `index2`. Si lo prefiere, puede incluir todos esos permisos en un solo rol.

- Usuarios: personas o aplicaciones que realizan solicitudes al OpenSearch clúster. Los usuarios tienen credenciales, ya sean claves de acceso de IAM o un nombre de usuario y una contraseña, que especifican al realizar las solicitudes.

Acerca del usuario maestro

El usuario maestro de OpenSearch Service es una combinación de nombre de usuario y contraseña, o un usuario principal de IAM, que tiene todos los permisos para acceder al OpenSearch clúster subyacente. Se considera que un usuario es un usuario maestro si tiene todos los accesos al OpenSearch clúster y la capacidad de crear usuarios internos, funciones y asignaciones de funciones en los paneles de control. OpenSearch

Un usuario maestro creado en la consola OpenSearch de servicio o mediante la CLI se asigna automáticamente a dos funciones predefinidas:

- `all_access`— Proporciona acceso total a todas las operaciones del clúster, permiso para escribir en todos los índices del clúster y permiso para escribir para todos los inquilinos.
- `security_manager`— Proporciona acceso al complemento de seguridad y gestiona los usuarios y los permisos.

Con estas dos funciones, el usuario accede a la pestaña Seguridad de los OpenSearch paneles, donde puede gestionar los usuarios y los permisos. Si crea otro usuario interno y solo lo asigna al `all_access` rol, el usuario no tendrá acceso a la pestaña Seguridad. Puede crear usuarios maestros adicionales asignándolos de forma explícita a `all_access` ambos `security_manager` roles. Para ver instrucciones, consulte the section called “Usuarios maestros adicionales”.

Al crear un usuario maestro para su dominio, puede especificar un usuario principal de IAM existente o crear un usuario maestro en la base de datos de usuarios interna. Tenga en cuenta lo siguiente a la hora de decidir cuál utilizar:

- Principal de IAM: si elige un principal de IAM para su usuario maestro, todas las solicitudes al clúster deben firmarse con la versión 4 de AWS Signature.

  OpenSearch El servicio no tiene en cuenta ninguno de los permisos del director de IAM. El usuario o rol de IAM sirve únicamente para la autenticación. Las políticas de ese usuario o rol no influyen en la autorización del usuario maestro. La autorización se gestiona a través de los distintos permisos del complemento OpenSearch de seguridad.

Por ejemplo, no puede asignar ningún permiso de IAM a un responsable de IAM y, siempre que la máquina o la persona puedan autenticarse ante ese usuario o función, tendrán el poder de usuario maestro de Service. OpenSearch

Recomendamos IAM si quiere usar los mismos usuarios en varios clústeres, si quiere usar Amazon Cognito para acceder a los paneles o si OpenSearch tiene clientes que admiten la firma de Signature Version 4.

- Base de datos de usuarios interna: si crea una base de datos maestra en la base de datos de usuarios interna (con una combinación de nombre de usuario y contraseña), puede utilizar la autenticación básica HTTP (además de las credenciales de IAM) para realizar solicitudes al clúster. La mayoría de los clientes admiten la autenticación básica, incluido curl, que también es compatible con la versión 4 de AWS Signature con la opción --aws-sigv4. La base de datos interna de usuarios se almacena en un OpenSearch índice, por lo que no puede compartirla con otros clústeres.

  Recomendamos la base de datos de usuarios interna si no se requiere reutilizar los usuarios en varios clústeres, si se desea utilizar la autenticación básica de HTTP para obtener acceso a Dashboards (en lugar de Amazon Cognito) o si se tienen clientes que solo admiten la autenticación básica. La base de datos de usuarios interna es la forma más sencilla de empezar a usar OpenSearch Service.

Habilitar el control de acceso detallado

Habilite un control de acceso detallado mediante la consola o la API de AWS CLIconfiguración. Para ver los pasos, consulte Creación y administración de dominios.

El control de acceso detallado requiere OpenSearch Elasticsearch 6.7 o una versión posterior. También requiere HTTPS para todo el tráfico al dominio, el cifrado de los datos en reposo y el cifrado. node-to-node Según cómo configure las características avanzadas del control de acceso detallado, el procesamiento adicional de sus solicitudes puede requerir recursos de cómputo y memoria en nodos de datos individuales. Después de habilitar el control de acceso detallado, no puede desactivarlo.

Habilitar el control de acceso detallado en los dominios existentes

Puedes habilitar un control de acceso detallado en los dominios existentes que ejecuten Elasticsearch 6.7 OpenSearch o una versión posterior.

Para habilitar el control de acceso detallado en un dominio existente (consola)

1. Seleccione el dominio y elija Acciones y Editar la configuración de seguridad.
2. Seleccione Habilitar el control de acceso detallado,
3. Seleccione cómo crear el usuario maestro:
   - Si desea utilizar IAM para la gestión de usuarios, seleccione Establecer ARN de IAM como usuario maestro y especifique el ARN para un rol de IAM.
   - Si desea utilizar la base de datos de usuarios interna, seleccione Crear usuario maestro y especifique un nombre de usuario y una contraseña.
4. (Opcional) Seleccione Habilitar el período de migración para la política de acceso abierta o basada en IP. Esta configuración permite un período de transición de 30 días durante el cual los usuarios existentes pueden seguir accediendo al dominio sin interrupciones, y las políticas de acceso basadas en IP y abiertas existentes seguirán funcionando con su dominio. Durante este período de migración, recomendamos a los administradores crear los roles necesarios y asignarlos a los usuarios para el dominio. Si utiliza políticas basadas en la identidad en lugar de una política de acceso abierta o basada en la IP, puede desactivar esta configuración.

   También debe actualizar sus clientes para que trabajen con un control de acceso de grano fino durante el periodo de migración. Por ejemplo, si asignas las funciones de IAM a un control de acceso detallado, debes actualizar tus clientes para empezar a firmar las solicitudes con la versión 4 de Signature. AWS Si configura la autenticación básica HTTP con un control de acceso detallado, debe actualizar los clientes para proporcionar las credenciales de autenticación básicas adecuadas en las solicitudes.

   Durante el período de migración, los usuarios que accedan al terminal de OpenSearch Dashboards del dominio accederán directamente a la página Discover en lugar de a la página de inicio de sesión. Los administradores y los usuarios maestros pueden elegir Inicio de sesión para iniciar sesión con credenciales de administrador y configurar asignaciones de roles.

   > **Important**
   >
   > OpenSearch El servicio desactiva automáticamente el período de migración después de 30 días. Recomendamos finalizarlo tan pronto como cree los roles necesarios y los asigne a los usuarios. Una vez finalizado el período de migración, no puedes volver a habilitarlo.

5. Seleccione Guardar cambios.

El cambio desencadena una implementación azul-verde durante el cual el estado del clúster se vuelve rojo, pero todas las operaciones de clúster no se ven afectadas.

Para habilitar el control de acceso detallado en un dominio (CLI) existente

Establezca `AnonymousAuthEnabled` a `true` para habilitar el período de migración con un control de acceso detallado:

```
aws opensearch update-domain-config --domain-name test-domain --region us-east-1 \
      --advanced-security-options '{ "Enabled": true,
 "InternalUserDatabaseEnabled":true, "MasterUserOptions": {"MasterUserName":"master-
username","MasterUserPassword":"master-password"},"AnonymousAuthEnabled": true}'
```

Acerca del default_role

El control de acceso detallado requiere asignación de roles. Si tu dominio usa políticas de acceso basadas en la identidad, OpenSearch Service asigna automáticamente a tus usuarios a un nuevo rol llamado default_role para ayudarte a migrar correctamente a los usuarios existentes. Esta asignación temporal garantiza que los usuarios puedan seguir enviando correctamente solicitudes GET y PUT firmadas por IAM hasta que cree sus propias asignaciones de roles.

La función no añade ninguna vulnerabilidad o fallo de seguridad a tu dominio de servicio. OpenSearch Recomendamos eliminar el rol predeterminado tan pronto como configure sus propios roles y los asigne en consecuencia.

Escenarios de migración

La siguiente tabla describe el comportamiento de cada método de autenticación antes y después de habilitar el control de acceso detallado en un dominio existente, y los pasos que deben seguir los administradores para asignar correctamente sus usuarios a los roles:

Método de autenticación	Antes de habilitar el control de acceso detallado	Después de habilitar el control de acceso detallado	Tareas administrativas
Políticas basadas en identidades	Todos los usuarios que cumplan la política de IAM pueden acceder al dominio.	No es necesario habilitar el período de migración. OpenSearch El servicio asigna automáticamente a todos los usuarios que cumplen la política de IAM al default_role para que puedan seguir accediendo al dominio.	1. Cree asignaciones de roles personalizadas en el dominio. 2. Elimine las default_role.
Políticas basadas en IP	Todos los usuarios de las direcciones IP permitidas o los bloques de CIDR pueden acceder al dominio.	Durante el período de migración de 30 días, todos los usuarios de las direccion es IP permitida s o los bloques de CIDR pueden seguir accediendo al dominio.	1. Cree asignaciones de roles personalizadas en el dominio. 2. Actualice sus clientes para proporcionar credenciales de autenticación básicas o credencia les de IAM, según la configuración de asignación de roles. 3. Desactive el período de migración. Los usuarios de las direcciones IP permitidas o los bloques de CIDR que envían solicitudes sin autentica ción básica o credenciales de IAM perderán el acceso al dominio.
Políticas de acceso abierto	Todos los usuarios en Internet	Durante el período de migración de 30 días, todos los usuarios	1. Cree asignaciones de roles en el dominio.

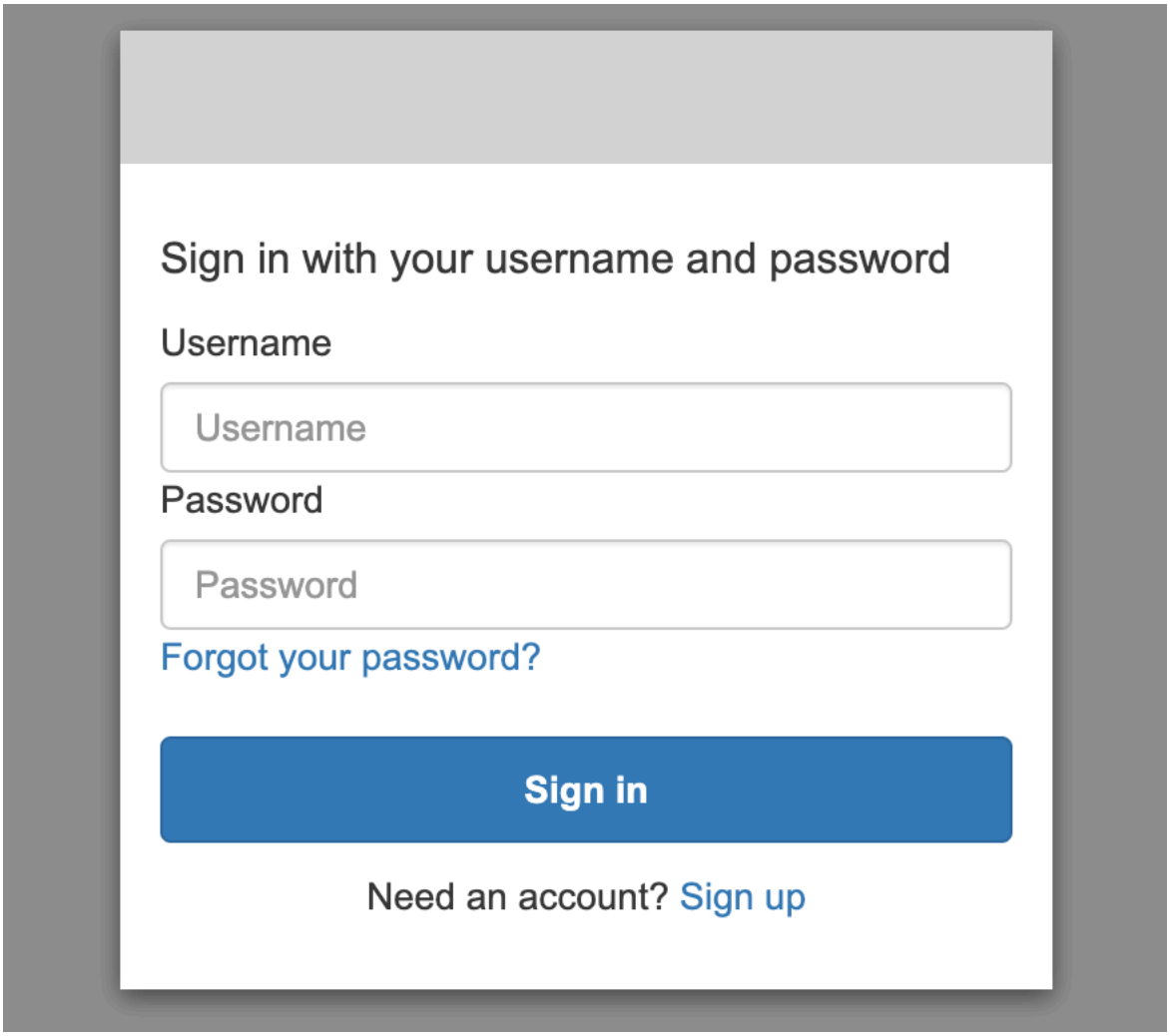
Método de autenticación	Antes de habilitar el control de acceso detallado	Después de habilitar el control de acceso detallado	Tareas administrativas
	pueden acceder al dominio.	de Internet pueden seguir accediendo al dominio.	2. Actualice sus clientes para proporcionar credenciales de autenticación básicas o credencia les de IAM, según la configuración de asignación de roles. 3. Desactive el período de migración. Los usuarios que envíen solicitudes sin autenticación básica o credencia les de IAM perderán el acceso al dominio.

Acceder a los OpenSearch paneles de control como usuario maestro

El control de acceso detallado tiene un complemento de OpenSearch paneles de control que simplifica las tareas de administración. Puede utilizar Dashboards para administrar usuarios, roles, mapeos, grupos de acciones e inquilinos. Sin embargo, la página de inicio de sesión de OpenSearch Dashboards y el método de autenticación subyacente varían según la forma en que administre los usuarios y configure su dominio.

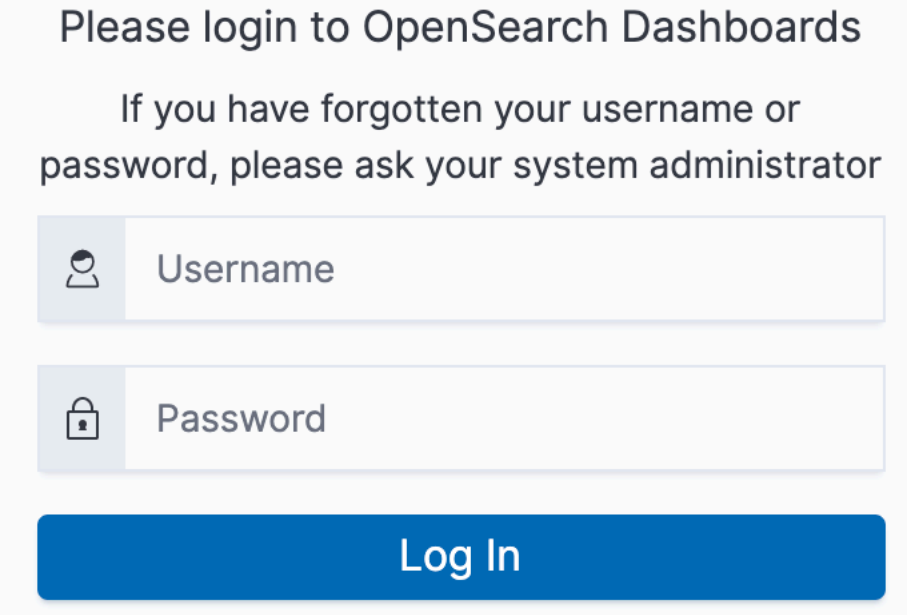
- Si desea utilizar IAM para la administración de usuarios, utilice the section called “Descripción de la autenticación de Amazon Cognito para OpenSearch Dashboards” para acceder a Dashboards. De lo contrario, Dashboards muestra una página de inicio de sesión no funcional. Consulte the section called “Limitaciones”.

  Con la autenticación de Amazon Cognito, uno de los roles asumidos del grupo de identidades debe coincidir con el rol de IAM especificado para el usuario maestro. Para obtener más información acerca de esta configuración, consulte the section called “(Opcional) Configuración de acceso pormenorizado” y the section called “Tutorial: Control de acceso detallado con la autenticación de Cognito”.



- Si decide utilizar la base de datos de usuarios interna, puede iniciar sesión en Dashboards con su nombre de usuario maestro y contraseña. Debe obtener acceso a Dashboards a través de HTTPS. La autenticación de Amazon Cognito y SAML para Dashboards reemplazan esta pantalla de inicio de sesión.

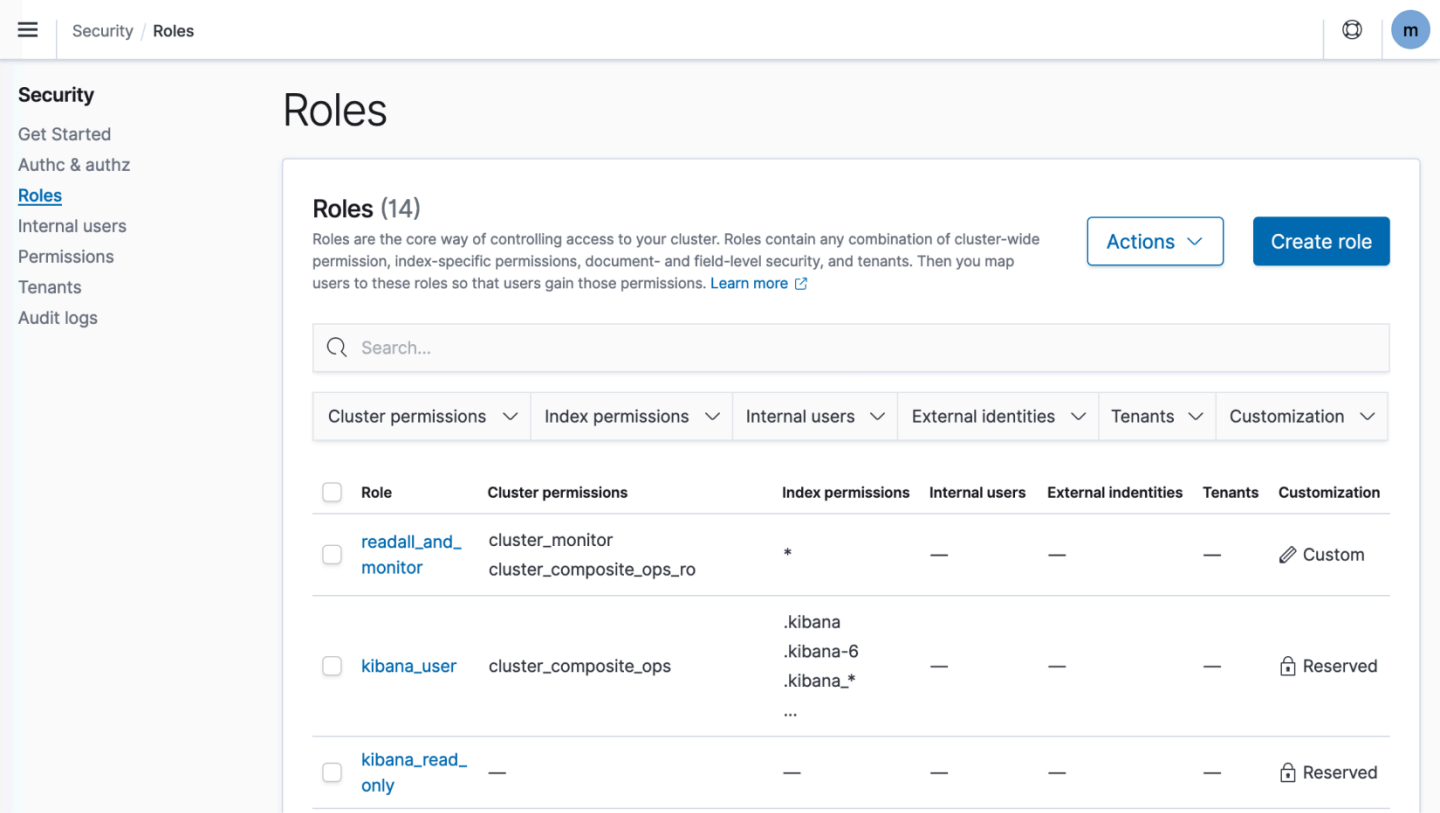
  Para obtener más información acerca de esta configuración, consulte the section called “Tutorial: Base de datos de usuarios interna con autenticación básica”.



- Si elige utilizar la autenticación SAML, puede iniciar sesión con credenciales de un proveedor de identidad externo. Para obtener más información, consulte the section called “Autenticación SAML para paneles OpenSearch ”.

Administrar permisos

Tal y como se indica en the section called “Conceptos clave”, puede administrar los permisos de control de acceso detallado mediante roles, usuarios y mapeos. En esta sección, se describe cómo crear y aplicar esos recursos. Recomendamos que inicie sesión en Dashboards como usuario maestro para realizar estas operaciones.



> **Note**
>
> Los permisos que elige conceder a los usuarios varían ampliamente en función del caso de uso. No podemos cubrir de forma factible todos los escenarios de esta documentación. Al determinar qué permisos conceder a sus usuarios, asegúrese de consultar los permisos de OpenSearch clúster e indexación que se mencionan en las siguientes secciones y siga siempre el principio de privilegios mínimos.

Crear roles

Puede crear nuevas funciones para un control de acceso más detallado mediante los OpenSearch paneles de control o la `_plugins/_security` operación en la API REST. Para obtener más información, consulte Create roles (Crear roles).

El control de acceso detallado también incluye varios roles predefinidos. Los clientes como OpenSearch Dashboards y Logstash realizan una amplia variedad de solicitudes OpenSearch, lo que puede dificultar la creación manual de roles con el conjunto mínimo de permisos. Por ejemplo, el rol `opensearch_dashboards_user` incluye los permisos que un usuario necesita para trabajar con

patrones de índices, visualizaciones, paneles e inquilinos. Recomendamos mapearlo a cualquier rol de usuario o backend que tenga acceso a Dashboards, junto con los roles adicionales que permitan el acceso a otros índices.

Amazon OpenSearch Service no ofrece las siguientes OpenSearch funciones:

- `observability_full_access`
- `observability_read_access`
- `reports_read_access`
- `reports_full_access`

Amazon OpenSearch Service ofrece varios roles que no están disponibles en OpenSearch:

- `ultrawarm_manager`
- `ml_full_access`
- `cold_manager`
- `notifications_full_access`
- `notifications_read_access`

Seguridad en el nivel del clúster

Los permisos en el nivel del clúster incluyen la capacidad de ejecutar solicitudes generales como `_mget`, `_msearch` y `_bulk`, monitorear el estado o tomar instantáneas, etc. Administre estos permisos mediante la sección Permisos de clúster al crear un rol. Para obtener una lista completa de los permisos de nivel de clúster, consulte Permisos de cluster.

En lugar de permisos individuales, a menudo puede alcanzar la posición de seguridad deseada mediante una combinación de los grupos de acciones predeterminadas. Para obtener una lista de grupos de acciones en el nivel del clúster, consulte Nivel del clúster.

Seguridad en el nivel del índice

Los permisos en el nivel del índice incluyen la capacidad de crear nuevos índices, buscar índices, leer y escribir documentos, eliminar documentos, administrar alias y mucho más. Administre estos permisos con la sección Permisos de índice al crear un rol. Para obtener una lista completa de los permisos de nivel de índice, consulte Permisos de índice.

En lugar de permisos individuales, a menudo puede alcanzar la posición de seguridad deseada mediante una combinación de los grupos de acciones predeterminadas. Para obtener una lista de grupos de acciones en el nivel del índice, consulte Nivel del índice.

Seguridad en el nivel del documento

La seguridad en el nivel del documento permite restringir los documentos de un índice que puede ver un usuario. Al crear un rol, especifique un patrón de índice y una OpenSearch consulta. Cualquier usuario que se mapee a ese rol únicamente podrá ver los documentos que coincidan con la consulta. La seguridad en el nivel del documento afecta al número de aciertos que se reciben al realizar una búsqueda.

Para obtener más información, consulte Seguridad en el nivel del documento.

Seguridad en el nivel del campo

La seguridad en el nivel del campo permite controlar qué campos de documento puede ver un usuario. Al crear un rol, agregue una lista de campos para incluirlos o excluirlos. Si incluye campos, los usuarios que mapee a ese rol solo podrán ver esos campos. Si excluye campos, podrán ver todos los campos excepto los excluidos. La seguridad en el nivel del campo afecta al número de campos que se incluyen en los aciertos al realizar una búsqueda.

Para obtener más información, consulte Seguridad en el nivel del campo.

Enmascarar campos

El enmascaramiento de campos es una alternativa a la seguridad en el nivel del campo que permite anonimizar los datos de un campo en lugar de eliminarlos por completo. Al crear un rol, agregue una lista de campos que se van a enmascarar. El enmascaramiento de campos afecta a si se podrá ver el contenido de un campo al realizar búsquedas.

> **Tip**
>
> Si aplica el enmascaramiento estándar a un campo, OpenSearch Service utiliza un hash aleatorio y seguro que puede provocar resultados de agregación imprecisos. Para realizar agregaciones en campos enmascarados, utilice el enmascaramiento con base en patrones en su lugar.

Crear usuarios

Si habilitó la base de datos de usuarios interna, puede crear usuarios mediante OpenSearch paneles o la `_plugins/_security` operación de la API REST. Para obtener más información, consulte Crear usuarios.

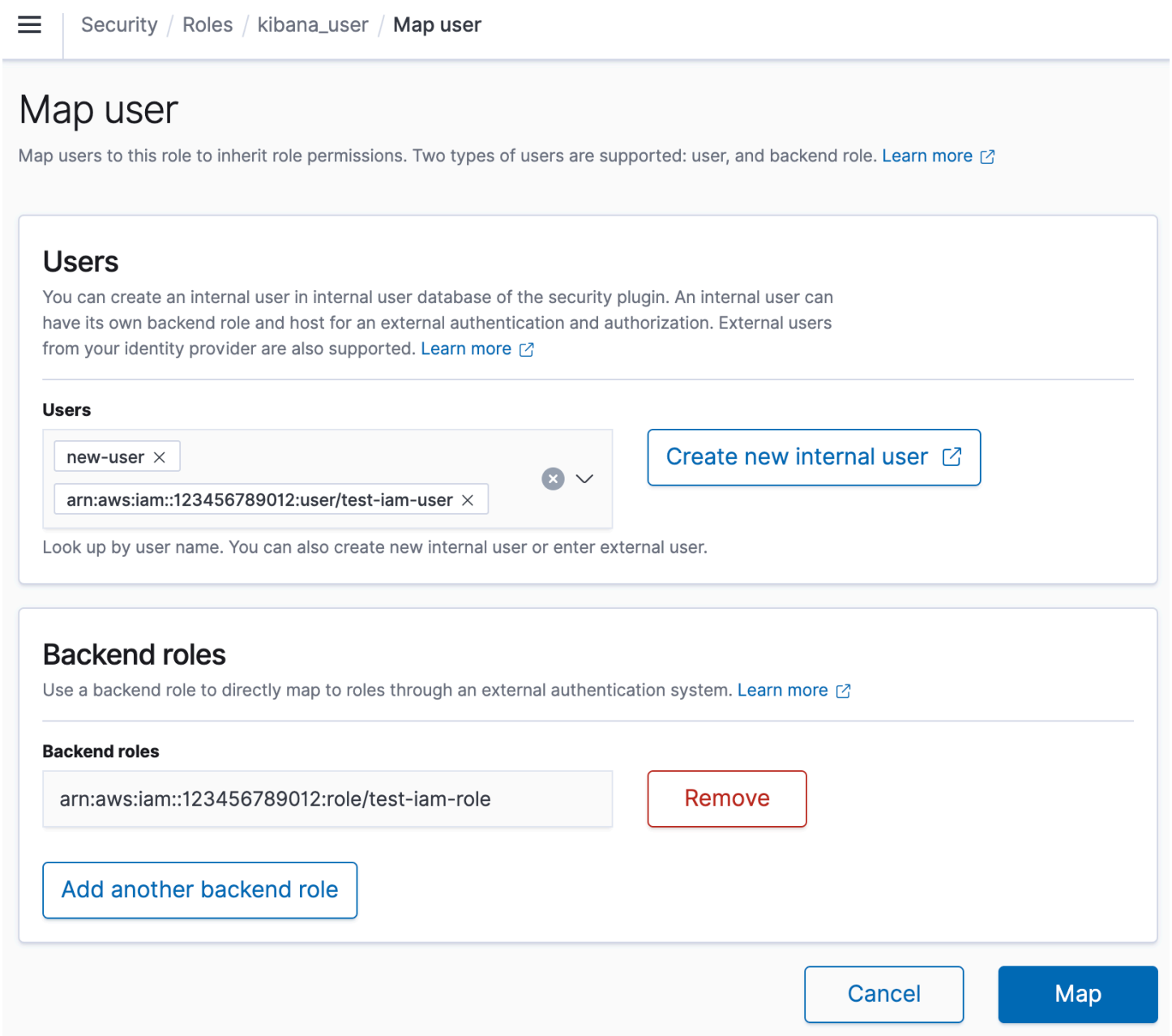
Si elige IAM para el usuario maestro, pase por alto esta parte de Dashboards. En su lugar, cree roles de IAM. Para obtener más información, consulte la Guía del usuario de IAM.

Mapear roles a usuarios

El mapeo de roles es el aspecto más crítico del control de acceso detallado. El control de acceso detallado tiene algunos roles predefinidos para ayudarlo a comenzar, pero a menos que mapee roles a los usuarios, cada solicitud al clúster dará lugar a un error de permisos.

Roles de backend pueden ayudar a simplificar el proceso de asignación de roles. En lugar de asignar el mismo rol a 100 usuarios individuales, puede asignar el rol a un único rol de backend que compartan los 100 usuarios. Los roles de backend pueden ser roles de IAM o cadenas arbitrarias.

- Especifique los usuarios, los ARN de usuario y las cadenas de usuario de Amazon Cognito en la sección Usuarios. Las cadenas de usuario de Cognito toman la forma de `Cognito/`*`user-pool-id`*`/`*`username`*.
- Especifique los roles de backend y los ARN de rol de IAM en la sección Roles de backend.



Puede asignar funciones a los usuarios mediante los OpenSearch paneles de control o la `_plugins/_security` operación en la API REST. Para obtener más información, consulte Mapear usuarios a roles.

Crear grupos de acciones

Los grupos de acciones son conjuntos de permisos que puede reutilizar en diferentes recursos. Puede crear nuevos grupos de acciones mediante OpenSearch paneles o la `_plugins/_security` operación de la API REST, aunque los grupos de acciones predeterminados son suficientes para

la mayoría de los casos de uso. Para obtener más información acerca de los grupos de acciones predeterminados, consulte Grupos de acciones predeterminados.

OpenSearch Tableros de mandos multiusuario

Los inquilinos son espacios para guardar patrones de índices, visualizaciones, paneles y otros objetos de Dashboards. El uso de varios inquilinos en Dashboards permite compartir el trabajo de forma segura con otros usuarios de Dashboards (o mantenerlo en privado) y configurar inquilinos de forma dinámica. Puede controlar qué roles tienen acceso a un inquilino y si esos roles tienen acceso de lectura o de escritura. El inquilino global es el predeterminado. Para obtener más información, consulte OpenSearch Dashboards sobre tenencia múltiple.

Para ver al inquilino actual o cambiar de inquilino

1. Ve a los OpenSearch paneles de control e inicia sesión.
2. Seleccione el icono de usuario en la parte superior derecha y elija Cambiar inquilinos.
3. Compruebe el inquilino antes de crear visualizaciones o paneles. Si desea compartir su trabajo con todos los demás usuarios de Dashboards, seleccione Global. Para compartir el trabajo con un subconjunto de usuarios de Dashboards, elija otro inquilino compartido. De lo contrario, seleccione Privado.

> **Note**
>
> OpenSearch Dashboards mantiene un índice independiente para cada inquilino y crea una plantilla de índice llamada. `tenant_template` No elimine ni modifique el `tenant_template` índice, ya que podría provocar un mal funcionamiento de los OpenSearch paneles si el mapeo del índice de inquilinos está mal configurado.

Configuraciones recomendadas

Debido a la forma en que el control de acceso detallado interactúa con otras características de seguridad, recomendamos varias configuraciones de control de acceso detallado que funcionan bien en la mayoría de los casos de uso.

Descripción	Usuario maestro	Política de acceso al dominio
Utilice las credenciales de IAM para las llamadas a OpenSearch las API y utilice la autenticación SAML para acceder a los paneles. Administr e los roles de control de acceso detallado mediante Dashboards o la API REST.	Rol o usuario de IAM	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`
Utilice las credenciales de IAM o la autenticación básica para las llamadas a las API. OpenSearc h Administre los roles de control de acceso detallado mediante Dashboards o la API REST. Esta configuración ofrece mucha flexibilidad, especialmente si tiene OpenSearch clientes que solo admiten la autentica ción básica. Si tiene un proveedor de identidad existente, utilice autenticación SAML para acceder a Dashboard	Nombre de usuario y contraseñ a	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Descripción	Usuario maestro	Política de acceso al dominio
s. En caso contrario, administre los usuarios de Dashboards en la base de datos de usuarios interna.		
Utilice las credenciales de IAM para las llamadas a las OpenSearch API y Amazon Cognito para acceder a los paneles. Administre los roles de control de acceso detallado mediante Dashboards o la API REST.	Rol o usuario de IAM	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "AWS": "*" }, "Action": "es:ESHttp*", "Resource": " domain-arn /*" } ] }`

Descripción	Usuario maestro	Política de acceso al dominio

Utilice las credenciales de IAM para las llamadas a las OpenSearch API y bloquee la mayoría de los accesos a los paneles. Administre los roles de control de acceso detallado mediante la API REST.	Rol o usuario de IAM	{
		"Version": "2012-10-17",
		"Statement": [
		{
		"Effect": "Allow",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /*"
		},
		{
		"Effect": "Deny",
		"Principal": {
		"AWS": "*"
		},
		"Action": "es:ESHttp*",
		"Resource": " *domain-arn* /_dashboards*"
		}
		]
		}

Limitaciones

El control de acceso detallado tiene varias limitaciones importantes:

- El aspecto `hosts` de los mapeos de roles, que mapea roles a nombres de anfitrión o direcciones IP, no funciona si el dominio está dentro de una VPC. Aun así, puede mapear roles a usuarios y roles de backend.
- Si elige IAM para el usuario maestro y no habilita la autenticación de Amazon Cognito o SAML, Dashboards muestra una página de inicio de sesión no funcional.
- Si elige IAM para el usuario maestro, podrá crear usuarios en la base de datos de usuarios interna. Sin embargo, debido a que la autenticación básica de HTTP no está habilitada en esta configuración, todas las solicitudes firmadas con esas credenciales de usuario se rechazarán.

- Si utiliza SQL para consultar un índice al que no tiene acceso, recibirá un error debido a que no tiene los permisos necesarios. Si el índice no existe, recibirá un error debido a que ese índice no existe. Esta diferencia en los mensajes de error significa que puede confirmar si un índice existe o no, en el caso de que trate de adivinar su nombre.

  Para minimizar el problema, no incluya información confidencial en los nombres de índice. Para denegar por completo el acceso a SQL, agregue el siguiente elemento a la política de acceso al dominio:

```
{
  "Effect": "Deny",
  "Principal": {
    "AWS": [
      "*"
    ]
  },
  "Action": [
    "es:*"
  ],
  "Resource": "arn:aws:es:us-east-1:123456789012:domain/my-domain/_plugins/_sql"
}
```

- Si la versión de su dominio es 2.3 o superior y tiene activado el control de acceso detallado, configurar `max_clause_count` en 1 provocará problemas con su dominio. Le recomendamos configurar esta cuenta con un número superior.
- Si está habilitando un control de acceso detallado en un dominio en el que no está configurado un control de acceso detallado, en el caso de las fuentes de datos creadas para consultas directas, tendrá que configurar usted mismo las funciones de control de acceso detalladas. Para obtener más información sobre cómo configurar funciones de acceso detalladas, consulte Creación de integraciones de fuentes de datos de Amazon OpenSearch Service con Amazon S3.

Modificar el usuario maestro

Si olvida los detalles del usuario maestro, puede reconfigurarlo mediante la consola, la AWS CLIo la API de configuración.

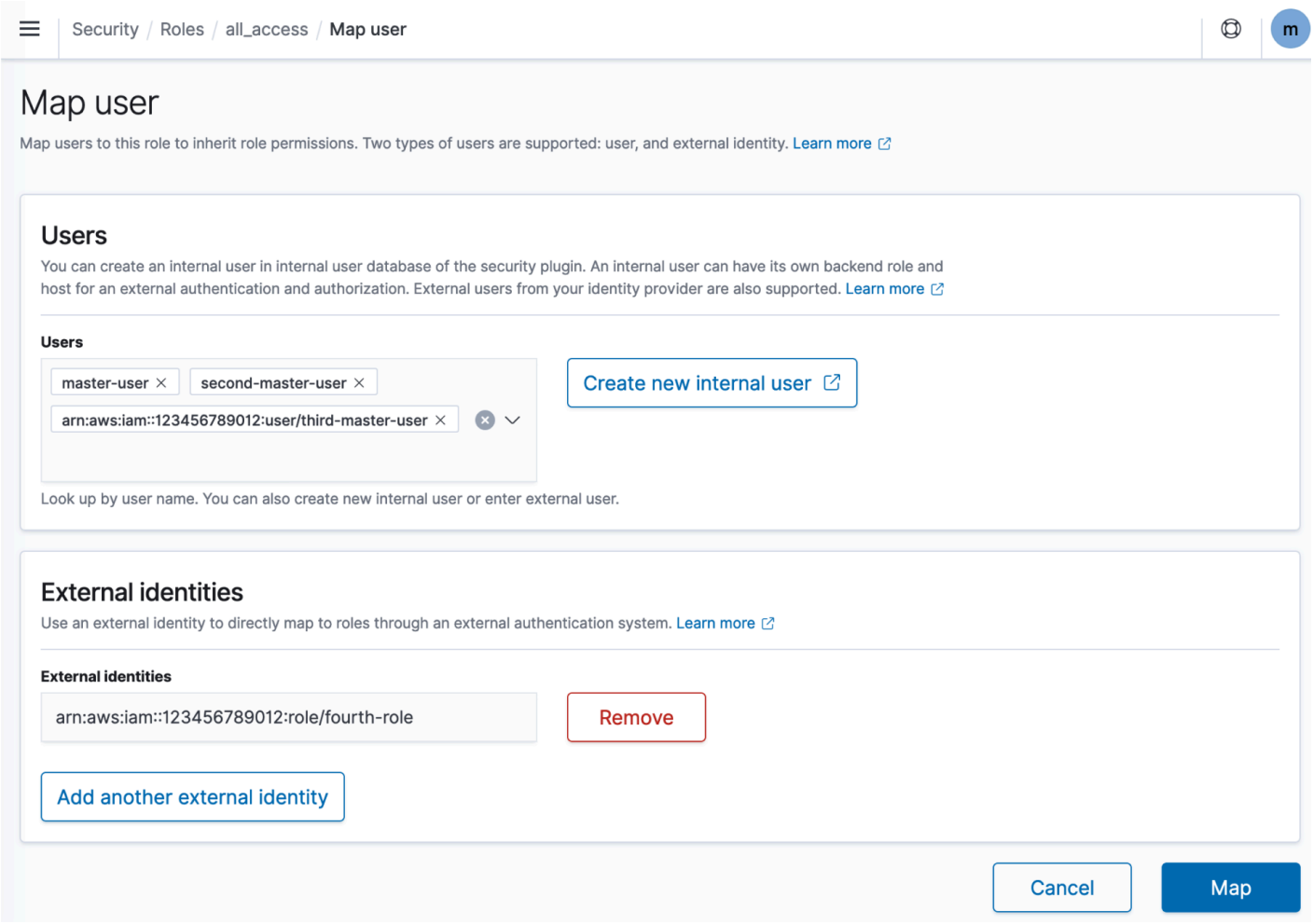
Para modificar el usuario maestro (consola)

1. Dirígete a la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/.
2. Seleccione el dominio y seleccione Acciones, Editar la configuración de seguridad.
3. Elika Establecer ARN de IAM como usuario maestro o bien Crear usuario maestro.
   - Si ha utilizado anteriormente un usuario maestro de IAM, el control de acceso detallado volverá a mapear el rol `all_access` al nuevo ARN de IAM que especifique.
   - Si ha utilizado previamente la base de datos de usuarios interna, el control de acceso detallado creará un usuario maestro. Puede utilizar el nuevo usuario maestro para eliminar el anterior.
   - Cambiar la base de datos de usuario interna a un usuario maestro de IAM no elimina ningún usuario de la base de datos de usuarios interna. En su lugar, simplemente desactiva la autenticación básica de HTTP. Elimine manualmente usuarios de la base de datos interna de usuarios o guárdelos en caso de que necesite volver a habilitar la autenticación básica de HTTP.
4. Seleccione Guardar cambios.

Usuarios maestros adicionales

Se designa un usuario maestro al crear un dominio. Sin embargo, si lo desea, puede utilizar este usuario maestro para crear usuarios maestros adicionales. Tienes dos opciones: OpenSearch paneles de control o la API REST.

- En Dashboards, seleccione Seguridad, Roles y, a continuación, mapee el nuevo usuario maestro a los roles `all_access` y `security_manager`.



- Para utilizar la API REST, envíe las siguientes solicitudes:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

```
PUT _plugins/_security/api/rolesmapping/security_manager
{
```

```
  "backend_roles": [
    "arn:aws:iam::123456789012:role/fourth-master-user"
  ],
  "hosts": [],
  "users": [
    "master-user",
    "second-master-user",
    "arn:aws:iam::123456789012:user/third-master-user"
  ]
}
```

Estas solicitudes reemplazan los mapeos de roles actuales. Por consiguiente, deber realizar las solicitudes `GET` primero para que pueda incluir todos los roles actuales en las solicitudes `PUT`. La API REST resulta especialmente útil si no puede obtener acceso a Dashboards y desea mapear un rol de IAM desde Amazon Cognito al rol `all_access`.

Instantáneas manuales

El control de acceso detallado presenta algunas complicaciones adicionales con la toma de instantáneas manuales. Para registrar un repositorio de instantáneas, aunque utilice la autenticación básica de HTTP para todos los demás fines, debe mapear el rol `manage_snapshots` a un rol de IAM que tenga permisos `iam:PassRole` para asumir `TheSnapshotRole`, tal como se define en the section called “Requisitos previos”.

A continuación, utilice ese rol de IAM para enviar una solicitud firmada al dominio, como se describe en the section called “Registrar un repositorio de instantáneas manuales”.

Integraciones

Si utiliza otros AWS servicios con el OpenSearch Servicio, debe proporcionar las funciones de IAM para esos servicios con los permisos adecuados. Por ejemplo, las transmisiones de entrega de Firehose suelen utilizar una función de IAM llamada. `firehose_delivery_role` En Dashboards, cree un rol para el control de acceso detallado y mapee el rol de IAM a ese rol. En este caso, el nuevo rol necesita los siguientes permisos:

```
{
  "cluster_permissions": [
    "cluster_composite_ops",
    "cluster_monitor"
```

```
  ],
  "index_permissions": [{
    "index_patterns": [
      "firehose-index*"
    ],
    "allowed_actions": [
      "create_index",
      "manage",
      "crud"
    ]
  }]
}
```

Los permisos varían en función de las acciones que realice cada servicio. Es probable que una AWS IoT regla o AWS Lambda función que indexe datos necesite permisos similares a los de Firehose, mientras que una función de Lambda que solo realiza búsquedas puede utilizar un conjunto más limitado.

Diferencias en la API REST

La API REST de control de acceso detallada varía ligeramente según la versión de /Elasticsearch. OpenSearch Antes de realizar una solicitud PUT, realice una solicitud GET para saber cómo es el cuerpo de la solicitud esperado. Por ejemplo, una solicitud GET para `_plugins/_security/api/user` devuelve todos los usuarios, que luego puede modificar y utilizar para realizar solicitudes PUT válidas.

En Elasticsearch 6.x, las solicitudes para crear usuarios tienen este aspecto:

```
PUT _opendistro/_security/api/user/new-user
{
  "password": "some-password",
  "roles": ["new-backend-role"]
}
```

En OpenSearch Elasticsearch 7.x, las solicitudes tienen este aspecto (cámbiese a si usa Elasticsearch): `_plugins` `_opendistro`

```
PUT _plugins/_security/api/user/new-user
{
  "password": "some-password",
  "backend_roles": ["new-backend-role"]
```

```
}
```

Además, los inquilinos son propiedades de los roles en Elasticsearch 6.x:

```
GET _opendistro/_security/api/roles/all_access

{
  "all_access": {
    "cluster": ["UNLIMITED"],
    "tenants": {
      "admin_tenant": "RW"
    },
    "indices": {
      "*": {
        "*": ["UNLIMITED"]
      }
    },
    "readonly": "true"
  }
}
```

En OpenSearch Elasticsearch 7.x, son objetos con su propio URI (cámbielo si usa Elasticsearch):: `_plugins` `_opendistro`

```
GET _plugins/_security/api/tenants

{
  "global_tenant": {
    "reserved": true,
    "hidden": false,
    "description": "Global tenant",
    "static": false
  }
}
```

Para obtener documentación sobre la API OpenSearch REST, consulta la referencia sobre la API del complemento de seguridad.

> **Tip**
>
> Si utiliza la base de datos de usuarios interna, puede utilizar curl para realizar solicitudes y probar el dominio. Pruebe los siguientes comandos de muestra:

```
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_search'
curl -XGET -u 'master-user:master-user-password' 'domain-endpoint/_plugins/
_security/api/user'
```

Tutorial: Configurar un dominio con un usuario maestro de IAM y la autenticación de Amazon Cognito

En este tutorial se describe un caso de uso popular de Amazon OpenSearch Service para un control de acceso detallado: un usuario maestro de IAM con autenticación de Amazon Cognito para paneles de control. OpenSearch

En el tutorial, configuraremos un rol de IAM maestro y un rol de IAM limitado, que luego asociaremos a los usuarios de Amazon Cognito. A continuación, el usuario maestro puede iniciar sesión en OpenSearch Dashboards, asignar al usuario limitado a un rol y usar un control de acceso detallado para limitar los permisos del usuario.

Aunque estos pasos utilizan el grupo de usuarios de Amazon Cognito para la autenticación, este mismo proceso básico funciona para cualquier proveedor de autenticación de Cognito que permita asignar diferentes roles de IAM a diferentes usuarios.

En este tutorial, deberá completar los siguientes pasos:

1. Crear roles de IAM maestros y limitados
2. Crear un dominio con la autenticación de Cognito
3. Configurar un grupo de usuarios y grupo de identidades de Cognito
4. Asigne funciones en los paneles OpenSearch
5. Evaluar los permisos

Paso 1: Crear roles de IAM maestros y limitados

Diríjase a la consola AWS Identity and Access Management (IAM) y cree dos funciones distintas:

- `MasterUserRole`: es el usuario maestro, que tiene permisos completos para el clúster y, además, administra los roles y las asignaciones de los roles.
- `LimitedUserRole`: es un rol más restringido, al que concederá acceso limitado como usuario maestro.

Para obtener instrucciones sobre cómo crear los roles, consulte Creación de un rol mediante políticas de confianza personalizadas.

Ambos roles deben tener la siguiente política de confianza, la cual permite que el grupo de identidades de Cognito asuma los roles:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Principal": {
      "Federated": "cognito-identity.amazonaws.com"
    },
    "Action": "sts:AssumeRoleWithWebIdentity",
    "Condition": {
      "StringEquals": {
        "cognito-identity.amazonaws.com:aud": "{identity-pool-id}"
      },
      "ForAnyValue:StringLike": {
        "cognito-identity.amazonaws.com:amr": "authenticated"
      }
    }
  }]
}
```

> **Note**
>
> Reemplace `identity-pool-id` por el identificador único de su grupo de identidades de Amazon Cognito. Por ejemplo, `us-east-1:0c6cdba7-3c3c-443b-a958-fb9feb207aa6`.

Paso 2: Crear un dominio con la autenticación de Cognito

Ve a la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/ y crea un dominio con los siguientes ajustes:

- OpenSearch 1.0 o posterior, o Elasticsearch 7.8 o posterior
- Acceso público
- Control de acceso detallado activado con `MasterUserRole` como el usuario maestro (creado en el paso anterior)
- Autenticación de Amazon Cognito habilitada para los paneles OpenSearch . Para obtener instrucciones sobre cómo habilitar la autenticación de Cognito y seleccionar un grupo de usuarios e identidades, consulte the section called “Configuración de un dominio para utilizar la autenticación de Amazon Cognito”.
- La siguiente política de acceso al dominio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:role/*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- Se requiere HTTPS para todo el tráfico al dominio
- Sin cifrado ode-to-node
- Cifrado de datos en reposo

Paso 3: configurar usuarios de Cognito

Mientras se crea su dominio, configure los usuarios maestros y limitados en Amazon Cognito siguiendo Crear un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito. Por último, configure su grupo de identidades siguiendo los pasos de Crear un grupo de identidades en Amazon Cognito. El grupo de usuarios y el grupo de identidades deben estar en la misma Región de AWS.

Paso 4: mapear las funciones en los OpenSearch paneles

Ahora que sus usuarios están configurados, puede iniciar sesión en OpenSearch Dashboards como usuario maestro y asignar los usuarios a los roles.

1. Vuelva a la consola OpenSearch de servicio y navegue hasta la URL de los OpenSearch paneles del dominio que creó. La URL tiene este formato: *domain-endpoint*`/_dashboards/`.
2. Inicie sesión con las credenciales de `master-user`.
3. Seleccione Agregar datos de muestra y agregue los datos de vuelos de muestra.
4. En el panel de navegación izquierdo, seleccione Seguridad, Roles, Crear rol.
5. Llame al rol `new-role`.
6. En Índice, especifique `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` en los dominios de Elasticsearch).
7. Para obtener Permisos de índice, seleccione leer.
8. Para Seguridad a nivel del documento, especifique la siguiente consulta:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

9. Para la seguridad a nivel del campo, seleccione Excluir y especifique `FlightNum`.
10. Para Anonimización, especifique `Dest`.
11. Seleccione Crear.
12. Seleccione Usuarios asignados, Administrar mapeo. A continuación, agregue el Nombre de recurso de Amazon (ARN) para `LimitedUserRole` como una identidad externa y elija Asignar.

13. Vuelva a la lista de roles y elija opensearch_dashboards_user. Seleccione Usuarios asignados, Administrar mapeo. Agregue el ARN para `LimitedUserRole` como un rol de backend y elija Mapear.

Paso 5: Probar los permisos

Cuando los roles están asignados de manera correcta, puede iniciar sesión como el usuario limitado y probar los permisos.

1. En una nueva ventana privada del navegador, navegue hasta la URL de OpenSearch Dashboards del dominio, inicie sesión con las `limited-user` credenciales y seleccione Explorar por mi cuenta.
2. Vaya a Herramientas para desarrolladores y ejecute la búsqueda predeterminada:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe el error de permisos. `limited-user` no tiene permisos para ejecutar búsquedas en todo el clúster.
3. Ejecute otra búsqueda:

   ```
   GET opensearch_dashboards_sample_data_flights/_search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Tenga en cuenta que todos los documentos coincidentes tienen un campo `FlightDelay` de `true`, un campo `Dest` anonimizado y ningún campo `FlightNum`.
4. En la ventana original del navegador, tras haber iniciado sesión como `master-user`, seleccione Herramientas para desarrolladores y, a continuación, realice las mismas búsquedas. Observe la diferencia en permisos, número de aciertos, documentos coincidentes y campos incluidos.

Tutorial: Configurar un dominio con la base de datos de usuarios interna y la autenticación básica de HTTP

En este tutorial se describe otro caso de uso muy detallado del control de acceso: un usuario maestro en la base de datos de usuarios interna y la autenticación básica mediante HTTP para los paneles. OpenSearch A continuación, el usuario maestro puede iniciar sesión en OpenSearch Dashboards, crear un usuario interno, asignar al usuario a un rol y usar un control de acceso detallado para limitar los permisos del usuario.

En este tutorial, deberá completar los siguientes pasos:

1. Cree un dominio con un usuario maestro
2. Configure un usuario interno en los paneles OpenSearch
3. Asigne funciones en los paneles OpenSearch
4. Evaluar los permisos

Paso 1: crear un dominio

Ve a la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/ y crea un dominio con los siguientes ajustes:

- OpenSearch 1.0 o posterior, o Elasticsearch 7.9 o posterior
- Acceso público
- Control de acceso detallado con un usuario maestro en la base de datos de usuarios interna (`TheMasterUser` en el resto de este tutorial)
- Autenticación de Amazon Cognito para Dashboards deshabilitada
- La siguiente política de acceso:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::{account-id}:user/*"
        ]
```

```
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:{region}:{account-id}:domain/{domain-name}/*"
    }
  ]
}
```

- Se requiere HTTPS para todo el tráfico al dominio
- Sin cifrado ode-to-node
- Cifrado de datos en reposo

Paso 2: Crear un usuario interno en los OpenSearch paneles

Ahora que tiene un dominio, puede iniciar sesión en OpenSearch Dashboards y crear un usuario interno.

1. Vuelva a la consola OpenSearch de servicio y navegue hasta la URL de los OpenSearch paneles del dominio que creó. La URL tiene este formato: *domain-endpoint*/_dashboards/.
2. Inicie sesión con el `TheMasterUser`.
3. Seleccione Agregar datos de muestra y agregue los datos de vuelos de muestra.
4. En el panel de navegación izquierdo, seleccione Seguridad, Usuarios internos y Crear usuario interno.
5. Llame al usuario `new-user` y especifique una contraseña. A continuación, seleccione Crear.

Paso 3: Asigne funciones en los paneles OpenSearch

Ahora que el usuario está configurado, puede asignarlo a un rol.

1. Permanezca en la sección Seguridad de los OpenSearch paneles de control y elija Roles y Crear rol.
2. Llame al rol `new-role`.
3. Para Índice, especifique `opensearch_dashboards_sample_data_fli*` (`kibana_sample_data_fli*` en dominios Elasticsearch) para el patrón de índice.
4. Para el grupo de acciones, seleccione leer.
5. Para Seguridad a nivel del documento, especifique la siguiente consulta:

```
{
  "match": {
    "FlightDelay": true
  }
}
```

6. Para la seguridad a nivel del campo, seleccione Excluir y especifique `FlightNum`.
7. Para Anonimización, especifique `Dest`.
8. Seleccione Crear.
9. Seleccione Usuarios asignados, Administrar mapeo. A continuación, agregue `new-user` a Usuarios y elija Mapear.
10. Vuelva a la lista de roles y elija opensearch_dashboards_user. Seleccione Usuarios asignados, Administrar mapeo. A continuación, agregue `new-user` a Usuarios y elija Mapear.

Paso 4: probar los permisos

Cuando los roles están asignados de manera correcta, puede iniciar sesión como el usuario limitado y probar los permisos.

1. En una nueva ventana privada del navegador, vaya a la URL de OpenSearch Dashboards del dominio, inicie sesión con las `new-user` credenciales y elija Explorar por mi cuenta.
2. Vaya a Herramientas para desarrolladores y ejecute la búsqueda predeterminada:

   ```
   GET _search
   {
     "query": {
       "match_all": {}
     }
   }
   ```

   Observe el error de permisos. `new-user` no tiene permisos para ejecutar búsquedas en todo el clúster.
3. Ejecute otra búsqueda:

   ```
   GET dashboards_sample_data_flights/_search
   {
     "query": {
   ```

```
    "match_all": {}
  }
}
```

Tenga en cuenta que todos los documentos coincidentes tienen un campo `FlightDelay` de `true`, un campo `Dest` anonimizado y ningún campo `FlightNum`.

4. En la ventana original del navegador, inicie sesión como `TheMasterUser`, seleccione Herramientas para desarrolladores y realice las mismas búsquedas. Observe la diferencia en permisos, número de aciertos, documentos coincidentes y campos incluidos.

Validación de conformidad para Amazon OpenSearch Service

Los auditores externos evalúan la seguridad y el cumplimiento de Amazon OpenSearch Service como parte de varios programas de AWS cumplimiento. Entre estos, se incluyen SOC, PCI e HIPAA.

Si tiene requisitos de conformidad, considere la posibilidad de utilizar cualquier versión de OpenSearch Elasticsearch 6.0 o posterior. Las versiones anteriores de Elasticsearch no ofrecen una combinación de cifrado de datos en reposo y node-to-node cifrado y es poco probable que satisfagan tus necesidades. También puedes considerar usar cualquier versión de Elasticsearch 6.7 OpenSearch o posterior si es importante tener un control de acceso detallado para tu caso de uso. En cualquier caso, elegir una versión concreta OpenSearch o de Elasticsearch al crear un dominio no garantiza la conformidad.

Para saber si uno Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte Servicios de AWS Alcance por programa de cumplimiento Servicios de AWS y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- Guías de inicio rápido sobre seguridad y cumplimiento: estas guías de implementación analizan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en AWS la seguridad y el cumplimiento.

- Diseño de arquitectura para garantizar la seguridad y el cumplimiento de la HIPAA en Amazon Web Services: en este documento técnico se describe cómo pueden utilizar AWS las empresas para crear aplicaciones aptas para la HIPAA.

  > **Note**
  >
  > No Servicios de AWS todas cumplen con los requisitos de la HIPAA. Para más información, consulte la Referencia de servicios compatibles con HIPAA.

- AWS Recursos de de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- AWS Guías de cumplimiento para clientes: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- Evaluación de los recursos con reglas en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la Referencia de controles de Security Hub.
- AWS Audit Manager— Esto le Servicio de AWS ayuda a auditar continuamente su AWS consumo para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

Resiliencia en Amazon OpenSearch Service

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS 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 tradicionales de centros de datos únicos o múltiples.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, OpenSearch Service ofrece varias características que lo ayudan con sus necesidades de resiliencia y copia de seguridad de los datos.

- Dominios Multi-AZ y fragmentos replicados
- Instantáneas automatizadas y manuales

Seguridad de la infraestructura en Amazon OpenSearch Service

Como servicio gestionado, Amazon OpenSearch Service está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte SeguridadAWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder al OpenSearch Servicio a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). 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.

Las llamadas a la API AWS publicadas se utilizan para acceder a la API OpenSearch de configuración del servicio a través de la red. A fin de configurar la versión mínima requerida de TLS para aceptar, especifique el valor `TLSSecurityPolicy` en las opciones de punto de conexión del dominio:

```
aws opensearch update-domain-config --domain-name my-domain --domain-endpoint-options
 '{"TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"}'
```

Para obtener más información, consulte la Referencia de comandos de laAWS CLI.

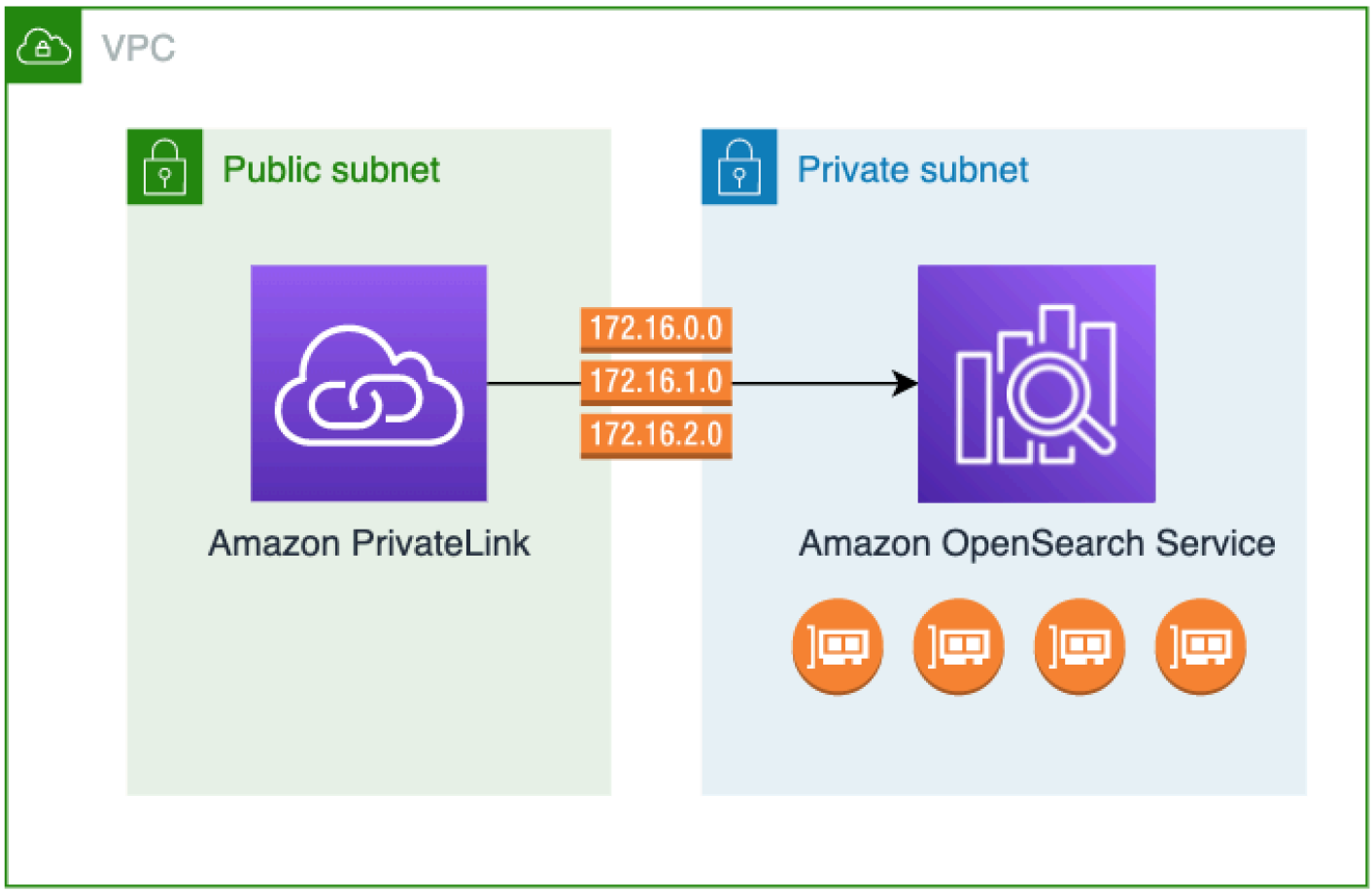
Dependiendo de su configuración de dominio, también podría ser necesario firmar solicitudes a las API de OpenSearch . Para obtener más información, consulte the section called “Realizar y firmar solicitudes de servicio OpenSearch ”.

OpenSearch El servicio admite dominios de acceso público, que pueden recibir solicitudes desde cualquier dispositivo conectado a Internet, y dominios de acceso de VPC, que están aislados de la Internet pública.

Acceda a Amazon OpenSearch Service mediante un punto de conexión de OpenSearch VPC gestionado por el servicio ()AWS PrivateLink

Para acceder a un dominio de Amazon OpenSearch Service, configura un punto final de OpenSearch VPC gestionado por el servicio (con tecnología de). AWS PrivateLinkEstos puntos de conexión crean una conexión privada entre tu VPC y Amazon OpenSearch Service. Puede acceder a los dominios de la VPC de OpenSearch servicio como si estuvieran en su VPC, sin utilizar una puerta de enlace a Internet, un dispositivo NAT, una conexión VPN o una conexión. AWS Direct Connect Las instancias de su VPC no necesitan direcciones IP públicas para acceder OpenSearch al Servicio.

Puede configurar los dominios de OpenSearch servicio para exponer puntos finales adicionales que se ejecuten en subredes públicas o privadas dentro de la misma VPC, una VPC diferente o diferente. Cuentas de AWSEsto le permite agregar una capa adicional de seguridad para acceder a sus dominios sin importar dónde se ejecuten, sin necesidad de administrar una infraestructura. En el siguiente diagrama, se muestran los puntos finales OpenSearch de VPC gestionados por el servicio dentro de la misma VPC:



Esta conexión privada se establece mediante la creación de un punto final de VPC OpenSearch de interfaz gestionada por el servicio, con tecnología de. AWS PrivateLinkCreamos una interfaz de red de punto de conexión en cada subred habilitada para el punto de conexión de VPC de interfaz. Se trata de interfaces de red administradas por el servicio que sirven como punto de entrada para el tráfico destinado al servicio. OpenSearch El precio estándarAWS PrivateLink de los puntos de conexión de interfaz se aplica a los puntos de enlace de OpenSearch VPC gestionados por el servicio facturados en virtud de. AWS PrivateLink

Puedes crear puntos de enlace de VPC para dominios que ejecuten todas las versiones de Elasticsearch OpenSearch y las versiones heredadas. Para obtener más información, consulte Acceso a Servicios de AWS a través de AWS PrivateLink en la Guía deAWS PrivateLink .

Consideraciones y limitaciones del servicio OpenSearch

Antes de configurar un punto final de VPC de interfaz para el OpenSearch servicio, consulte las consideraciones de laAWS PrivateLink guía.

Cuando utilice puntos finales de OpenSearch VPC gestionados por el servicio, tenga en cuenta lo siguiente:

- Solo puede utilizar puntos de conexión de VPC de interfaz para conectarse a los dominios de la VPC. Los dominios públicos no son compatibles.
- Los puntos de conexión de VPC solo pueden conectarse a dominios dentro de la misma Región de AWS.
- HTTPS es el único protocolo compatible para los puntos de conexión de VPC. No se permite el protocolo HTTP.
- OpenSearch El servicio permite realizar llamadas a todas las operaciones de OpenSearch API compatibles a través de un punto final de VPC de interfaz.
- Puede configurar un máximo de 50 puntos de conexión por cuenta y un máximo de 10 puntos de conexión por dominio. Un solo dominio puede tener un máximo de 10 entidades principales autorizadas.
- Actualmente no se pueden utilizar AWS CloudFormation para crear puntos finales de VPC de interfaz.
- Solo puede crear puntos finales de VPC de interfaz a través de la consola de OpenSearch servicio o mediante la OpenSearch API de servicio. No puede crear puntos de enlace de VPC de interfaz para el OpenSearch servicio mediante la consola de Amazon VPC.
- OpenSearch No se puede acceder a los puntos finales de VPC gestionados por el servicio desde Internet. Solo se puede acceder a un punto final de OpenSearch VPC administrado por el servicio dentro de la VPC en la que se aprovisiona el punto final o en cualquier VPC emparejada con la VPC en la que se aprovisiona el punto final, según lo permitan las tablas de enrutamiento y los grupos de seguridad.
- Las políticas de puntos finales de VPC no son compatibles con el servicio. OpenSearch Puede asociar un grupo de seguridad a las interfaces de red de los puntos finales para controlar el tráfico al OpenSearch Servicio a través del punto final de la VPC de la interfaz.
- Su función vinculada al servicio debe estar en la misma AWS cuenta que utilizó para crear el punto de enlace de la VPC.
- Para crear, actualizar y eliminar el punto de enlace de la VPC de OpenSearch servicio, debe tener los siguientes permisos de Amazon EC2 además de los permisos de Amazon OpenSearch Service:
  - `ec2:CreateVpcEndpoint`
  - `ec2:DescribeVpcEndpoints`

- `ec2:ModifyVpcEndpoint`
- `ec2:DeleteVpcEndpoints`
- `ec2:CreateTags`
- `ec2:DescribeTags`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`

> **Note**
>
> Actualmente, no puede limitar la creación de puntos finales de VPC al OpenSearch servicio. Estamos trabajando para que esto sea posible en una futura actualización.

Proporcionar el acceso a un dominio

Si la VPC a la que quieres acceder a tu dominio se encuentra en otro dominio Cuenta de AWS, debes autorizarla desde la cuenta del propietario antes de poder crear un punto final de VPC de interfaz.

Para permitir que una VPC de otra persona acceda Cuenta de AWS a tu dominio

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/.
2. En el panel de navegación, seleccione Dominios y abra el dominio al que desea proporcionar acceso.
3. Vaya a la pestaña Puntos de conexión de VPC, que muestra las cuentas y las VPC correspondientes que tienen acceso a su dominio.
4. Seleccione Autorizar entidad principal.
5. Introduce el Cuenta de AWS ID de la cuenta que accederá a tu dominio. Este paso autoriza a la cuenta especificada a crear puntos de conexión de VPC en el dominio.
6. Seleccione Autorizar.

Creación de un punto de conexión de VPC de interfaz para un dominio de VPC

Puede crear un punto final de VPC de interfaz para el OpenSearch servicio mediante la consola de OpenSearch servicio o el AWS Command Line Interface ()AWS CLI.

Para crear un punto final de VPC de interfaz para un dominio de servicio OpenSearch

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home/.
2. En el panel de navegación izquierdo, seleccione Puntos de conexión de VPC.
3. Seleccione Crear punto de conexión.
4. Seleccione si desea conectar un dominio del actual Cuenta de AWS o de otro Cuenta de AWS.
5. Seleccione el dominio al que se conecta con este punto de conexión. Si el dominio está en el actual Cuenta de AWS, usa el menú desplegable para elegir el dominio. Si el dominio se encuentra en otra cuenta, escriba el nombre de recurso de Amazon (ARN) del dominio para conectarse. Para elegir un dominio en una cuenta diferente, el propietario debe otorgarle acceso al dominio.
6. En el caso de la VPC, seleccione la VPC desde la que accederá al servicio. OpenSearch
7. En el caso de las subredes, seleccione una o más subredes desde las que accederá al Servicio. OpenSearch
8. En Grupos de seguridad, seleccione los grupos de seguridad que deban asociarse a las interfaces de red del punto de conexión. Este es un paso fundamental para limitar los puertos, los protocolos y los orígenes del tráfico entrante que autoriza para el punto de conexión. Las reglas del grupo de seguridad deben permitir que los recursos que utilizarán el punto final de la VPC para comunicarse con el OpenSearch Servicio se comuniquen con la interfaz de red del punto final.
9. Seleccione Crear punto de conexión. El punto de conexión debería estar activo en un plazo de 2 a 5 minutos.

Trabajar con puntos finales de OpenSearch VPC gestionados por el servicio mediante la API de configuración

Utilice las siguientes operaciones de API para crear y administrar puntos de enlace de OpenSearch VPC gestionados por el servicio.

- CreateVpcEndpoint

- ListVpcEndpoints
- UpdateVpcEndpoint
- DeleteVpcEndpoint

Utilice las siguientes operaciones de la API para administrar el acceso de los puntos de conexión a los dominios de la VPC:

- AuthorizeVpcEndpointAccess
- ListVpcEndpointAccess
- ListVpcEndpointsForDomain
- RevokeVpcEndpointAccess

Autenticación SAML para paneles OpenSearch

La autenticación SAML para OpenSearch Dashboards te permite usar tu proveedor de identidad actual para ofrecer el inicio de sesión único (SSO) para los Dashboards de los dominios de Amazon OpenSearch Service que ejecuten OpenSearch Elasticsearch 6.7 o versiones posteriores. Para utilizar la autenticación SAML, debe habilitar el control de acceso detallado.

En lugar de autenticarse a través de Amazon Cognito o la base de datos de usuarios interna, la autenticación SAML OpenSearch para los paneles le permite utilizar proveedores de identidad de terceros para iniciar sesión en los paneles, administrar un control de acceso detallado, buscar sus datos y crear visualizaciones. OpenSearch El servicio es compatible con los proveedores que utilizan el estándar SAML 2.0, como Okta, Keycloak, Active Directory Federation Services (ADFS), Auth0 y. AWS IAM Identity Center

La autenticación SAML para los paneles solo sirve para acceder a los paneles a través de un navegador web. OpenSearch Sus credenciales de SAML no le permiten realizar solicitudes HTTP directas a las API ni a las API de Dashboards. OpenSearch

Información general de la configuración de SAML

En esta documentación se supone que tiene un proveedor de identidad existente y que está familiarizado con él en cierta medida. No podemos proporcionar pasos de configuración detallados para su proveedor exacto, solo para su dominio de OpenSearch servicio.

El flujo de inicio de sesión en OpenSearch Dashboards puede adoptar una de estas dos formas:

- Proveedor de servicios (SP) iniciado: navegue al panel (por ejemplo, `https://my-domain.us-east-1.es.amazonaws.com/_dashboards`), que lo redirige a la pantalla de inicio de sesión. Después de iniciar sesión, el proveedor de identidades lo redirige al panel.
- Iniciado por el proveedor de identidad (IdP): navega hasta su proveedor de identidad, inicia sesión y elige OpenSearch Dashboards en un directorio de aplicaciones.

OpenSearch El servicio proporciona dos URL de inicio de sesión único, iniciadas por SP e iniciadas por IdP, pero solo necesita la que coincida con el flujo de inicio de sesión deseado en Dashboards. OpenSearch

Independientemente del tipo de autenticación que utilice, el objetivo es iniciar sesión a través de su proveedor de identidades y recibir una aserción SAML que contenga su nombre de usuario (requerido) y cualquier rol backend (opcional, pero recomendado). Esta información permite el control de acceso detallado para asignar permisos a usuarios de SAML. En los proveedores de identidad externos, los roles backend se denominan generalmente “roles” o “grupos”.

Consideraciones

Tenga en cuenta lo siguiente cuando configure la autenticación SAML:

- Debido al tamaño del archivo de metadatos del proveedor de identidades, se recomienda encarecidamente utilizar la consola de AWS para configurar la autenticación SAML.
- Los dominios solo admiten un método de autenticación del panel a la vez. Si tiene habilitada la autenticación de Amazon Cognito para OpenSearch paneles, debe deshabilitarla antes de poder habilitar la autenticación SAML.
- Si utiliza un equilibrador de carga de red con SAML, primero debe crear un punto de conexión personalizado. Para obtener más información, consulte ???.

Autenticación SAML para dominios de VPC

SAML no requiere comunicación directa entre el proveedor de identidades y el proveedor de servicios. Por lo tanto, aunque tu OpenSearch dominio esté alojado en una VPC privada, puedes seguir usando SAML siempre que tu navegador pueda comunicarse con tu OpenSearch clúster y tu proveedor de identidad. En esencia, el navegador actúa como intermediario entre el proveedor de identidades y el proveedor de servicios. Para ver un útil diagrama que explica el flujo de autenticación SAML, consulte la documentación de Okta.

Modificación de la política de acceso al dominio

Antes de configurar la autenticación SAML, debe actualizar la política de acceso al dominio para permitir a los usuarios de SAML acceder al dominio. De lo contrario, aparecerán errores de acceso denegado.

Recomendamos la siguiente política de acceso al dominio, que proporciona acceso completo a los subrecursos (`/*`) en el dominio:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESHttp*",
      "Resource": "domain-arn/*"
    }
  ]
}
```

Para hacer que la política sea más restrictiva, puedes añadir una condición de dirección IP a la política. Esta condición limita el acceso únicamente a la subred o rango de direcciones IP especificados. Por ejemplo, la siguiente política permite el acceso únicamente desde la subred 192.0.2.0/24:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Condition": {
        "IpAddress": {
```

```
          "aws:SourceIp": [
            "192.0.2.0/24"
          ]
        }
      },
      "Resource": "domain-arn/*"
    }
  ]
}
```

> **Note**
>
> Una política de acceso a un dominio abierto requiere que se habilite un control de acceso detallado en tu dominio; de lo contrario, aparece el siguiente error: `To protect domains with public access, a restrictive policy or fine-grained access control is required.` Si tienes un usuario maestro o un usuario interno configurado con una contraseña segura, mantener la política abierta mientras utilizas un control de acceso detallado podría ser aceptable desde el punto de vista de la seguridad. Para obtener más información, consulte ???.

Configuración de la autenticación iniciada por proveedor de servicios o por proveedor de identidades

En estos pasos se explica cómo habilitar la autenticación SAML con la autenticación iniciada por el SP o por el IdP para los paneles de control. OpenSearch Para conocer el paso adicional necesario para habilitar ambas, consulte Configuración de la autenticación iniciada por proveedor de servicios o por proveedor de identidades.

Paso 1: habilitar la autenticación SAML

Puede habilitar la autenticación SAML bien durante la creación del dominio o bien seleccionando Acciones, Editar la configuración de seguridad en un dominio existente. Los siguientes pasos varían ligeramente según lo que seleccione.

En la configuración del dominio, en Autenticación SAML para OpenSearch Dashboards/Kibana, selecciona Habilitar la autenticación SAML.

Paso 2: configurar el proveedor de identidades

Ejecute los siguientes pasos en función del momento de configuración de la autenticación SAML.

Si va a crear un nuevo dominio

Si estás creando un dominio nuevo, el servicio aún no puede generar un ID de entidad del proveedor de OpenSearch servicios ni una URL de inicio de sesión único. El proveedor de identidades requiere estos valores para habilitar correctamente la autenticación SAML, pero solo se pueden generar después de crear el dominio. Para evitar esta interdependencia durante la creación del dominio, puede proporcionar valores temporales en la configuración del IdP con el fin de generar los metadatos necesarios, y luego actualizarlos una vez que el dominio esté activo.

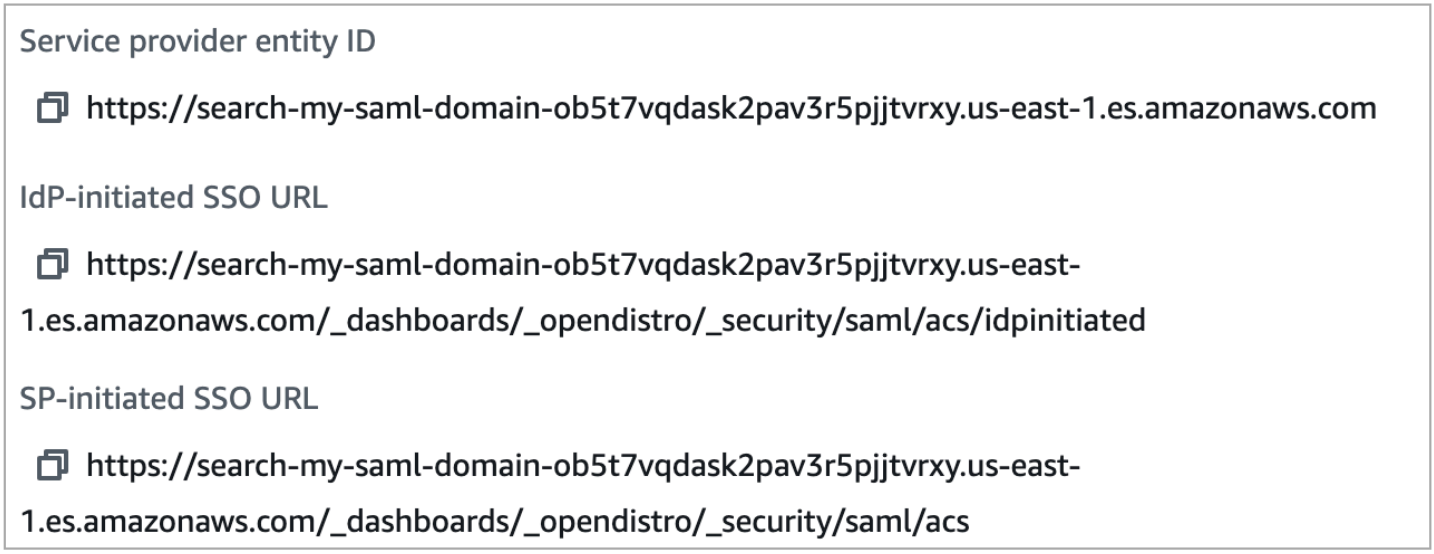
Si utiliza un punto de conexión personalizado, puede inferir cuáles serán las URL. Por ejemplo, si el punto de conexión personalizado es `www.custom-endpoint.com`, el ID de entidad del proveedor de servicios será`www.custom-endpoint.com`, la URL de SSO iniciado por IdP será `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs/idpinitiated`, y la URL de SSO iniciado por SP será `www.custom-endpoint.com/_dashboards/_opendistro/_security/saml/acs`. Puede utilizar los valores para configurar el proveedor de identidades antes de crear el dominio. Consulte la siguiente sección para ver ejemplos.

Si no utiliza un punto de conexión personalizado, puede introducir valores temporales en el IdP para generar los metadatos necesarios, y luego actualizarlos una vez que el dominio esté activo.

Por ejemplo, en Okta puede introducir `https://temp-endpoint.amazonaws.com` en los campos URL de inicio de sesión único y URI de audiencia (ID de entidad del SP), lo que permite generar los metadatos. A continuación, una vez que el dominio esté activo, podrás recuperar los valores correctos de OpenSearch Service y actualizarlos en Okta. Para ver instrucciones, consulte the section called “Paso 6: Actualizar las URL del IdP”.

Si va a editar un dominio existente

Si va habilitar la autenticación SAML en un dominio existente, copie el ID de entidad del proveedor de servicios y una de las URL de SSO. Para obtener orientación sobre qué URL debe utilizar, consulte the section called “Información general de la configuración de SAML”.



Utilice los valores para configurar el proveedor de identidades. Esta es la parte más compleja del proceso, y, desafortunadamente, la terminología y los pasos varían enormemente según el proveedor. Consulte la documentación de su proveedor.

En Okta, por ejemplo, crea una aplicación web SAML 2.0. En URL de inicio de sesión único, especifique la URL de SSO. Para URI de audiencia (ID de identidad del SP), especifique el ID de entidad del SP.

En lugar de usuarios y roles de backend, Okta tiene usuarios y grupos. En Instrucciones de atributo de grupo, se recomienda agregar `role` al campo Nombre y la expresión regular `.+` al campo Filtro. Esta instrucción indica al proveedor de identidades de Okta que incluya todos los grupos de usuarios bajo el campo `role` de la aserción SAML después de que un usuario se autentica.

En el Centro de identidades de IAM, especifique el ID de la entidad del SP como la audiencia de SAML de la aplicación. También debe especificar las siguientes asignaciones de atributos: `Subject=${user:name}` y `Role=${user:groups}`.

En Auth0, crea una aplicación web regular y habilita el complemento SAML 2.0. En Keycloak, crea un cliente.

Paso 3: Importar metadatos del IdP

Después de configurar el proveedor de identidades, genera un archivo de metadatos de IdP. Este archivo XML contiene información sobre el proveedor, como un certificado TLS, puntos de conexión de inicio de sesión único y el ID de entidad del proveedor de identidad.

Copie el contenido del archivo de metadatos del IdP y péguelo en el campo Metadatos del IdP de la consola de servicio. OpenSearch Alternativamente, seleccione Importar desde archivo XML y cargue el archivo. El archivo de metadatos debe tener un aspecto similar al siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor entityID="entity-id"
 xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="false"
 protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>tls-certificate</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</
md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
 Location="idp-sso-url"/>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="idp-sso-url"/>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Paso 4: configurar los campos SAML

Después de introducir los metadatos del IdP, configure los siguientes campos adicionales en la consola de OpenSearch servicio:

- ID de entidad del IdP: copie el valor de la propiedad `entityID` del archivo de metadatos y péguelo en este campo. Muchos proveedores de identidades también muestran este valor como parte de un resumen posterior a la configuración. Algunos proveedores lo llaman el “emisor”.
- Nombre de usuario maestro de SAML y función de backend principal de SAML: el usuario o la función de backend que especifique reciben todos los permisos para el clúster, lo que equivale a un nuevo usuario maestro, pero solo pueden usar esos permisos en los paneles. OpenSearch

  Por ejemplo, en Okta, es posible que tenga un usuario `jdoe` que pertenece al grupo `admins`. Si agrega `jdoe` al nombre de usuario maestro de SAML, solo ese usuario recibe permisos

completos. Si agrega `admins` Rol de backend maestro de SAML, cualquier usuario que pertenezca al grupo `admins` recibe permisos completos.

> **Note**
>
> El contenido de la aserción SAML debe coincidir exactamente con las cadenas que se utilicen para el nombre de usuario maestro de SAML y el rol maestro de SAML. Algunos proveedores de identidad añaden un prefijo antes de sus nombres de usuario, lo que puede provocar que no coincidan. hard-to-diagnose En la interfaz de usuario del proveedor de identidades, es posible que vea `jdoe`, pero la aserción SAML podría contener `auth0|jdoe`. Utilice siempre la cadena de la aserción SAML.

Muchos proveedores de identidades permiten ver una aserción de muestra durante el proceso de configuración, y herramientas como Rastreo SAML pueden ayudarlo a examinar y solucionar problemas del contenido de las aserciones reales. Las aserciones se ven algo similar a lo siguiente:

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2:Assertion ID="id67229299299259351343340162"
 IssueInstant="2020-09-22T22:03:08.633Z" Version="2.0"
  xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">idp-issuer</
saml2:Issuer>
  <saml2:Subject>
    <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">username</saml2:NameID>
    <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml2:SubjectConfirmationData NotOnOrAfter="2020-09-22T22:08:08.816Z"
 Recipient="domain-endpoint/_dashboards/_opendistro/_security/saml/acs"/>
    </saml2:SubjectConfirmation>
  </saml2:Subject>
  <saml2:Conditions NotBefore="2020-09-22T21:58:08.816Z"
 NotOnOrAfter="2020-09-22T22:08:08.816Z">
    <saml2:AudienceRestriction>
      <saml2:Audience>domain-endpoint</saml2:Audience>
    </saml2:AudienceRestriction>
  </saml2:Conditions>
  <saml2:AuthnStatement AuthnInstant="2020-09-22T19:54:37.274Z">
    <saml2:AuthnContext>
```

```
 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport<
saml2:AuthnContextClassRef>
    </saml2:AuthnContext>
  </saml2:AuthnStatement>
  <saml2:AttributeStatement>
    <saml2:Attribute Name="role" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:unspecified">
      <saml2:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="xs:string">GroupName Match Matches regex ".+" (case-sensitive)
      </saml2:AttributeValue>
    </saml2:Attribute>
  </saml2:AttributeStatement>
</saml2:Assertion>
```

Paso 5: (opcional) configurar ajustes adicionales

En Configuración adicional, configure los siguientes campos opcionales:

- Clave de asunto: puede dejar este campo vacío con el fin de utilizar el elemento `NameID` de la aserción SAML para el nombre de usuario. Si su aserción no utiliza este elemento estándar y, en su lugar, incluye el nombre de usuario como un atributo personalizado, especifique ese atributo aquí.
- Clave de roles: si desea utilizar roles de backend (se recomienda), especifique un atributo de la aserción en este campo; por ejemplo, `role` o `group`. Esta es otra situación en la que herramientas como Rastreo SAML pueden ayudar.
- Duración de la sesión: de forma predeterminada, OpenSearch Dashboards cierra la sesión de los usuarios después de 24 horas. Puede establecer este valor en cualquier número comprendido entre 60 y 1440 (24 horas) especificando un nuevo valor.

Cuando la configuración le parezca adecuada, guarde el dominio.

Paso 6: Actualizar las URL del IdP

Si ha habilitado la autenticación SAML mientras creaba un dominio, habrá tenido que especificar URL temporales para el IdP con el fin de generar el archivo de metadatos XML. Cuando el estado del dominio cambia a `Active`, puede obtener las URL correctas y modificar el IdP.

Para recuperar las URL, seleccione el dominio, y luego Acciones y Editar la configuración de seguridad. En la sección Autenticación SAML para OpenSearch Dashboards/Kibana, puedes encontrar el ID de entidad del proveedor de servicios y las URL de SSO correctos. Copie los valores y utilícelos para configurar el proveedor de identidades, sustituyendo las URL temporales que proporcionó en el paso 2.

Paso 7: Asignar usuarios de SAML a roles

Una vez que el estado de su dominio sea Activo y su IDP esté configurado correctamente, navegue hasta los OpenSearch paneles.

- Si eligió la dirección URL iniciada por el SP, diríjase a *domain-endpoint*`/_dashboards`. Para iniciar sesión directamente en un inquilino específico, puede agregar `?security_tenant=`*tenant-name* a la URL.
- Si eligió la dirección URL iniciada por el IdP, diríjase al directorio de aplicaciones de su proveedor de identidad.

En ambos casos, inicie sesión como usuario maestro SAML o como usuario que pertenece al rol de backend maestro SAML. Para continuar con el ejemplo del paso 7, inicie sesión como `jdoe` o un miembro del grupo `admins`.

Cuando se OpenSearch carguen los paneles, selecciona Seguridad, Funciones. A continuación, asigne los roles para permitir que otros usuarios accedan a los OpenSearch paneles.

Por ejemplo, podría asignar a su colega de confianza `jroe` a los roles `all_access` y `security_manager`. También puede asignar el rol de backend `analysts` a los roles `readall` y `opensearch_dashboards_user`.

Si prefiere usar la API en lugar de los OpenSearch paneles, consulte el siguiente ejemplo de solicitud:

```
PATCH _plugins/_security/api/rolesmapping
[
  {
    "op": "add", "path": "/security_manager", "value": { "users": ["master-user",
 "jdoe", "jroe"], "backend_roles": ["admins"] }
  },
  {
    "op": "add", "path": "/all_access", "value": { "users": ["master-user", "jdoe",
 "jroe"], "backend_roles": ["admins"] }
```

```
  },
  {
    "op": "add", "path": "/readall", "value": { "backend_roles": ["analysts"] }
  },
  {
    "op": "add", "path": "/opensearch_dashboards_user", "value": { "backend_roles":
 ["analysts"] }
  }
]
```

Configuración de la autenticación iniciada por proveedor de servicios y por proveedor de identidades

Si desea configurar la autenticación iniciada por SP e IdP, debe hacerlo a través de su proveedor de identidades. Por ejemplo, en Okta, puede seguir estos pasos:

1. Dentro de su aplicación SAML, vaya a General, Configuración SAML.
2. Para la URL de inicio de sesión único, proporcione URL SSO iniciado por IdP. Por ejemplo, `https://search-`*`domain-hash`*`/_dashboards/_opendistro/_security/saml/acs/`*`idpinitiated`*.
3. Habilite Permitir que esta aplicación solicite otras URL de SSO.
4. En Direcciones URL de SSO que se pueden solicitar, agregue una o varias URL de SSO iniciadas por SP. Por ejemplo, `https://search-`*`domain-hash`*`/_dashboards/_opendistro/_security/saml/`*`acs`*.

Configuración de la autenticación SAML (AWS CLI)

El siguiente AWS CLI comando habilita la autenticación SAML para los OpenSearch paneles de control de un dominio existente:

```
aws opensearch update-domain-config \
  --domain-name my-domain \
  --advanced-security-options '{"SAMLOptions":{"Enabled":true,"MasterUserName":"my-
idp-user","MasterBackendRole":"my-idp-group-or-role","Idp":{"EntityId":"entity-
id","MetadataContent":"metadata-content-with-quotes-escaped"},"RolesKey":"optional-
roles-key","SessionTimeoutMinutes":180,"SubjectKey":"optional-subject-key"}}'
```

Debe escapar de todas las comillas y caracteres de nueva línea en el XML de metadatos. Por ejemplo, utilice `<KeyDescriptor use=\"signing\">\n` en lugar de `<KeyDescriptor use="signing">` y un salto de línea. Para obtener información detallada sobre el uso de AWS CLI, consulte la Referencia de AWS CLI comandos.

Configuración de la autenticación SAML (API de configuración)

La siguiente solicitud a la API de configuración habilita la autenticación SAML para los OpenSearch paneles de control de un dominio existente:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/domain/my-domain/config
{
  "AdvancedSecurityOptions": {
    "SAMLOptions": {
      "Enabled": true,
      "MasterUserName": "my-idp-user",
      "MasterBackendRole": "my-idp-group-or-role",
      "Idp": {
        "EntityId": "entity-id",
        "MetadataContent": "metadata-content-with-quotes-escaped"
      },
      "RolesKey": "optional-roles-key",
      "SessionTimeoutMinutes": 180,
      "SubjectKey": "optional-subject-key"
    }
  }
}
```

Debe escapar de todas las comillas y caracteres de nueva línea en el XML de metadatos. Por ejemplo, utilice `<KeyDescriptor use=\"signing\">\n` en lugar de `<KeyDescriptor use="signing">` y un salto de línea. Para obtener información detallada sobre el uso de la API de configuración, consulta la referencia de la API OpenSearch de servicio.

Solución de problemas de SAML

Error	Detalles
Your request: "*/some/path* " is not allowed (Su solicitud, "/some/path", no está permitida).	Compruebe que ha proporcionado la dirección URL de SSO correcta (paso 3) a su proveedor de identidad .

Error	Detalles
Proporcione un documento de metadatos del proveedor de identidad válido para habilitar SAML.	El archivo de metadatos del IdP no cumple con el estándar SAML 2.0. Verifique si hay errores mediante una herramienta de validación.
Las opciones de configuración de SAML no son visibles en la consola.	Actualice a la versión más reciente del software de servicio.
Error de configuración de SAML: se produjo un error al recuperar la configuración de SAML. Verifique su configuración.	Este error genérico puede producirse por muchas razones. • Compruebe que ha proporcionado a su proveedor de identidad el ID de entidad del SP y la dirección URL de SSO correctos. • Vuelva a generar el archivo de metadatos del IdP y verifique el ID de entidad de IdP. Agregue todos los metadatos actualizados en la consola de AWS . • Compruebe que la política de acceso a su dominio permita el acceso a los OpenSearch paneles y `_plugins/_security/*` . En general, recomendamos una política de acceso abierto para dominios que utilicen un control de acceso detallado. • Consulte la documentación de su proveedor de identidades a fin de conocer los pasos necesarios para configurar SAML.

Error	Detalles
Rol faltante: no hay roles disponibles para este usuario. Póngase en contacto con el administrador del sistema.	Se ha autenticado correctamente, pero el nombre de usuario y los roles de backend de la aserción SAML no se asignan a ningún rol y, por lo tanto, no tienen permisos. Estos mapeos distinguen entre mayúsculas y minúsculas. El administrador del sistema puede verificar el contenido de su afirmación de SAML mediante una herramienta como SAML-Tracer y, a continuación, comprobar la asignación de funciones mediante la siguiente solicitud: `GET _plugins/_security/api/rolesmapping`
Su navegador redirige o recibe continuamente errores HTTP 500 al intentar acceder a los paneles. OpenSearch	Estos errores pueden producirse si la aserción SAML contiene un gran número de roles con un total aproximado de 1500 caracteres. Por ejemplo, si transfiere 80 roles, cuya longitud media es de 20 caracteres, es posible que supere el límite de tamaño de las cookies en su navegador web. A partir de OpenSearch la versión 2.7, la aserción SAML admite funciones de hasta 5000 caracteres.
No puede cerrar sesión en ADFS.	ADFS requiere que todas las solicitudes de cierre de sesión estén firmadas, algo que el OpenSearch servicio no admite. Elimine `<SingleLogoutService />` del archivo de metadatos del IdP para obligar al OpenSearch Servicio a utilizar su propio mecanismo de cierre de sesión interno.

Error	Detalles
`Could not find entity descriptor for __PATH__.`	El ID de entidad del IdP proporcionado en el XML de metadatos al OpenSearch servicio es diferente al de la respuesta de SAML. Para ello, asegúrese de que coincidan. Active los registros de errores de aplicacio nes de CW en su dominio para encontrar el mensaje de error y depurar el problema de integración con SAML.
`Signature validation failed. SAML response rejected.`	OpenSearch El servicio no puede verificar la firma de la respuesta de SAML mediante el certificado del IdP proporcionado en el XML de metadatos. Puede deberse a un error manual o a que su IdP haya rotado su certificado. Actualice el certificado más reciente de su IdP en el XML de metadatos proporcionado al OpenSearch Servicio a través del. AWS Management Console
`__PATH__ is not a valid audience for this response.`	El campo de audiencia de la respuesta de SAML no coincide con el punto de conexión del dominio. Para corregir este error, actualice el campo de audiencia del SP para que coincida con el punto de conexión de su dominio. Si ha activado los puntos de conexión personalizados, el campo de audiencia debe coincidir con su punto de conexión personalizado. Active los registros de errores de aplicaciones de CW en su dominio para encontrar el mensaje de error y depurar el problema de integración con SAML.
Su navegador recibe un mensaje de error HTTP 400 con `Invalid Request Id` en la respuesta.	Este error suele producirse si ha configurado la URL iniciada por el IdP con este formato *<DashboardsURL>* `/_opendistro/_security/saml/acs`. En su lugar, configure la URL con el formato *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated` .

Error	Detalles
La respuesta se recibió en `__PATH__` en vez de `__PATH__`.	El campo de destino de la respuesta SAML no coincide con ninguno de los siguientes formatos de URL: • *<DashboardsURL>* `/_opendistro/_security/saml/acs` • *<DashboardsURL>* `/_opendistro/_security/saml/acs/idpinitiated` . Según el flujo de inicio de sesión que utilice (iniciado por SP o iniciado por IdP), introduzca un campo de destino que coincida con una de las URL. OpenSearch
La respuesta tiene un atributo `InResponseTo` , pero no se esperaba `InResponseTo` .	Está utilizando la URL iniciada por IdP para un flujo de inicio de sesión iniciado por SP. En su lugar, utilice la URL iniciada por SP.

Deshabilitar la autenticación SAML

Para deshabilitar la autenticación SAML en los paneles de control (consola) OpenSearch

1. Seleccione el dominio, Acciones y Editar la configuración de seguridad.
2. Desmarque Habilitar la autenticación SAML.
3. Seleccione Guardar cambios.
4. Después de que el dominio termine de procesar, compruebe el mapeo de roles de control de acceso detallado con la siguiente solicitud:

   ```
   GET _plugins/_security/api/rolesmapping
   ```

   Deshabilitar la autenticación SAML para Dashboards no elimina los mapeos del nombre de usuario maestro SAML o del rol de backend maestro SAML. Si desea eliminar estos mapeos, inicie sesión en Dashboards con la base de datos de usuario interna (si está habilitada) o utilice la API para eliminarlos:

```
PUT _plugins/_security/api/rolesmapping/all_access
{
  "users": [
    "master-user"
  ]
}
```

Configuración de la autenticación de Amazon Cognito para OpenSearch Dashboards

Puede autenticar y proteger la instalación predeterminada de Amazon OpenSearch Service para OpenSearch Dashboards mediante Amazon Cognito. La autenticación de Amazon Cognito es opcional y solo está disponible para dominios que utilicen OpenSearch o Elasticsearch 5.1 o una versión posterior. Si no configura la autenticación de Amazon Cognito, puede seguir protegiendo Dashboards con una política de acceso basada en IP y un servidor proxy, una autenticación básica de HTTP o SAML.

Gran parte del proceso de autenticación se produce en Amazon Cognito, pero esta sección ofrece instrucciones y requisitos para configurar los recursos de Amazon Cognito para trabajar con dominios de OpenSearch Service. Se aplican precios estándar a todos los recursos de Amazon Cognito.

> **Tip**
>
> Recomendamos utilizar la consola la primera vez que configure un dominio para utilizar la autenticación de Amazon Cognito para OpenSeach Dashboards. Los recursos de Amazon Cognito se pueden personalizar en gran medida y la consola puede ayudar a identificar y comprender las funciones importantes.

Temas

- (Opcional) Personalización de la página de inicio de sesión
- (Opcional) Configuración de seguridad avanzada
- Pruebas
- Cuotas
- Problemas habituales de configuración
- Deshabilitar la autenticación de Amazon Cognito para OpenSearch Dashboards
- Eliminación de dominios que utilizan la autenticación de Amazon Cognito para OpenSearch Dashboards

Requisitos previos

Antes de poder configurar la autenticación de Amazon Cognito para OpenSearch Dashboards, debe cumplir varios requisitos previos. La consola de OpenSearch Service ayuda a simplificar la creación de estos recursos, pero comprender la finalidad de cada recurso ayuda a la hora de configurar y resolver problemas. La autenticación de Amazon Cognito para Dashboards requiere los siguientes recursos:

- Grupo de usuarios de Amazon Cognito
- Grupo de identidades de Amazon Cognito
- Rol de IAM que tiene la política de `AmazonOpenSearchServiceCognitoAccess` adjunta (`CognitoAccessForAmazonOpenSearch`)

> **Note**
>
> El grupo de usuarios y el grupo de identidades deben estar en la misma Región de AWS. Puede utilizar el mismo grupo de usuarios, el mismo grupo de identidades y el mismo rol de IAM para agregar la autenticación de Amazon Cognito para Dashboards a varios dominios de OpenSearch Service. Para obtener más información, consulte the section called “Cuotas”.

Acerca del grupo de usuarios

Los grupos de usuarios tiene dos características principales: crear y administrar un directorio de usuarios y permitir que los usuarios se inscriban e inicien sesión. Para obtener instrucciones acerca

de cómo crear un grupo de usuarios, consulte Creación de un grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

Al crear un grupo de usuarios que se va a utilizar con OpenSearch Service, tenga en cuenta lo siguiente:

- El grupo de usuarios de Amazon Cognito debe tener un nombre de dominio. OpenSearch Service utiliza este nombre de dominio para redirigir a los usuarios a una página de inicio de sesión para acceder a Dashboards. Aparte de un nombre de dominio, el grupo de usuarios no requiere ninguna configuración no predeterminada.
- Debe especificar los atributos estándar necesarios del grupo como nombre, fecha de nacimiento, dirección de email y número de teléfono. No se pueden cambiar estos atributos después de crear el grupo de usuarios, por lo que debe elegir los que considere importantes en este momento.
- Al crear el grupo de usuarios, elija si los usuarios pueden crear sus propias cuentas, el nivel mínimo de seguridad de la contraseña para las cuentas y si se va a habilitar la autenticación multifactor. Si tiene previsto utilizar un proveedor de identidades externo, estos ajustes no tienen importancia. Técnicamente puede habilitar el grupo de usuarios como un proveedor de identidades y habilitar un proveedor de identidades externo, pero la mayoría de las personas prefieren uno u otro.

Los ID de grupos de usuarios adoptan la forma de *region*_*ID*. Si tiene previsto utilizar la CLI de AWS o un SDK de AWS para configurar OpenSearch Service, anote el ID.

Acerca del grupo de identidades

Los grupos de identidades permiten asignar funciones temporales con privilegios limitados a los usuarios después de que inicien sesión. Para obtener instrucciones sobre la creación de un grupo de identidades, consulte Grupos de usuarios en la Guía para desarrolladores de Amazon Cognito. Al crear un grupo de identidades que se va a utilizar con OpenSearch Service, tenga en cuenta lo siguiente:

- Si utiliza la consola de Amazon Cognito, debe seleccionar la casilla de verificación Habilitar el acceso a identidades sin autenticar para crear el grupo de identidades. Después de crear el grupo de identidades y de configurar el dominio de OpenSearch Service, Amazon Cognito deshabilita esta configuración.

- No es necesario agregar proveedores de identidades externos al grupo de identidades. Cuando se configura OpenSearch Service para utilizar la autenticación de Amazon Cognito, configura el grupo de identidades para utilizar el grupo de usuarios que acaba de crear.
- Después de crear el grupo de identidades, debe elegir funciones de IAM autenticadas y sin autenticar. Estos roles especifican las políticas de acceso que los usuarios tienen antes y después de que inicien sesión. Si utiliza la consola de Amazon Cognito, puede crear estas funciones para usted. Una vez creado el rol autenticado, anote el ARN, que adopta la forma de `arn:aws:iam::`*`123456789012`*`:role/Cognito_`*`identitypoolname`*`Auth_Role`.

Los ID de grupos de identidades adoptan la forma de *`region`*`:`*`ID`*`-`*`ID`*`-`*`ID`*`-`*`ID`*`-`*`ID`*. Si tiene previsto utilizar la CLI de AWS o un SDK de AWS para configurar OpenSearch Service, anote el ID.

Acerca del rol CognitoAccessForAmazonOpenSearch

OpenSearch Service necesita permisos para configurar los grupos de usuarios y de identidades de Amazon Cognito y utilizarlos para la autenticación. Para esto, puede utilizar `AmazonOpenSearchServiceCognitoAccess`, que es una política administrada por AWS. `AmazonESCognitoAccess` es una política heredada que fue reemplazada por `AmazonOpenSearchServiceCognitoAccess` cuando el servicio fue renombrado a Amazon OpenSearch Service. Ambas políticas proporcionan los permisos mínimos de Amazon Cognito necesarios para habilitar la autenticación de Cognito. Para ver la política JSON, consulte la consola de IAM.

Si utiliza la consola para crear o configurar el dominio de OpenSearch Service, se crea un rol de IAM para usted y se adjunta a dicho rol la política `AmazonOpenSearchServiceCognitoAccess` (o la política `AmazonESCognitoAccess` si es un dominio de Elasticsearch). El nombre predeterminado del rol es `CognitoAccessForAmazonOpenSearch`.

Las políticas de permisos de rol `AmazonOpenSearchServiceCognitoAccess` y `AmazonESCognitoAccess` permiten a OpenSearch Service completar las siguientes acciones en todos los grupos de identidades y usuarios:

- Acción: `cognito-idp:DescribeUserPool`
- Acción: `cognito-idp:CreateUserPoolClient`
- Acción: `cognito-idp:DeleteUserPoolClient`
- Acción: `cognito-idp:UpdateUserPoolClient`
- Acción: `cognito-idp:DescribeUserPoolClient`

- Acción: `cognito-idp:AdminInitiateAuth`
- Acción: `cognito-idp:AdminUserGlobalSignOut`
- Acción: `cognito-idp:ListUserPoolClients`
- Acción: `cognito-identity:DescribeIdentityPool`
- Acción: `cognito-identity:SetIdentityPoolRoles`
- Acción: `cognito-identity:GetIdentityPoolRoles`

Si utiliza la AWS CLI o uno de los SDK de AWS, debe crear un rol propio, adjuntar la política y especificar el ARN para este rol al configurar el dominio de OpenSearch Service. El rol debe tener la siguiente relación de confianza:

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

Para obtener instrucciones, consulte Creación de un rol para delegar permisos a un servicio de AWS y Adjuntar y desconectar políticas de IAM en la Guía del usuario de IAM.

Configuración de un dominio para utilizar la autenticación de Amazon Cognito

Después de completar los requisitos previos, puede configurar un dominio de OpenSearch Service para que utilice Amazon Cognito para Dashboards.

> **Note**
>
> Amazon Cognito no está disponible en todas las Regiones de AWS. Para consultar una lista de las regiones y los puntos de enlace compatibles, visite Regiones de AWS y puntos

de enlace. No es necesario utilizar la misma región para Amazon Cognito que utiliza para OpenSearch Service.

Configuración de la autenticación de Amazon Cognito (consola)

La consola ofrece la experiencia de configuración más sencilla, ya que crea automáticamente el rol CognitoAccessForAmazonOpenSearch. Además de los permisos de OpenSearch Service estándar, se necesita el siguiente conjunto de permisos para utilizar la consola con el fin de crear un dominio que emplee la autenticación de Amazon Cognito para OpenSearch Dashboards.

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools",
        "iam:CreateRole",
        "iam:AttachRolePolicy"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Para obtener instrucciones sobre cómo agregar permisos a una identidad (usuario, grupo de usuarios o rol), consulteAdición de permisos de identidad de IAM (consola).

Si el `CognitoAccessForAmazonOpenSearch` ya existe, necesita menos permisos:

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "cognito-identity:ListIdentityPools",
        "cognito-idp:ListUserPools"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/service-
role/CognitoAccessForAmazonOpenSearch"
    }
  ]
}
```

Para configurar la autenticación de Amazon Cognito para Dashboards (consola)

1. Abra la consola de Amazon OpenSearch Service enhttps://console.aws.amazon.com/aos/home/.
2. En Dominios, seleccione el dominio que desea configurar.
3. Elija Acciones y Editar la configuración de seguridad.
4. Elija Habilitar la autenticación de Amazon Cognito.
5. En Región, seleccione la Región de AWS que contiene el grupo de usuarios y de identidades de Amazon Cognito.
6. En Grupo de usuarios de Cognito, seleccione un grupo de usuarios o cree uno. Para obtener instrucciones, consulte the section called “Acerca del grupo de usuarios”.
7. En Grupo de identidades de Cognito, seleccione un grupo de identidades o cree uno. Para obtener instrucciones, consulte the section called “Acerca del grupo de identidades”.

> **Note**
>
> Los enlaces Crear grupo de usuarios y Crear grupo de identidades dirigen a la consola de Amazon Cognito y requieren crear estos recursos de forma manual. El proceso no

es automático. Para obtener más información, consulte the section called “Requisitos previos”.

8. Para INombre de rol de IAM, utilice el valor de `CognitoAccessForAmazonOpenSearch` predeterminado (recomendado) o ingrese un nombre nuevo. Para obtener más información acerca de la finalidad de este rol, consulte the section called “Acerca del rol CognitoAccessForAmazonOpenSearch”.
9. Elija Guardar cambios.

Después de que el dominio termine de procesarse, consulte the section called “Permitir el rol autenticado” y the section called “Configuración de proveedores de identidades” para conocer los pasos adicionales de configuración.

Configuración de la autenticación de Amazon Cognito (AWS CLI)

Utilice el parámetro `--cognito-options` para configurar el dominio de OpenSearch Service. Los comandos `create-domain` y `update-domain-config` emplean la siguiente sintaxis:

```
--cognito-options Enabled=true,UserPoolId="user-pool-id",IdentityPoolId="identity-pool-id",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Ejemplo

En el siguiente ejemplo se crea un dominio en la región `us-east-1` que habilita la autenticación de Amazon Cognito para Dashboards mediante el rol `CognitoAccessForAmazonOpenSearch` y proporciona acceso al dominio a `Cognito_Auth_Role`:

```
aws opensearch create-domain --domain-name my-domain --region us-east-1 --access-policies '{ "Version":"2012-10-17", "Statement":[{"Effect":"Allow","Principal":{"AWS":
 ["arn:aws:iam::123456789012:role/Cognito_Auth_Role"]},"Action":"es:ESHttp*","Resource":"arn:aws:es:us-east-1:123456789012:domain/*" }]}' --engine-version "OpenSearch_1.0"
 --cluster-config InstanceType=m4.xlarge.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeSize=10 --cognito-options
 Enabled=true,UserPoolId="us-east-1_123456789",IdentityPoolId="us-east-1:12345678-1234-1234-1234-123456789012",RoleArn="arn:aws:iam::123456789012:role/CognitoAccessForAmazonOpenSearch"
```

Después de que el dominio termine de procesarse, consulte the section called “Permitir el rol autenticado” y the section called “Configuración de proveedores de identidades” para conocer los pasos adicionales de configuración.

Configuración de la autenticación de Amazon Cognito (SDK de AWS)

Los AWS SDK (excepto los SDK de Android e iOS) admiten todas las operaciones definidas en la referencia de API de Amazon OpenSearch Service, incluido el parámetro `CognitoOptions` para las operaciones `CreateDomain` y `UpdateDomainConfig`. Para obtener más información acerca de cómo instalar y utilizar los SDK de AWS, consulte los Kits de desarrollo de software de AWS.

Después de que el dominio termine de procesarse, consulte the section called “Permitir el rol autenticado” y the section called “Configuración de proveedores de identidades” para conocer los pasos adicionales de configuración.

Permitir el rol autenticado

De forma predeterminada, el rol de IAM autenticado que configuró de acuerdo con las instrucciones de the section called “Acerca del grupo de identidades” no cuenta con los privilegios necesarios para obtener acceso a OpenSearch Dashboards. Debe proporcionar permisos adicionales al rol.

> **Note**
>
> Si configuró el control de acceso detallado y utiliza una política de acceso abierta o basada en IP, puede omitir este paso.

Puede incluir estos permisos en una política basada en identidades, pero, a menos que quiera que los usuarios autenticados obtengan acceso a todos los dominios de OpenSearch Service, el mejor enfoque es una política basada en recursos adjunta a un solo dominio.

Para el `Principal`, especifique el ARN del rol autenticado de Cognito que configuró con las pautas que figuran en the section called “Acerca del grupo de identidades”.

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

```
            "AWS":[
               "arn:aws:iam::123456789012:role/Cognito_identitypoolnameAuth_Role"
            ]
         },
         "Action":[
            "es:ESHttp*"
         ],
         "Resource":"arn:aws:es:region:123456789012:domain/domain-name/*"
      }
   ]
}
```

Para obtener instrucciones sobre cómo agregar una política basada en recursos a un dominio de OpenSearch Service, consulte the section called “Configurar políticas de acceso”.

Configuración de proveedores de identidades

Al configurar un dominio para que utilice la autenticación de Amazon Cognito para Dashboards, OpenSearch Service agrega un cliente de aplicación al grupo de usuarios y agrega el grupo de usuarios al grupo de identidades como proveedor de autenticación.

> **Warning**
>
> No cambie el nombre ni elimine el cliente de aplicación.

En función de cómo configure el grupo de usuarios, puede que necesite crear cuentas de usuarios de forma manual, o bien los usuarios podrían crear sus propias cuentas. Si estos ajustes son aceptables, no es necesario realizar más acciones. Sin embargo, muchas personas prefieren usar proveedores de identidades externos.

Para habilitar un proveedor de identidades SAML 2.0, debe proporcionar un documento de metadatos de SAML. Para habilitar proveedores de identidades sociales como Login with Amazon, Facebook y Google, debe disponer de un ID de aplicación y de la clave secreta de la aplicación de esos proveedores. Puede habilitar cualquier combinación de proveedores de identidades.

La forma más sencilla de configurar el grupo de usuarios consiste en utilizar la consola de Amazon Cognito. Para obtener instrucciones, consulte Utilización de la federación desde un grupo de usuarios y Especificación de la configuración del proveedor de identidad para la aplicación de grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

(Opcional) Configuración de acceso pormenorizado

Es posible que haya observado que la configuración del grupo de identidades predeterminado asigna el mismo rol de IAM (`Cognito_identitypoolAuth_Role`) a cada usuario que inicia sesión, lo cual significa que todos los usuarios pueden obtener acceso a los mismos recursos de AWS. Si desea utilizar el control de acceso detallado con Amazon Cognito, por ejemplo, si desea que los analistas de la organización tengan acceso de solo lectura a varios índices, pero que los desarrolladores tengan acceso de escritura a todos los índices, tiene dos opciones:

- Cree grupos de usuarios y configure su proveedor de identidades de tal forma que elija el rol de IAM en función del token de autenticación del usuario (recomendado).
- Configure su proveedor de identidades para que elija el rol de IAM en función de una o varias reglas.

Para obtener un tutorial que incluya el control de acceso detallado, consulte the section called "Tutorial: Control de acceso detallado con la autenticación de Cognito".

> **Important**
>
> Al igual que sucede con el rol predeterminado, Amazon Cognito debe formar parte de la relación de confianza de cada rol adicional. Para obtener más información, consulte Creación de roles para el mapeo de roles en la Guía para desarrolladores de Amazon Cognito.

Grupos de usuarios y tokens

Al crear un grupo de usuarios, elige un rol de IAM para los miembros del grupo. Para obtener información sobre cómo crear grupos, consulte Grupos de usuarios en la Guía para desarrolladores de Amazon Cognito.

Después de crear uno o más grupos de usuarios, puede configurar su proveedor de autenticación para asignar a los usuarios las funciones de sus grupos en lugar del rol predeterminado del grupo de identidades. Seleccione Elegir rol a partir de un token, luego elija Utilizar rol autenticado predeterminado o DENEGAR para especificar de qué manera el grupo de identidades se encargará de los usuarios que no forman parte del grupo.

Reglas

Las reglas son básicamente una serie de instrucciones `if` que Amazon Cognito evalúa de forma secuencial. Por ejemplo, si una dirección de email del usuario contiene `@corporate`, Amazon Cognito asigna `Role_A` a ese usuario. Si la dirección de correo electrónico de un usuario contiene `@subsidiary`, asigna a ese usuario `Role_B`. De lo contrario, asigna al usuario el rol autenticado predeterminado.

Para obtener más información, consulte Utilización del mapeo basado en reglas para la asignación de roles a los usuarios en la Guía para desarrolladores de Amazon Cognito.

(Opcional) Personalización de la página de inicio de sesión

Puede usar la consola de Amazon Cognito para cargar un logotipo personalizado y realizar cambios de CSS en la página de inicio de sesión. Para obtener instrucciones y una lista completa de propiedades CSS, consulte Especificación de la configuración de personalización de la interfaz de usuario de la aplicación para el grupo de usuarios en la Guía para desarrolladores de Amazon Cognito.

(Opcional) Configuración de seguridad avanzada

Los grupos de usuarios de Amazon Cognito admiten características de seguridad avanzadas como la autenticación multifactor, la verificación de credenciales comprometidas y la autenticación flexible. Para obtener más información, consulte Administración de seguridad en la Guía para desarrolladores de Amazon Cognito.

Pruebas

Una vez que esté satisfecho con la configuración, verifique que la experiencia del usuario cumpla sus expectativas.

Para acceder a OpenSearch Dashboards

1. Vaya a `https://`*`opensearch-domain`*`/_dashboards` en un navegador Web. Para iniciar sesión directamente en un inquilino específico, agregue `?security_tenant=`*`tenant-name`* a la URL.
2. Inicie sesión con las credenciales que prefiera.

3. Una vez que se carga OpenSearch Dashboards, configure al menos un patrón de índice. Dashboards utiliza estos patrones para identificar los índices que desea analizar. Escriba `*`, elija Siguiente paso y, a continuación, elija Crear patrón de índice.
4. Para buscar datos o explorar en ellos, elija Detección.

Si cualquier paso de este proceso da error, consulte the section called “Problemas habituales de configuración” para obtener información sobre resolución de problemas.

Cuotas

Amazon Cognito cuenta con límites flexibles en muchos de los recursos. Si desea habilitar la autenticación de Dashboards para una gran cantidad de dominios de OpenSearch Service, consulte Cuotas en Amazon Cognito y solicite un aumento de los límites si es necesario.

Cada dominio de OpenSearch Service agrega un cliente de aplicación al grupo de usuarios, lo cual agrega un proveedor de autenticación al grupo de identidades. Si habilita la autenticación de OpenSearch Dashboards para más de 10 dominios, puede que llegue al límite de “máximo de proveedores de grupo de usuarios de Amazon Cognito por grupo de identidades”. Si supera un límite, cualquier dominio de OpenSearch Service que intente configurar para que utilice la autenticación de Amazon Cognito para Dashboards puede bloquearse en un estado de configuración o En proceso.

Problemas habituales de configuración

En las tablas siguientes se muestran los problemas habituales de configuración y las soluciones.

Configuración de OpenSearch Service

Problema	Solución
`OpenSearch Service can't create the role` (consola)	No dispone de los permisos de IAM correctos. Añada los permisos especificados en the section called “Configuración de la autenticación de Amazon Cognito (consola)”.
`User is not authorized to perform: iam:PassRole on resource CognitoAccessForAmazonOpenSearch` (consola)	No cuenta con permisos `iam:PassRole` para el rol CognitoAccessForAmazonOpenSearch. Asocie la siguiente política a su cuenta: `{`

Problema	Solución
	"Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["iam:PassRole"], "Resource": "arn:aws:iam:: *123456789012:role/service-role/CognitoAccessForAmazonOpenSearch* " }] } Como alternativa, puede adjuntar la política `IAMFullAccess` .
`User is not authorized to perform: cognito-identity:ListIdentityPools on resource`	No tiene permisos de lectura para Amazon Cognito. Adjunte la política `AmazonCognitoReadOnly` a su cuenta.
`An error occurred (ValidationException) when calling the CreateDomain operation: OpenSearch Service must be allowed to use the passed role`	OpenSearch Service no se especifica en la relación de confianza del rol `CognitoAccessForAmazonOpenSearch` . Verifique si el rol utiliza la relación de confianza que se especifica en the section called “Acerca del rol CognitoAccessForAmazonOpenSearch”. De manera alternativa, utilice la consola para configurar la autenticación de Amazon Cognito. La consola crea un rol para usted.

Problema	Solución
`An error occurred (ValidationException) when calling the CreateDomain operation: User is not authorized to perform: cognito-idp: action on resource: user pool`	El rol especificado en `--cognito-options` no cuenta con permisos para acceder a Amazon Cognito. Verifique que el rol tenga adjunta la política administrada AWS de `AmazonOpenSearchServiceCognitoAccess`. De manera alternativa, utilice la consola para configurar la autenticación de Amazon Cognito. La consola crea un rol para usted.
`An error occurred (ValidationException) when calling the CreateDomain operation: User pool does not exist`	OpenSearch Service no encuentra el grupo de usuarios. Verifique que creó uno y que tiene el ID correcto. Para encontrar el ID, puede utilizar la consola de Amazon Cognito o el siguiente comando de la AWS CLI: `aws cognito-idp list-user-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation: IdentityPool not found`	OpenSearch Service no encuentra el grupo de identidades. Verifique que creó uno y que tiene el ID correcto. Para encontrar el ID, puede utilizar la consola de Amazon Cognito o el siguiente comando de la AWS CLI: `aws cognito-identity list-identity-pools --max-results 60 --region region`
`An error occurred (ValidationException) when calling the CreateDomain operation: Domain needs to be specified for user pool`	El grupo de usuarios no tiene un nombre de dominio. Puede configurar uno con la consola de Amazon Cognito o el siguiente comando de la AWS CLI: `aws cognito-idp create-user-pool-domain --domain name --user-pool-id id`

Acceso a OpenSearch Dashboards

Problema	Solución
La página de inicio de sesión no muestra mis proveedores de identidades preferidos.	Verifique que habilitó el proveedor de identidades del cliente de la aplicación de OpenSearch Service tal y como se especifica en the section called “Configuración de proveedores de identidades”.
La página de inicio de sesión no parece estar asociada a mi organización.	Consulte the section called “(Opcional) Personalización de la página de inicio de sesión”.
Mis credenciales de inicio de sesión no funcionan.	Verifique que configuró el proveedor de identidades tal y como se especifica en the section called “Configuración de proveedores de identidades”. Si utiliza el grupo de usuarios como proveedor de identidades, verifique que la cuenta exista en la consola de Amazon Cognito.
OpenSearch Dashboards no se carga en absoluto o no funciona correctamente.	El rol autenticado de Amazon Cognito necesita permisos `es:ESHttp*` para el dominio (`/*`) a fin de obtener acceso y utilizar Dashboards. Verifique que agregó una política de acceso tal y como se especifica en the section called “Permitir el rol autenticado”.
Cuando cierro sesión en OpenSearch Dashboard desde una pestaña, las pestañas restantes muestran un mensaje que indica que se ha revocado el token de actualización.	Al cerrar sesión en una sesión de OpenSearch Dashboards con la autenticación de Amazon Cognito, OpenSearch Service ejecuta la operación AdminUserGlobalSignOut, que cierra sesión en todas las sesiones activas de OpenSearch Dashboards.
`Invalid identity pool configuration. Check assigned IAM roles for this pool.`	Amazon Cognito no cuenta con permisos para asumir el rol de IAM en nombre del usuario autenticado. Modifique la relación de confianza para el rol de tal forma que incluya: `{`

Problema	Solución

	"Version": "2012-10-17",
	"Statement": [{
	"Effect": "Allow",
	"Principal": {
	"Federated": "cognito-identity.amazonaws.com"
	},
	"Action": "sts:AssumeRoleWithWebIdentity",
	"Condition": {
	"StringEquals": {
	"cognito-identity.amazonaws.com:aud": " *identity-pool-id* "
	},
	"ForAnyValue:StringLike": {
	"cognito-identity.amazonaws.com:amr": "authenticated"
	}
	}
	}]
	}

`Token is not from a supported provider of this identity pool.`	Este error poco habitual se puede producir al eliminar el cliente de aplicación del grupo de usuarios. Intente abrir Dashboards en una nueva sesión del navegador.

Deshabilitar la autenticación de Amazon Cognito para OpenSearch Dashboards

Utilice el siguiente procedimiento para deshabilitar la autenticación de Amazon Cognito para Dashboards.

Para deshabilitar la autenticación de Amazon Cognito para Dashboards (consola)

1. Abra la consola de Amazon OpenSearch Service enhttps://console.aws.amazon.com/aos/home/.
2. En Dominios, elija el dominio que desea configurar.
3. Elija Acciones y Editar la configuración de seguridad.

4. Desactive Habilitar la autenticación de Amazon Cognito.
5. Elija Guardar cambios.

> **Important**
>
> Si ya no necesita el grupo de usuarios y de identidades de Amazon Cognito, elimínelos. De lo contrario, seguirá incurriendo en costos.

Eliminación de dominios que utilizan la autenticación de Amazon Cognito para OpenSearch Dashboards

Para evitar que los dominios que utilizan la autenticación de Amazon Cognito para Dashboards se bloqueen en un estado de configuración En proceso, elimine los dominios de OpenSearch Service antes de eliminar los grupos de identidades y de usuarios de Amazon Cognito asociados.

Uso de roles vinculados a servicios para Amazon OpenSearch Service.

Amazon OpenSearch Service utiliza roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a OpenSearch Service. OpenSearch Service predefine los roles vinculados a servicios y estos incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a servicios simplifica la configuración de OpenSearch Service porque ya no tendrá que agregar manualmente los permisos necesarios. OpenSearch Service define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo OpenSearch Service puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM. Para obtener información actualizada sobre las políticas de permisos y rples vinculados a servicios, consulte el historial de documentos de Amazon OpenSearch Service.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Yes (Sí) en la

columna Service-linked roles (Roles vinculados a servicios). Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Temas

Uso de roles vinculados a un servicio para crear dominios de VPC

Amazon OpenSearch Service utiliza roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a OpenSearch Service. OpenSearch Service predefine los roles vinculados a servicios y estos incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

OpenSearch Service utiliza la función vinculada al servicio AWSServiceRoleForAmazonOpenSearchService, que proporciona los permisos mínimos de Amazon EC2 y Elastic Load Balancing necesarios para que la función permita el acceso a la VPC para un dominio.

Función heredada de Elasticsearch

Amazon OpenSearch Service utiliza un rol vinculado a servicios denominado `AWSServiceRoleForAmazonOpenSearchService`. Es posible que las cuentas también contengan un rol vinculado a servicio denominado `AWSServiceRoleForAmazonElasticsearchService`, que funciona con los puntos de conexión de la API de Elasticsearch obsoletos.

Si el rol de Elasticsearch heredado no existe en la cuenta, OpenSearch Service creará automáticamente un nuevo rol vinculado a servicio de OpenSearch la primera vez que se cree un dominio de OpenSearch. En caso contrario, la cuenta seguirá utilizando el rol de Elasticsearch. Para que esta creación automática se realice correctamente, es necesario disponer de permisos para la acción `iam:CreateServiceLinkedRole`.

Permisos

El rol vinculado a servicios `AWSServiceRoleForAmazonOpenSearchService` confía en los siguientes servicios para asumir el rol:

- `opensearchservice.amazonaws.com`

La política de permisos del rol denominada `AmazonOpenSearchServiceRolePolicy` permite que OpenSearch Service realice las siguientes acciones en los recursos especificados:

- Acción: `acm:DescribeCertificate` en *
- Acción: `cloudwatch:PutMetricData` en *
- Acción: `ec2:CreateNetworkInterface` en *
- Acción: `ec2:DeleteNetworkInterface` en *
- Acción: `ec2:DescribeNetworkInterfaces` en *
- Acción: `ec2:ModifyNetworkInterfaceAttribute` en *
- Acción: `ec2:DescribeSecurityGroups` en *
- Acción: `ec2:DescribeSubnets` en *
- Acción: `ec2:DescribeVpcs` en *
- Acción: `ec2:CreateTags` en todas las interfaces de red y puntos de conexión de VPC
- Acción: `ec2:DescribeTags` en *
- Acción: `ec2:CreateVpcEndpoint` en todas las VPC, grupos de seguridad, subredes y tablas de enrutamiento, así como en todos los puntos de conexión de VPC, cuando la solicitud contiene la etiqueta `OpenSearchManaged=true`
- Acción: `ec2:ModifyVpcEndpoint` en todas las VPC, grupos de seguridad, subredes y tablas de enrutamiento, así como en todos los puntos de conexión de VPC, cuando la solicitud contiene la etiqueta `OpenSearchManaged=true`
- Acción: `ec2:DeleteVpcEndpoints` en todos los extremos cuando la solicitud contiene la etiqueta `OpenSearchManaged=true`
- Acción: `ec2:AssignIpv6Addresses` en *
- Acción: `ec2:UnAssignIpv6Addresses` en *
- Acción: `elasticloadbalancing:AddListenerCertificates` en *
- Acción: `elasticloadbalancing:RemoveListenerCertificates` en *

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a servicio

No necesita crear manualmente un rol vinculado a servicios. Cuando crea un dominio habilitado a la VPC mediante la AWS Management Console, OpenSearch Service crea el rol vinculado a servicios por usted. Para que esta creación automática se realice correctamente, es necesario disponer de permisos para la acción `iam:CreateServiceLinkedRole`.

También puede utilizar la consola de IAM, la CLI de IAM o la API de IAM para crear un rol vinculado a servicios manualmente. Para obtener más información, consulte Crear un rol vinculado a servicios en la Guía del usuario de IAM.

Edición del rol vinculado al servicio

OpenSearch Service no permite editar el rol vinculado a servicios `AWSServiceRoleForAmazonOpenSearchService`. 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 del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación del rol vinculado a un servicio

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a un servicio, recomendamos que elimine dicho rol. De esta forma, no tiene una entidad no utilizada que no se monitoree ni mantenga de forma activa. Sin embargo, debe limpiar el rol vinculado a servicios antes de eliminarlo manualmente.

Limpieza del rol vinculado al servicio de

Antes de poder utilizar IAM para eliminar un rol vinculado a un servicio, primero debe confirmar que dicho rol no tiene sesiones activas y eliminar los recursos que utiliza.

Para comprobar si el rol vinculado a un servicio tiene una sesión activa en la consola de IAM

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación de la consola de IAM, elija Roles (Roles). A continuación, seleccione el nombre (no la casilla de verificación) del rol de `AWSServiceRoleForAmazonOpenSearchService`.
3. En la página Resumen del rol seleccionado, elija la pestaña Asesor de acceso.
4. En la pestaña Asesor de acceso, revise la actividad reciente del rol vinculado a servicios.

> **Note**
>
> Si no está seguro de si OpenSearch Service utiliza el rol `AWSServiceRoleForAmazonOpenSearchService`, puede intentar eliminar el rol. Si el servicio utiliza el rol, este no podrá eliminarse y se podrán ver los recursos que lo utilizan. Si el rol se está utilizando, debe esperar que la sesión finalice para poder eliminarlo, o para eliminar los recursos que lo utilizan. No se puede revocar la sesión de un rol vinculado a servicios.

Eliminar manualmente un rol vinculado a servicios

Eliminar roles vinculados a servicios de la consola de IAM, API o la CLI de AWS. Para obtener más información, consulte Eliminar un rol vinculado a servicios en la Guía del usuario de IAM.

Uso de roles vinculados a un servicio para crear colecciones de OpenSearch sin servidor

OpenSearch sin servidor utiliza roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a OpenSearch Service. OpenSearch Service predefine los roles vinculados a servicios y estos incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

OpenSearch sin servidor usa el rol vinculado al servicio denominado AWSServiceRoleForAmazonOpenSearchServerless, que proporciona los permisos necesarios para que el rol publique las métricas de CloudWatch sin servidor en su cuenta.

Permisos de rol vinculados a servicios para OpenSearch sin servidor

OpenSearch sin servidor utiliza el rol vinculado a un servicio denominado AWSServiceRoleForAmazonOpenSearchServerless, que permite a OpenSearch sin servidor llame a servicios de AWS en su nombre.

El rol vinculado a un servicio AWSServiceRoleForAmazonOpenSearchServerless confía en que los siguientes servicios asuman el rol:

- `observability.aoss.amazonaws.com`

La política de permisos del rol denominada `AmazonOpenSearchServerlessServiceRolePolicy` permite que OpenSearch sin servidor realice las siguientes acciones en los recursos especificados:

- Acción: `cloudwatch:PutMetricData` en todos los recursos de AWS.

> **Note**
>
> La política incluye la clave de condición `{"StringEquals": {"cloudwatch:namespace": "AWS/AOSS"}}`, lo que significa que el rol vinculado al servicio solo puede enviar datos métricos al espacio de nombres de `AWS/AOSS` CloudWatch.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado al servicio para OpenSearch sin servidor

No necesita crear manualmente un rol vinculado a servicios. Cuando se crea una colección de OpenSearch sin servidor en la AWS Management Console, la AWS CLI, o la API de AWS, OpenSearch sin servidor crea el rol vinculado al servicio por usted.

> **Note**
>
> La primera vez que cree una colección, se le debe asignar la `iam:CreateServiceLinkedRole` en una política basada en identidades.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una colección de OpenSearch sin servidor, OpenSearch sin servidor vuelve a crear el rol vinculado al servicio.

Además, puede utilizar la consola de IAM para crear un rol vinculado al servicio con el caso de uso de Amazon OpenSearch sin servidor. En la AWS CLI o AWS API, cree un rol vinculado al servicio con el nombre de servicio `observability.aoss.amazonaws.com`.

```
aws iam create-service-linked-role --aws-service-name
 "observability.aoss.amazonaws.com"
```

Para obtener más información, consulte Creación de un rol vinculado a un servicio en la Guía del usuario de IAM. Si elimina este rol vinculado al servicio, puede utilizar este mismo proceso para volver a crear el rol.

Edición del rol vinculado a un servicio para OpenSearch sin servidor

OpenSearch sin servidor no permite editar el rol vinculado al servicio AWSServiceRoleForAmazonOpenSearchServerless. 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 del rol utilizando IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación del rol vinculado a un servicio para OpenSearch sin servidor

Si ya no necesita utilizar una característica o servicio que requiere un rol vinculado a servicios, recomendamos que elimine dicho rol. Esto evita tener una entidad sin uso que no se supervisa ni mantiene activamente. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

Para eliminar AWSServiceRoleForAmazonOpenSearchServerless, primero, debe eliminar todas las colecciones de OpenSearch sin servidor en su Cuenta de AWS.

> **Note**
>
> Si OpenSearch sin servidor está utilizando el rol cuando intenta eliminar los recursos, entonces la eliminación podría fallar. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForAmazonOpenSearchServerless. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones compatibles para roles vinculados a servicios de OpenSearch sin servidor

OpenSearch sin servidor admite el uso del rol vinculado al servicio AWSServiceRoleForAmazonOpenSearchServerless en todas las regiones en las que OpenSearch sin servidor esté disponible. Para obtener una lista de las regiones compatibles, consulte Puntos de conexión y cuotas de Amazon OpenSearch sin servidor en la Referencia general de Referencia general de AWS.

Uso de roles vinculados a servicio para crear canalizaciones de OpenSearch Ingestion

Amazon OpenSearch Ingestion utiliza roles vinculados al servicio de AWS Identity and Access Management (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a OpenSearch Ingestion. OpenSearch Ingestion predefine los roles vinculados a servicios y estos incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

OpenSearch Ingestion usa el rol vinculado al servicio denominado AWSServiceRoleForAmazonOpenSearchIngestion. La política adjunta proporciona los permisos necesarios para que el rol cree una nube privada virtual (VPC) entre su cuenta y OpenSearch Ingestion, y para publicar métricas de CloudWatch en su cuenta.

Permisos

El rol vinculado a servicios `AWSServiceRoleForAmazonOpenSearchIngestion` confía en los siguientes servicios para asumir el rol:

- `osis.amazon.com`

La política de permisos del rol denominada `AmazonOpenSearchIngestionServiceRolePolicy` permite que OpenSearch Ingestion realice las siguientes acciones en los recursos especificados:

- Acción: `ec2:DescribeSubnets` en `*`

- Acción: `ec2:DescribeSecurityGroups` en `*`
- Acción: `ec2:DeleteVpcEndpoints` en `*`
- Acción: `ec2:CreateVpcEndpoint` en `*`
- Acción: `ec2:DescribeVpcEndpoints` en `*`
- Acción: `ec2:CreateTags` en `arn:aws:ec2:*:*:network-interface/*`
- Acción: `cloudwatch:PutMetricData` en `cloudwatch:namespace": "AWS/OSIS"`

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a servicio para OpenSearch Ingestion

No necesita crear manualmente un rol vinculado a servicios. Cuando se crea una canalización de OpenSearch Ingestion en la AWS Management Console, la AWS CLI, o la API de AWS, OpenSearch Ingestion crea el rol vinculado al servicio por usted.

Si elimina este rol vinculado al servicio y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una canalización de OpenSearch Ingestion, OpenSearch Ingestion vuelve a crear el rol vinculado al servicio.

Edición del rol vinculado a servicio para OpenSearch Ingestion

OpenSearch Ingestion no le permite editar el rol vinculado a servicios de `AWSServiceRoleForAmazonOpenSearchIngestion`. Después de crear un rol vinculado a servicios, no puede cambiarle el nombre, ya que varias entidades pueden hacer referencia al mismo. Sin embargo, puede editar la descripción del rol mediante IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminación del rol vinculado a un servicio para OpenSearch Ingestion

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. Sin embargo, debe limpiar los recursos del rol vinculado al servicio antes de eliminarlo manualmente.

Limpiar un rol vinculado a servicios

Antes de que pueda utilizar IAM para eliminar un rol vinculado a servicios, primero debe eliminar los recursos que utiliza el rol.

> **Note**
>
> Si OpenSearch Ingestion está utilizando el rol cuando intenta eliminar los recursos, entonces la eliminación podría fallar. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de OpenSearch Ingestion utilizados por el **`AWSServiceRoleForAmazonOpenSearchIngestion`**

1. Vaya a la consola de Amazon OpenSearch Service y elija Ingestion.
2. Elimine todas las canalizaciones. Para obtener instrucciones, consulte the section called “Eliminar canalizaciones”.

Elimine el rol vinculado a servicio para OpenSearch Ingestion

Puede utilizar la consola de OpenSearch Ingestion para eliminar un rol vinculado a un servicio.

Para eliminar un rol vinculado a un servicio (consola)

1. Desplácese hasta la consola de IAM.
2. Elija Roles y busque el rol AWSServiceRoleForAmazonOpenSearchIngestion.
3. Seleccione el rol y elija Eliminar.

Código de muestra para Amazon OpenSearch Service

Este capítulo contiene un código de muestra común para trabajar con Amazon OpenSearch Service: la firma de solicitudes HTTP en una variedad de lenguajes de programación, la compresión de cuerpos de solicitudes HTTP y la utilización de SDK de AWS para crear dominios.

Temas

Compatibilidad con clientes de Elasticsearch

Las versiones más recientes de los clientes de Elasticsearch pueden incluir verificaciones de licencia o versión que rompen artificialmente la compatibilidad. En la tabla siguiente, se incluyen recomendaciones sobre las versiones de esos clientes que se utilizarán para obtener la mejor compatibilidad con OpenSearch Service.

> **Important**
>
> Estas versiones de cliente están desactualizadas y no se actualizan con las dependencias más recientes, incluida Log4j. Recomendamos encarecidamente utilizar las versiones de OpenSearch de los clientes siempre que sea posible.

Cliente	Versión recomendada
Cliente REST de bajo nivel de Java	7,1364
Cliente REST de alto nivel de Java	7,13.4
Cliente de Elasticsearch de Python	7,13.4
Cliente de Elasticsearch de Ruby	7,13.3
Cliente de Elasticsearch de Node.js	7,13.0

Compresión de solicitudes HTTP en Amazon OpenSearch Service

Puede comprimir solicitudes y respuestas HTTP en dominios de Amazon OpenSearch Service mediante la compresión gzip. La compresión gzip puede ayudar a reducir el tamaño de los documentos y a reducir la utilización y la latencia de la banda ancha, lo que permite mejorar las velocidades de transferencia.

La compresión gzip es compatible con todos los dominios que ejecutan OpenSearch, Elasticsearch 6.0 o posterior. Algunos clientes de OpenSearch cuentan con soporte integrado para la compresión gzip y muchos lenguajes de programación disponen de bibliotecas que simplifican el proceso.

Habilitar la compresión gzip

No debe confundirse con configuraciones similares de OpenSearch, `http_compression.enabled` es específico de OpenSearch Service y habilita o deshabilita la compresión gzip en un dominio. Los dominios que ejecutan OpenSearch o Elasticsearch 7.x tienen la compresión gzip habilitada de forma predeterminada, mientras que los dominios que ejecutan Elasticsearch 6.x la tienen desactivada de forma predeterminada.

Para habilitar la compresión gzip, envíe la siguiente solicitud:

```
PUT _cluster/settings
{
  "persistent" : {
    "http_compression.enabled": true
  }
}
```

Solicitudes a `_cluster/settings` deben estar descomprimidas, por lo que es posible que necesite utilizar un cliente independiente o una solicitud HTTP estándar para actualizar la configuración del clúster.

Encabezados obligatorios

Al incluir un cuerpo de la solicitud comprimido por gzip, mantenga el encabezado estándar `Content-Type: application/json` y agregue el encabezado `Content-Encoding: gzip`. Para aceptar una respuesta comprimida con gzip, agregue también el encabezado `Accept-Encoding: gzip`. Si un cliente de OpenSearch admite la compresión gzip, es probable que incluya estos encabezados automáticamente.

Código de muestra (Python 3)

En el siguiente ejemplo se utiliza opensearch-py para realizar la compresión y enviar la solicitud. Este código firma la solicitud mediante sus credenciales de IAM.

```
from opensearchpy import OpenSearch, RequestsHttpConnection
from requests_aws4auth import AWS4Auth
import boto3

host = '' # e.g. my-test-domain.us-east-1.es.amazonaws.com
region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Create the client.
search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    http_compress = True, # enables gzip compression for request bodies
    connection_class = RequestsHttpConnection
)

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Send the request.
print(search.index(index='movies', id='1', body=document, refresh=True))

# print(search.index(index='movies', doc_type='_doc', id='1', body=document,
 refresh=True))
```

Como alternativa, puede especificar los encabezados adecuados, comprimir el cuerpo de la solicitud usted mismo y utilizar una biblioteca HTTP estándar como Solicitudes. Este código firma la solicitud con credenciales básicas HTTP, que podrían ser compatibles con el dominio si utiliza el control de acceso detallado.

```
import requests
import gzip
import json

base_url = '' # The domain with https:// and a trailing slash. For example, https://my-test-domain.us-east-1.es.amazonaws.com/
auth = ('master-user', 'master-user-password') # For testing only. Don't store credentials in code.

headers = {'Accept-Encoding': 'gzip', 'Content-Type': 'application/json',
           'Content-Encoding': 'gzip'}

document = {
  "title": "Moneyball",
  "director": "Bennett Miller",
  "year": "2011"
}

# Compress the document.
compressed_document = gzip.compress(json.dumps(document).encode())

# Send the request.
path = 'movies/_doc?refresh=true'
url = base_url + path
response = requests.post(url, auth=auth, headers=headers, data=compressed_document)
print(response.status_code)
print(response.text)
```

Utilizar SDK de AWS para interactuar con Amazon OpenSearch Service

En esta sección, se incluyen ejemplos de cómo utilizar los SDK de AWS para interactuar con la API de configuración de Amazon OpenSearch Service. Estos ejemplos de código muestran cómo crear, actualizar y eliminar dominios de OpenSearch Service.

Java

Esta sección incluye ejemplos para las versiones 1 y 2 del AWS SDK for Java.

Version 2

En este ejemplo se utiliza el constructor OpenSearchClientBuilder de la versión 2 de AWS SDK for Java para crear un dominio OpenSearch, actualizar su configuración y eliminarlo. Quite los comentarios de las llamadas a `waitForDomainProcessing` (y el comentario de la llamada a `deleteDomain`) para permitir que se active el dominio y que se pueda utilizar.

```
package com.example.samples;

import java.util.concurrent.TimeUnit;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.opensearch.OpenSearchClient;
import software.amazon.awssdk.services.opensearch.model.ClusterConfig;
import software.amazon.awssdk.services.opensearch.model.EBSOptions;
import software.amazon.awssdk.services.opensearch.model.CognitoOptions;
import software.amazon.awssdk.services.opensearch.model.NodeToNodeEncryptionOptions;
import software.amazon.awssdk.services.opensearch.model.CreateDomainRequest;
import software.amazon.awssdk.services.opensearch.model.CreateDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigRequest;
import software.amazon.awssdk.services.opensearch.model.UpdateDomainConfigResponse;
import software.amazon.awssdk.services.opensearch.model.DescribeDomainResponse;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainRequest;
import software.amazon.awssdk.services.opensearch.model.DeleteDomainResponse;
import software.amazon.awssdk.services.opensearch.model.OpenSearchException;
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

     String domainName = "my-test-domain";

     // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
```

```
        OpenSearchClient client = OpenSearchClient.builder()
          // Unnecessary, but lets you use a region different than your default.
          .region(Region.US_EAST_1)
          // Unnecessary, but if desired, you can use a different provider chain.
          .credentialsProvider(DefaultCredentialsProvider.create())
                    .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        //waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain you want to create
     */

    public static void createDomain(OpenSearchClient client, String domainName) {

     // Create the request and set the desired configuration options

        try {

            ClusterConfig clusterConfig = ClusterConfig.builder()
                    .dedicatedMasterEnabled(true)
                    .dedicatedMasterCount(3)
                    // Small, inexpensive instance types for testing. Not
recommended for production.
                    .dedicatedMasterType("t2.small.search")
                    .instanceType("t2.small.search")
                    .instanceCount(5)
                    .build();
```

```
            // Many instance types require EBS storage.
            EBSOptions ebsOptions = EBSOptions.builder()
                    .ebsEnabled(true)
                    .volumeSize(10)
                    .volumeType("gp2")
                    .build();

            NodeToNodeEncryptionOptions encryptionOptions =
 NodeToNodeEncryptionOptions.builder()
                    .enabled(true)
                    .build();

            CreateDomainRequest createRequest = CreateDomainRequest.builder()
                    .domainName(domainName)
                    .engineVersion("OpenSearch_1.0")
                    .clusterConfig(clusterConfig)
                    .ebsOptions(ebsOptions)
                    .nodeToNodeEncryptionOptions(encryptionOptions)
                    // You can uncomment this line and add your account ID, a
 username, and the
                    // domain name to add an access policy.
                    // .accessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")
                    .build();

            // Make the request.
            System.out.println("Sending domain creation request...");
            CreateDomainResponse createResponse =
 client.createDomain(createRequest);
            System.out.println("Domain status:
 "+createResponse.domainStatus().toString());
            System.out.println("Domain ID:
 "+createResponse.domainStatus().domainId());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
```

```
    * Updates the configuration of an Amazon OpenSearch Service domain with the
    * specified options. Some options require other Amazon Web Services resources,
such as an
    * Amazon Cognito user pool and identity pool, whereas others require just an
    * instance type or instance count.
    *
    * @param client
    *            The client to use for the requests to Amazon OpenSearch Service
    * @param domainName
    *            The name of the domain to update
    */

   public static void updateDomain(OpenSearchClient client, String domainName) {

    // Updates the domain to use three data instances instead of five.
       // You can uncomment the Cognito line and fill in the strings to enable
Cognito
       // authentication for OpenSearch Dashboards.

       try {

           ClusterConfig clusterConfig = ClusterConfig.builder()
                   .instanceCount(5)
                   .build();

           CognitoOptions cognitoOptions = CognitoOptions.builder()
                   .enabled(true)
                   .userPoolId("user-pool-id")
                   .identityPoolId("identity-pool-id")
                   .roleArn("role-arn")
                   .build();

           UpdateDomainConfigRequest updateRequest =
UpdateDomainConfigRequest.builder()
                   .domainName(domainName)
                   .clusterConfig(clusterConfig)
                   //.cognitoOptions(cognitoOptions)
                   .build();

           System.out.println("Sending domain update request...");
           UpdateDomainConfigResponse updateResponse =
client.updateDomainConfig(updateRequest);
           System.out.println("Domain config:
"+updateResponse.domainConfig().toString());
```

```
        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain that you want to delete
     */

    public static void deleteDomain(OpenSearchClient client, String domainName) {

        try {

            DeleteDomainRequest deleteRequest = DeleteDomainRequest.builder()
                    .domainName(domainName)
                    .build();

            System.out.println("Sending domain deletion request...");
            DeleteDomainResponse deleteResponse =
client.deleteDomain(deleteRequest);
            System.out.println("Domain status: "+deleteResponse.toString());


        } catch (OpenSearchException e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
```

```
     * take a similar amount of time. This method checks every 15 seconds and
 finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */

    public static void waitForDomainProcessing(OpenSearchClient client, String
 domainName) {
        // Create a new request to check the domain status.
        DescribeDomainRequest describeRequest = DescribeDomainRequest.builder()
                .domainName(domainName)
                .build();

        // Every 15 seconds, check whether the domain is processing.
        DescribeDomainResponse describeResponse =
 client.describeDomain(describeRequest);
        while (describeResponse.domainStatus().processing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse = client.describeDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
 changes for your domain.");
        System.out.println("Domain description: "+describeResponse.toString());
    }
}
```

Version 1

En este ejemplo se utiliza el constructor AWSElasticsearchClientBuilder de la versión 1 del AWS SDK for Java para crear un dominio Elasticsearch heredado, actualizar su configuración y eliminarlo. Quite los comentarios de las llamadas a `waitForDomainProcessing` (y el

comentario de la llamada a `deleteDomain`) para permitir que se active el dominio y que se pueda utilizar.

```
package com.amazonaws.samples;

import java.util.concurrent.TimeUnit;
import com.amazonaws.auth.DefaultAWSCredentialsProviderChain;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.elasticsearch.AWSElasticsearch;
import com.amazonaws.services.elasticsearch.AWSElasticsearchClientBuilder;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.CreateElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DeleteElasticsearchDomainResult;
import
 com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainRequest;
import com.amazonaws.services.elasticsearch.model.DescribeElasticsearchDomainResult;
import com.amazonaws.services.elasticsearch.model.EBSOptions;
import com.amazonaws.services.elasticsearch.model.ElasticsearchClusterConfig;
import com.amazonaws.services.elasticsearch.model.ResourceNotFoundException;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigRequest;
import
 com.amazonaws.services.elasticsearch.model.UpdateElasticsearchDomainConfigResult;
import com.amazonaws.services.elasticsearch.model.VolumeType;

/**
 * Sample class demonstrating how to use the Amazon Web Services SDK for Java to
 create, update,
 * and delete Amazon OpenSearch Service domains.
 */

public class OpenSearchSample {

    public static void main(String[] args) {

        final String domainName = "my-test-domain";

        // Build the client using the default credentials chain.
        // You can use the CLI and run `aws configure` to set access key, secret
        // key, and default region.
        final AWSElasticsearch client = AWSElasticsearchClientBuilder
                .standard()
```

```
                // Unnecessary, but lets you use a region different than your
default.
                .withRegion(Regions.US_WEST_2)
                // Unnecessary, but if desired, you can use a different provider
chain.
                .withCredentials(new DefaultAWSCredentialsProviderChain())
                .build();

        // Create a new domain, update its configuration, and delete it.
        createDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        updateDomain(client, domainName);
        // waitForDomainProcessing(client, domainName);
        deleteDomain(client, domainName);
    }

    /**
     * Creates an Amazon OpenSearch Service domain with the specified options.
     * Some options require other Amazon Web Services resources, such as an Amazon
Cognito user pool
     * and identity pool, whereas others require just an instance type or instance
     * count.
     *
     * @param client
     *             The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *             The name of the domain you want to create
     */
    private static void createDomain(final AWSElasticsearch client, final String
domainName) {

        // Create the request and set the desired configuration options
        CreateElasticsearchDomainRequest createRequest = new
CreateElasticsearchDomainRequest()
                .withDomainName(domainName)
                .withElasticsearchVersion("7.10")
                .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                        .withDedicatedMasterEnabled(true)
                        .withDedicatedMasterCount(3)
                        // Small, inexpensive instance types for testing. Not
recommended for production
                        // domains.
                        .withDedicatedMasterType("t2.small.elasticsearch")
                        .withInstanceType("t2.small.elasticsearch")
```

```
                        .withInstanceCount(5))
                // Many instance types require EBS storage.
                .withEBSOptions(new EBSOptions()
                        .withEBSEnabled(true)
                        .withVolumeSize(10)
                        .withVolumeType(VolumeType.Gp2));
                // You can uncomment this line and add your account ID, a username,
 and the
                // domain name to add an access policy.
                // .withAccessPolicies("{\"Version\":\"2012-10-17\",
\"Statement\":[{\"Effect\":\"Allow\",\"Principal\":{\"AWS\":
[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:region:123456789012:domain/domain-name/*\"}]}")


        // Make the request.
        System.out.println("Sending domain creation request...");
        CreateElasticsearchDomainResult createResponse =
 client.createElasticsearchDomain(createRequest);
        System.out.println("Domain creation response from Amazon OpenSearch
 Service:");
        System.out.println(createResponse.getDomainStatus().toString());
    }

    /**
     * Updates the configuration of an Amazon OpenSearch Service domain with the
     * specified options. Some options require other Amazon Web Services resources,
 such as an
     * Amazon Cognito user pool and identity pool, whereas others require just an
     * instance type or instance count.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain to update
     */
    private static void updateDomain(final AWSElasticsearch client, final String
 domainName) {
        try {
            // Updates the domain to use three data instances instead of five.
            // You can uncomment the Cognito lines and fill in the strings to enable
 Cognito
            // authentication for OpenSearch Dashboards.
```

```
            final UpdateElasticsearchDomainConfigRequest updateRequest = new
UpdateElasticsearchDomainConfigRequest()
                    .withDomainName(domainName)
                    // .withCognitoOptions(new CognitoOptions()
                            // .withEnabled(true)
                            // .withUserPoolId("user-pool-id")
                            // .withIdentityPoolId("identity-pool-id")
                            // .withRoleArn("role-arn")
                    .withElasticsearchClusterConfig(new ElasticsearchClusterConfig()
                            .withInstanceCount(3));

            System.out.println("Sending domain update request...");
            final UpdateElasticsearchDomainConfigResult updateResponse = client
                    .updateElasticsearchDomainConfig(updateRequest);
            System.out.println("Domain update response from Amazon OpenSearch
Service:");
            System.out.println(updateResponse.toString());
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }

    /**
     * Deletes an Amazon OpenSearch Service domain. Deleting a domain can take
     * several minutes.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to delete
     */
    private static void deleteDomain(final AWSElasticsearch client, final String
domainName) {
        try {
            final DeleteElasticsearchDomainRequest deleteRequest = new
DeleteElasticsearchDomainRequest()
                    .withDomainName(domainName);

            System.out.println("Sending domain deletion request...");
            final DeleteElasticsearchDomainResult deleteResponse =
client.deleteElasticsearchDomain(deleteRequest);
            System.out.println("Domain deletion response from Amazon OpenSearch
Service:");
            System.out.println(deleteResponse.toString());
```

```
        } catch (ResourceNotFoundException e) {
            System.out.println("Domain not found. Please check the domain name.");
        }
    }

    /**
     * Waits for the domain to finish processing changes. New domains typically take
15-30 minutes
     * to initialize, but can take longer depending on the configuration. Most
updates to existing domains
     * take a similar amount of time. This method checks every 15 seconds and
finishes only when
     * the domain's processing status changes to false.
     *
     * @param client
     *            The client to use for the requests to Amazon OpenSearch Service
     * @param domainName
     *            The name of the domain that you want to check
     */
    private static void waitForDomainProcessing(final AWSElasticsearch client, final
String domainName) {
        // Create a new request to check the domain status.
        final DescribeElasticsearchDomainRequest describeRequest = new
DescribeElasticsearchDomainRequest()
                .withDomainName(domainName);

        // Every 15 seconds, check whether the domain is processing.
        DescribeElasticsearchDomainResult describeResponse =
client.describeElasticsearchDomain(describeRequest);
        while (describeResponse.getDomainStatus().isProcessing()) {
            try {
                System.out.println("Domain still processing...");
                TimeUnit.SECONDS.sleep(15);
                describeResponse =
client.describeElasticsearchDomain(describeRequest);
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
        }

        // Once we exit that loop, the domain is available
        System.out.println("Amazon OpenSearch Service has finished processing
changes for your domain.");
```

```
        System.out.println("Domain description response from Amazon OpenSearch
 Service:");
        System.out.println(describeResponse.toString());
    }
}
```

Python

En este ejemplo se utiliza el cliente Python de bajo nivel OpenSearchService desde AWS SDK for Python (Boto) para crear un dominio, actualizar su configuración y eliminarlo.

```
import boto3
import botocore
from botocore.config import Config
import time

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-west-2'
)

client = boto3.client('opensearch', config=my_config)

domainName = 'my-test-domain'  # The name of the domain


def createDomain(client, domainName):
    """Creates an Amazon OpenSearch Service domain with the specified options."""
    response = client.create_domain(
        DomainName=domainName,
        EngineVersion='OpenSearch_1.0',
        ClusterConfig={
            'InstanceType': 't2.small.search',
            'InstanceCount': 5,
            'DedicatedMasterEnabled': True,
            'DedicatedMasterType': 't2.small.search',
            'DedicatedMasterCount': 3
        },
```

```
        # Many instance types require EBS storage.
        EBSOptions={
            'EBSEnabled': True,
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
        AccessPolicies="{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-west-2:123456789012:domain/my-test-domain/*
\"}]}",
        NodeToNodeEncryptionOptions={
            'Enabled': True
        }
    )
    print("Creating domain...")
    print(response)


def updateDomain(client, domainName):
    """Updates the domain to use three data nodes instead of five."""
    try:
        response = client.update_domain_config(
            DomainName=domainName,
            ClusterConfig={
                'InstanceCount': 3
            }
        )
        print('Sending domain update request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def deleteDomain(client, domainName):
    """Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes."""
    try:
        response = client.delete_domain(
            DomainName=domainName
        )
```

```
        print('Sending domain deletion request...')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def waitForDomainProcessing(client, domainName):
    """Waits for the domain to finish processing changes."""
    try:
        response = client.describe_domain(
            DomainName=domainName
        )
        # Every 15 seconds, check whether the domain is processing.
        while response["DomainStatus"]["Processing"] == True:
            print('Domain still processing...')
            time.sleep(15)
            response = client.describe_domain(
                DomainName=domainName)

        # Once we exit the loop, the domain is available.
        print('Amazon OpenSearch Service has finished processing changes for your
 domain.')
        print('Domain description:')
        print(response)

    except botocore.exceptions.ClientError as error:
        if error.response['Error']['Code'] == 'ResourceNotFoundException':
            print('Domain not found. Please check the domain name.')
        else:
            raise error


def main():
    """Create a new domain, update its configuration, and delete it."""
    createDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    updateDomain(client, domainName)
    waitForDomainProcessing(client, domainName)
    deleteDomain(client, domainName)
```

Nodo

En este ejemplo, se utiliza la versión 3 del SDK para JavaScript in Node.js OpenSearch client para crear un dominio, actualizar su configuración y eliminarlo.

```
var {
    OpenSearchClient,
    CreateDomainCommand,
    DescribeDomainCommand,
    UpdateDomainConfigCommand,
    DeleteDomainCommand
} = require("@aws-sdk/client-opensearch");
var sleep = require('sleep');

var client = new OpenSearchClient();

var domainName = 'my-test-domain'

// Create a new domain, update its configuration, and delete it.
createDomain(client, domainName)
waitForDomainProcessing(client, domainName)
updateDomain(client, domainName)
waitForDomainProcessing(client, domainName)
deleteDomain(client, domainName)

async function createDomain(client, domainName) {
    // Creates an Amazon OpenSearch Service domain with the specified options.
    var command = new CreateDomainCommand({
        DomainName: domainName,
        EngineVersion: 'OpenSearch_1.0',
        ClusterConfig: {
        'InstanceType': 't2.small.search',
        'InstanceCount': 5,
        'DedicatedMasterEnabled': 'True',
        'DedicatedMasterType': 't2.small.search',
        'DedicatedMasterCount': 3
        },
        EBSOptions:{
            'EBSEnabled': 'True',
            'VolumeType': 'gp2',
            'VolumeSize': 10
        },
```

```
        AccessPolicies: "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"arn:aws:iam::123456789012:user/user-name\"]},\"Action\":
[\"es:*\"],\"Resource\":\"arn:aws:es:us-east-1:123456789012:domain/my-test-domain/*
\"}]}",
         NodeToNodeEncryptionOptions:{
            'Enabled': 'True'
        }
    });
    const response = await client.send(command);
    console.log("Creating domain...");
    console.log(response);
}

async function updateDomain(client, domainName) {
    // Updates the domain to use three data nodes instead of five.
    var command = new UpdateDomainConfigCommand({
        DomainName: domainName,
        ClusterConfig: {
        'InstanceCount': 3
        }
    });
    const response = await client.send(command);
    console.log('Sending domain update request...');
    console.log(response);
}

async function deleteDomain(client, domainName) {
    // Deletes an OpenSearch Service domain. Deleting a domain can take several
 minutes.
    var command = new DeleteDomainCommand({
        DomainName: domainName
    });
    const response = await client.send(command);
    console.log('Sending domain deletion request...');
    console.log(response);
}

async function waitForDomainProcessing(client, domainName) {
    // Waits for the domain to finish processing changes.
    try {
        var command = new DescribeDomainCommand({
            DomainName: domainName
        });
        var response = await client.send(command);
```

```
        while (response.DomainStatus.Processing == true) {
            console.log('Domain still processing...')
            await sleep(15000) // Wait for 15 seconds, then check the status again
            function sleep(ms) {
                return new Promise((resolve) => {
                    setTimeout(resolve, ms);
                });
            }
            var response = await client.send(command);
        }
        // Once we exit the loop, the domain is available.
        console.log('Amazon OpenSearch Service has finished processing changes for your
 domain.');
        console.log('Domain description:');
        console.log(response);

    } catch (error) {
        if (error.name === 'ResourceNotFoundException') {
            console.log('Domain not found. Please check the domain name.');
            }
    };
}
```

Indexación de datos en Amazon OpenSearch Service

Dado que Amazon OpenSearch Service utiliza una API de REST, existen numerosos métodos para indexar documentos. Puede utilizar clientes estándar como curl o cualquier lenguaje de programación que pueda enviar solicitudes HTTP. Para simplificar aún más el proceso de interacción, OpenSearch Service cuenta con clientes para diversos lenguajes de programación. Los usuarios avanzados pueden pasar directamente a the section called “Cargando datos de streaming en el OpenSearch servicio”.

Le recomendamos mucho que utilice Amazon OpenSearch Ingestion para incorporar datos, que es un recopilador de datos totalmente administrado e integrado en OpenSearch Service. Para más información, consulte Amazon OpenSearch Ingestion.

Para ver una introducción a la indexación, consulte la documentación de OpenSearch.

Restricciones de nomenclatura de los índices

Los índices de OpenSearch Service tienen las siguientes restricciones de nomenclatura:

- Todas las letras deben estar en minúsculas.
- Los nombres de los índices no pueden empezar por `_` ni `-`.
- Los nombres de los índices no pueden contener espacios, comas, `:`, `"`, `*`, `+`, `/`, `\`, `|`, `?`, `#`, `>` o `<`.

No incluya información confidencial en los nombres de ID de índice, tipo o documento. OpenSearch Service utiliza estos nombres en sus identificadores uniformes de recursos (URI). A menudo, los servidores y las aplicaciones registran solicitudes HTTP, lo que puede dar lugar a que se expongan datos innecesariamente si los URI contienen información confidencial:

```
2018-10-03T23:39:43 198.51.100.14 200 "GET https://opensearch-domain/dr-jane-doe/flu-patients-2018/202-555-0100/ HTTP/1.1"
```

Aunque no tenga permisos para ver el documento JSON asociado, puede inferir de esta línea de registro falsa que uno de los pacientes del Dr. Doe, cuyo número de teléfono es el 202-555-0100, tuvo gripe en 2018.

Si OpenSearch Service detecta una dirección IP real o percibida en un nombre de índice (por ejemplo, `my-index-12.34.56.78.91`), enmascara la dirección IP. Una llamada a `_cat/indices` produce la siguiente respuesta:

```
green open my-index-x.x.x.x.91    soY19tBERoKo71WcEScidw 5 1 0 0   2kb  1kb
```

Para evitar confusiones innecesarias, evite incluir direcciones IP en los nombres de los índices.

Reducción del tamaño de la respuesta

Las respuestas de las API `_bulk` y `_index` contienen bastante información. Esta información puede resultar útil para resolver problemas de las solicitudes o para implementar la lógica de reintentos, aunque puede utilizar una banda ancha considerable. En este ejemplo, la indexación de un documento de 32 bytes se traduce en una respuesta de 339 bytes (incluidos los encabezados):

```
PUT opensearch-domain/more-movies/_doc/1
{"title": "Back to the Future"}
```

Respuesta

```
{
  "_index": "more-movies",
  "_type": "_doc",
  "_id": "1",
  "_version": 4,
  "result": "updated",
  "_shards": {
    "total": 2,
    "successful": 2,
    "failed": 0
  },
  "_seq_no": 3,
  "_primary_term": 1
}
```

Este tamaño de respuesta puede parecer mínimo, pero si indexa 1 000 000 de documentos al día (aproximadamente 11,5 documentos por segundo), 339 bytes por respuesta equivalen a 10,17 GB de tráfico de descarga al mes.

Si los costos de transferencia de datos son una preocupación, utilice el parámetro `filter_path` para reducir el tamaño de la respuesta de OpenSearch Service, pero procure no filtrar campos que necesita para poder identificar o reintentar solicitudes que fallaron. Estos campos varían por cliente. El parámetro `filter_path` funciona para todas las API de REST de OpenSearch Service, pero resulta especialmente útil con las API a las que se llama con frecuencia, como las API `_index` y `_bulk`:

```
PUT opensearch-domain/more-movies/_doc/1?filter_path=result,_shards.total
{"title": "Back to the Future"}
```

Respuesta

```
{
  "result": "updated",
  "_shards": {
    "total": 2
  }
}
```

En lugar de incluir campos, puede excluir campos con un prefijo `-`. `filter_path` también es compatible con comodines:

```
POST opensearch-domain/_bulk?filter_path=-took,-items.index._*
{ "index": { "_index": "more-movies", "_id": "1" } }
{"title": "Back to the Future"}
{ "index": { "_index": "more-movies", "_id": "2" } }
{"title": "Spirited Away"}
```

Respuesta

```
{
  "errors": false,
  "items": [
    {
      "index": {
        "result": "updated",
        "status": 200
      }
    },
    {
      "index": {
```

```
        "result": "updated",
        "status": 200
      }
    }
  ]
}
```

Códecs de índice

Los códecs de índice determinan cómo se comprimen y almacenan en el disco los campos almacenados en un índice. El códec de índice se controla mediante la configuración `index.codec` estática, que especifica el algoritmo de compresión. Esta configuración afecta el tamaño de la partición del índice y el rendimiento de la operación.

Para obtener una lista de los códecs compatibles y sus características de rendimiento, consulte los Códecs compatibles en la documentación de OpenSearch.

Cuando elija un códec de índice, tenga en cuenta lo siguiente:

- Para evitar los problemas que supone cambiar la configuración del códec de un índice existente, pruebe una carga de trabajo representativa en un entorno que no sea de producción antes de utilizar una nueva configuración de códec. Para más información, consulte Cambio de un códec de índice.
- No puede usar los códecs de compresión `zstd` y `zstd_no_dict` para los índices k-NN o Security Analytics.
- La migración a instancias de UltraWarm está deshabilitada para los índices ZStandard.

Carga de datos de streaming en Amazon OpenSearch Service

Puedes usar OpenSearch Ingestion para cargar directamente los datos de streaming en tu dominio de Amazon OpenSearch Service, sin necesidad de utilizar soluciones de terceros. Para enviar datos a OpenSearch Ingestion, debes configurar tus generadores de datos y el servicio entrega automáticamente los datos al dominio o la colección que especifiques. Para empezar a usar OpenSearch Ingestion, consulte. the section called “Tutorial: incorporar datos en una colección”

Puedes seguir utilizando otras fuentes para cargar datos de streaming, como Amazon Data Firehose y Amazon CloudWatch Logs, que tienen soporte integrado para OpenSearch Service. Otros, como Amazon S3, Amazon Kinesis Data Streams y Amazon DynamoDB, utilizan funciones AWS

Lambda como controladores de eventos. Las funciones de Lambda responden a los nuevos datos procesándolos y transmitiéndolos al dominio.

> **Note**
>
> Lambda es compatible con varios lenguajes de programación populares y está disponible en la mayoría de las Regiones de AWS. Para más información, consulte Introducción a Lambda en la Guía para desarrolladores deAWS Lambda y Puntos de conexión de servicio deAWS en Referencia general de AWS.

Temas

- Cargando datos de streaming desde Ingestion OpenSearch
- Carga de datos de streaming desde Amazon S3
- Cargar datos de streaming desde Amazon Kinesis Data Streams
- Carga de datos de streaming desde Amazon DynamoDB
- Carga de datos de streaming desde Amazon Data Firehose
- Carga de datos de streaming desde Amazon CloudWatch
- Carga de datos de streaming desde AWS IoT

Cargando datos de streaming desde Ingestion OpenSearch

Puede usar Amazon OpenSearch Ingestion para cargar datos en un dominio OpenSearch de servicio. Usted configura sus generadores de datos para que envíen datos a OpenSearch Ingestion y esta entrega automáticamente los datos a la colección que usted especifique. También puede configurar OpenSearch Ingestion para transformar los datos antes de entregarlos. Para obtener más información, consulte OpenSearch Ingestión de Amazon.

Carga de datos de streaming desde Amazon S3

Puede usar Lambda para enviar datos a su dominio de OpenSearch servicio desde Amazon S3. Cuando llegan datos nuevos a un bucket de S3, activan una notificación de eventos en Lambda que, a su vez, ejecuta el código personalizado para realizar la indexación.

Este método de streaming de datos es extremadamente flexible. Es posible indexar los metadatos del objeto o, si el objeto contiene texto sin formato, analizar e indexar algunos elementos del cuerpo

del objeto. En esta sección, se incluye código de muestra sencillo de Python que utiliza expresiones regulares para analizar un archivo de registros e indexar los resultados obtenidos.

Requisitos previos

Antes de continuar, debe contar con los siguientes recursos.

Requisito previo	Descripción
Bucket de Amazon S3	Para más información, consulte Crear su primer bucket de S3 en la Guía del usuario de Amazon Simple Storage Service. El bucket debe residir en la misma región que su dominio OpenSearch de servicio.
OpenSearch Dominio de servicio	Es el destino de los datos después de que la función de Lambda los procesa. Para más información, consulte the section called “ Creación de dominios OpenSearch de servicio”.

Crear el paquete de implementación de Lambda

Los paquetes de implementación son archivos ZIP o JAR que contienen el código y sus dependencias. En esta sección, se incluye un código de muestra de Python. Para otros lenguajes de programación, consulte Paquetes de implementación de Lambda en la Guía para desarrolladores deAWS Lambda .

1. Cree un directorio. En este ejemplo, utilizamos el nombre `s3-to-opensearch`.
2. Cree un archivo en el directorio denominado `sample.py`:

```
import boto3
import re
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
```

```
index = 'lambda-s3-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype

headers = { "Content-Type": "application/json" }

s3 = boto3.client('s3')

# Regular expressions used to parse some simple log lines
ip_pattern = re.compile('(\d+\.\d+\.\d+\.\d+)')
time_pattern = re.compile('\[(\d+\/\w\w\w\/\d\d\d\d:\d\d:\d\d:\d\d\s-\d\d\d\d)\]')
message_pattern = re.compile('\"(.+)\"')

# Lambda execution starts here
def handler(event, context):
    for record in event['Records']:

        # Get the bucket name and key for the new file
        bucket = record['s3']['bucket']['name']
        key = record['s3']['object']['key']

        # Get, read, and split the file into lines
        obj = s3.get_object(Bucket=bucket, Key=key)
        body = obj['Body'].read()
        lines = body.splitlines()

        # Match the regular expressions to each line and index the JSON
        for line in lines:
            line = line.decode("utf-8")
            ip = ip_pattern.search(line).group(1)
            timestamp = time_pattern.search(line).group(1)
            message = message_pattern.search(line).group(1)

            document = { "ip": ip, "timestamp": timestamp, "message": message }
            r = requests.post(url, auth=awsauth, json=document, headers=headers)
```

Edite las variables para `region` y `host`.

3. Instale pip, si todavía no lo hizo, luego instale las dependencias en un directorio `package` nuevo:

```
cd s3-to-opensearch
```

```
pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

Todos los entornos de ejecución de Lambda tienen instalado Boto3, por lo que no es necesario incluirlo en el paquete de implementación.

4. Cree el paquete con el código de la aplicación y las dependencias:

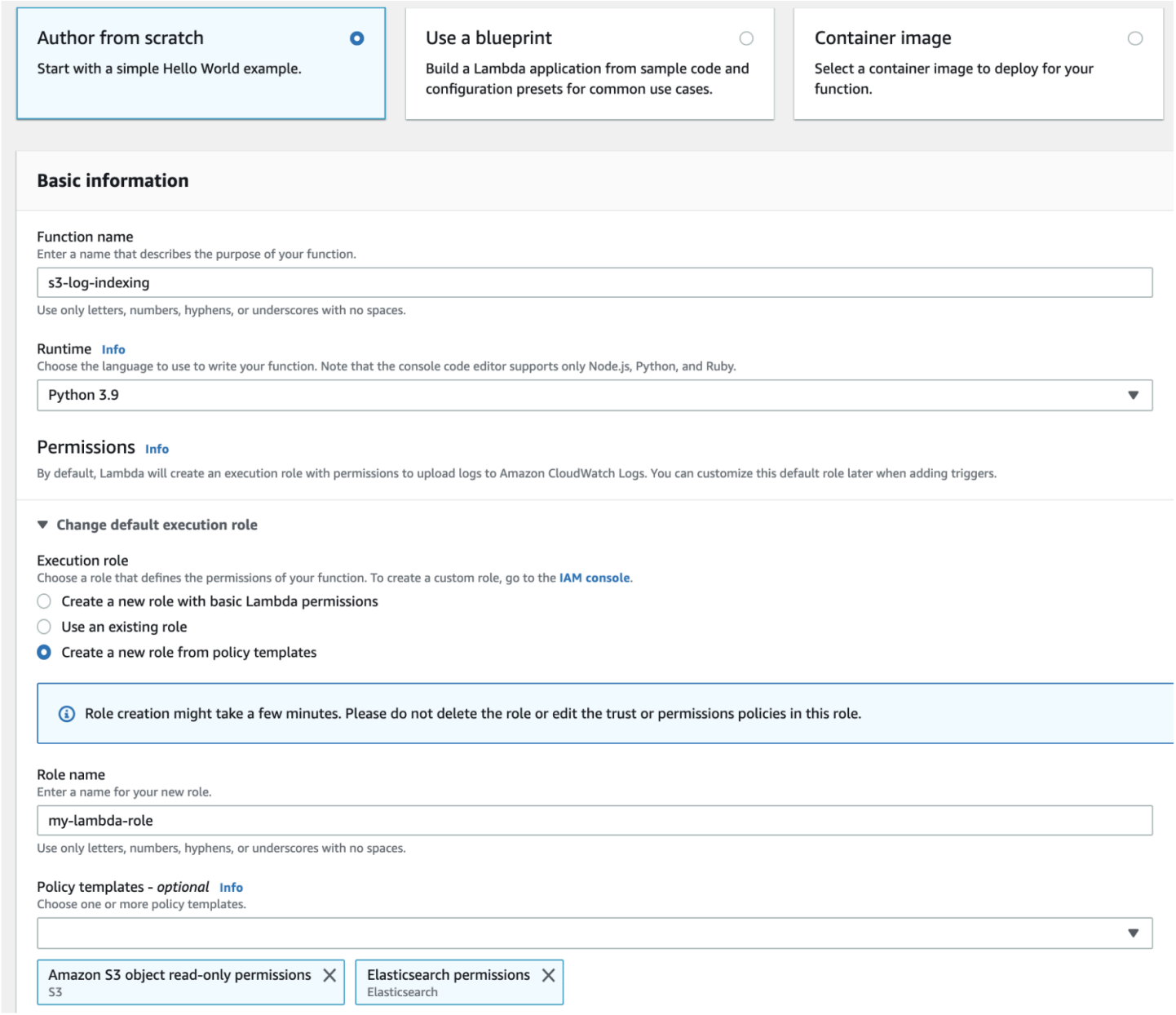
```
cd package
zip -r ../lambda.zip .

cd ..
zip -g lambda.zip sample.py
```

Crear la función de Lambda

Después de crear el paquete de implementación, puede crear la función de Lambda. Al crear una función, elija un nombre, un tiempo de ejecución (por ejemplo, Python 3.8) y un rol de IAM. El rol de IAM define los permisos para la función. Para obtener instrucciones detalladas, consulte Create a Lambda function with the consol en la Guía para desarrolladores deAWS Lambda .

En este ejemplo, se supone que utiliza la consola. Elija Python 3.9 y un rol que tenga permisos de lectura en S3 y permisos de escritura en el OpenSearch servicio, como se muestra en la siguiente captura de pantalla:



Después de crear la función, debe agregar un desencadenador. En este ejemplo, queremos que el código se ejecute cada vez que llega un archivo de registros a un bucket de S3:

1. Seleccione Agregar desencadenador y Seleccione S3.
2. Seleccione el bucket.
3. Para el Tipo de evento, elija PUT.
4. Para el Prefijo, escriba `logs/`.
5. Para el Sufijo, escriba `.log`.
6. Reconozca la advertencia de invocación recursiva y elija Agregar.

Por último, puede cargar el paquete de implementación:

1. Seleccione Cargar desde y archivo .zip, luego siga las instrucciones para cargar el paquete de implementación.
2. Una vez finalizada la carga, edite la Configuración de tiempo de ejecución y cambie el Controlador a `sample.handler`. Esta configuración indica a Lambda el archivo (`sample.py`) y el método (`handler`) que debe ejecutar cuando se produzca un desencadenador.

En este punto, dispone de un conjunto completo de recursos: un depósito para los archivos de registro, una función que se ejecuta cada vez que se añade un archivo de registro al depósito, un código que realiza el análisis y la indexación y un dominio de OpenSearch servicio para la búsqueda y la visualización.

Prueba de la función de Lambda

Después de crear la función, puede probarla mediante la carga de un archivo en el bucket de Amazon S3. Cree un archivo denominado `sample.log` que contenga los siguientes ejemplos de líneas de registro:

```
12.345.678.90 - [10/Oct/2000:13:55:36 -0700] "PUT /some-file.jpg"
12.345.678.91 - [10/Oct/2000:14:56:14 -0700] "GET /some-file.jpg"
```

Cargue el archivo en la carpeta `logs` del bucket de S3. Para obtener instrucciones, consulte Carga de un objeto en el bucket en la Guía del usuario de Amazon Simple Storage Service.

A continuación, utilice la consola OpenSearch de servicio o los OpenSearch paneles de control para comprobar que el `lambda-s3-index` índice contiene dos documentos. También puede realizar una petición de búsqueda estándar:

```
GET https://domain-name/lambda-s3-index/_search?pretty
{
  "hits" : {
    "total" : 2,
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vTYXaWIBJWV_TTkEuSDg",
```

```
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.91",
          "message" : "GET /some-file.jpg",
          "timestamp" : "10/Oct/2000:14:56:14 -0700"
        }
      },
      {
        "_index" : "lambda-s3-index",
        "_type" : "_doc",
        "_id" : "vjYmaWIBJWV_TTkEuCAB",
        "_score" : 1.0,
        "_source" : {
          "ip" : "12.345.678.90",
          "message" : "PUT /some-file.jpg",
          "timestamp" : "10/Oct/2000:13:55:36 -0700"
        }
      }
    ]
  }
}
```

Cargar datos de streaming desde Amazon Kinesis Data Streams

Puede cargar datos de streaming desde Kinesis Data Streams OpenSearch a Service. Cuando llegan datos nuevos al flujo de datos, activan una notificación de eventos en Lambda que, a su vez, ejecuta el código personalizado para realizar la indexación. En esta sección, se incluye un código de muestra simple de Python.

Requisitos previos

Antes de continuar, debe contar con los siguientes recursos.

Requisito previo	Descripción
Amazon Kinesis Data Streams	Fuente de eventos de la función Lambda Para más información, consulte Kinesis Data Streams.
OpenSearch Dominio de servicio	Es el destino de los datos después de que la función Lambda los procesa. Para más información, consulte the section called “ Creación de dominios OpenSearch de servicio”.

Requisito previo	Descripción

Rol de IAM	Esta función debe tener permisos básicos OpenSearch de Servicio, Kinesis y Lambda, como los siguientes:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Action": [ "es:ESHttpPost", "es:ESHttpPut", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents", "kinesis:GetShardIterator", "kinesis:GetRecords", "kinesis:DescribeStream", "kinesis:ListStreams" ], "Resource": "*" } ] }`
	
	El rol debe tener la siguiente relación de confianza:
	
	`{ "Version": "2012-10-17", "Statement": [ { "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" } ] }`

Requisito previo	Descripción
	Para más información, consulte Creación de roles de IAM en la Guía del usuario de IAM.

Crear la función de Lambda

Siga las instrucciones de the section called “Crear el paquete de implementación de Lambda”, pero cree un directorio denominado `kinesis-to-opensearch` y utilice el siguiente código para `sample.py`:

```
import base64
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-kine-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        id = record['eventID']
        timestamp = record['kinesis']['approximateArrivalTimestamp']

        # Kinesis data is base64-encoded, so decode here
        message = base64.b64decode(record['kinesis']['data'])

        # Create the JSON document
        document = { "id": id, "timestamp": timestamp, "message": message }
```

```
        # Index the document
        r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return 'Processed ' + str(count) + ' items.'
```

Edite las variables para `region` y `host`.

Instale pip, si todavía no lo hizo, luego utilice los siguientes comandos para instalar las dependencias:

```
cd kinesis-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

A continuación, siga las instrucciones de the section called “Crear la función de Lambda”, pero especifique el rol de IAM de the section called “Requisitos previos” y la configuración siguiente para el desencadenador:

- Flujo de Kinesis: su flujo de Kinesis
- Tamaño del lote: 100
- Posición inicial: Trim horizon

Para más información, consulte ¿Qué es Amazon Kinesis Data Streams? en la Guía para desarrolladores de Amazon Kinesis Data Streams.

En este punto, dispone de un conjunto completo de recursos: una transmisión de datos de Kinesis, una función que se ejecuta después de que la transmisión reciba nuevos datos y los indexe, y un dominio de OpenSearch servicio para la búsqueda y la visualización.

Prueba de la función de Lambda

Después de crear la función, puede probarla al agregar un registro al flujo de datos mediante la AWS CLI:

```
aws kinesis put-record --stream-name test --data "My test data." --partition-key
 partitionKey1 --region us-west-1
```

A continuación, utilice la consola OpenSearch de servicio o los OpenSearch paneles de control para comprobar que `lambda-kine-index` contiene un documento. También puede utilizar la solicitud siguiente:

```
GET https://domain-name/lambda-kine-index/_search
{
  "hits" : [
    {
      "_index": "lambda-kine-index",
      "_type": "_doc",
      "_id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42",
      "_score": 1,
      "_source": {
        "timestamp": 1523648740.051,
        "message": "My test data.",
        "id":
 "shardId-000000000000:495835116157626994950129608214214566865294366804960870 42"
      }
    }
  ]
}
```

Carga de datos de streaming desde Amazon DynamoDB

Puede utilizarlos AWS Lambda para enviar datos a su dominio de OpenSearch servicio desde Amazon DynamoDB. Cuando llegan datos nuevos a la tabla de base de datos, activan una notificación de eventos en Lambda que, a su vez, ejecuta el código personalizado para realizar la indexación.

Requisitos previos

Antes de continuar, debe contar con los siguientes recursos.

Requisito previo	Descripción
Tabla de DynamoDB	La tabla contiene los datos de origen. Para más información, consulte Operaciones básicas en tablas de DynamoDB en la Guía para desarroll adores de Amazon DynamoDB.

Requisito previo	Descripción
	La tabla debe residir en la misma región que su dominio de OpenSearch servicio y tener una transmisión configurada como Nueva imagen. Para más información, consulte Habilitación de un flujo.
OpenSearch Dominio de servicio	Es el destino de los datos después de que la función de Lambda los procesa. Para más información, consulte the section called “ Creación de dominios OpenSearch de servicio”.

Requisito previo	Descripción
Rol de IAM	Esta función debe tener permisos básicos OpenSearch de ejecución de Servicios, DynamoDB y Lambda, como los siguientes: `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": ["es:ESHttpPost", "es:ESHttpPut", "dynamodb:DescribeStream", "dynamodb:GetRecords", "dynamodb:GetShardIterator", "dynamodb:ListStreams", "logs:CreateLogGroup", "logs:CreateLogStream", "logs:PutLogEvents"], "Resource": "*" }] }`  El rol debe tener la siguiente relación de confianza:  `{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Principal": { "Service": "lambda.amazonaws.com" }, "Action": "sts:AssumeRole" }] }`

Requisito previo	Descripción
	Para más información, consulte Creación de roles de IAM en la Guía del usuario de IAM.

Crear la función de Lambda

Siga las instrucciones de the section called “Crear el paquete de implementación de Lambda”, pero cree un directorio denominado `ddb-to-opensearch` y utilice el siguiente código para `sample.py`:

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

region = '' # e.g. us-east-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # the OpenSearch Service domain, e.g. https://search-mydomain.us-
west-1.es.amazonaws.com
index = 'lambda-index'
datatype = '_doc'
url = host + '/' + index + '/' + datatype + '/'

headers = { "Content-Type": "application/json" }

def handler(event, context):
    count = 0
    for record in event['Records']:
        # Get the primary key for use as the OpenSearch ID
        id = record['dynamodb']['Keys']['id']['S']

        if record['eventName'] == 'REMOVE':
            r = requests.delete(url + id, auth=awsauth)
        else:
            document = record['dynamodb']['NewImage']
            r = requests.put(url + id, auth=awsauth, json=document, headers=headers)
        count += 1
    return str(count) + ' records processed.'
```

Edite las variables para `region` y `host`.

Instale pip, si todavía no lo hizo, luego utilice los siguientes comandos para instalar las dependencias:

```
cd ddb-to-opensearch

pip install --target ./package requests
pip install --target ./package requests_aws4auth
```

A continuación, siga las instrucciones de the section called “Crear la función de Lambda”, pero especifique el rol de IAM de the section called “Requisitos previos” y la configuración siguiente para el desencadenador:

- Tabla: tabla de DynamoDB
- Tamaño del lote: 100
- Posición inicial: Trim horizon

Para más información, consulte Process New Items with DynamoDB Streams and Lambda en la Guía para desarrolladores de Amazon DynamoDB.

En este punto, dispone de un conjunto completo de recursos: una tabla de DynamoDB para los datos de origen, un flujo de cambios de DynamoDB en la tabla, una función que se ejecuta después de que los datos de origen cambien e indexa esos cambios, y un dominio de servicio para la búsqueda y la visualización. OpenSearch

Probar la función de Lambda

Después de crear la función, puede probarla al agregar un elemento a la tabla de DynamoDB mediante la AWS CLI:

```
aws dynamodb put-item --table-name test --item '{"director": {"S": "Kevin
 Costner"},"id": {"S": "00001"},"title": {"S": "The Postman"}}' --region us-west-1
```

A continuación, utilice la consola de OpenSearch servicio o los OpenSearch paneles de control para comprobar que contiene un documento. `lambda-index` También puede utilizar la solicitud siguiente:

```
GET https://domain-name/lambda-index/_doc/00001
```

```
{
    "_index": "lambda-index",
    "_type": "_doc",
    "_id": "00001",
    "_version": 1,
    "found": true,
    "_source": {
        "director": {
            "S": "Kevin Costner"
        },
        "id": {
            "S": "00001"
        },
        "title": {
            "S": "The Postman"
        }
    }
}
```

Carga de datos de streaming desde Amazon Data Firehose

Firehose admite el OpenSearch servicio como destino de entrega. Para obtener instrucciones sobre cómo cargar datos de streaming en el OpenSearch servicio, consulte Crear una transmisión de entrega de Kinesis Data Firehose OpenSearch y elegir un servicio para su destino en la Guía para desarrolladores de Amazon Data Firehose.

Antes de cargar datos en OpenSearch Service, es posible que deba realizar transformaciones en los datos. Para obtener más información acerca de cómo utilizar las funciones de Lambda para realizar esta tarea, consulte Amazon Kinesis Data Firehose Data Transformation en la misma guía.

Al configurar una transmisión de entrega, Firehose incluye una función de IAM con un solo clic que le proporciona el acceso a los recursos que necesita para enviar datos al OpenSearch Servicio, hacer copias de seguridad de los datos en Amazon S3 y transformar los datos con Lambda. Debido a la complejidad que supone la creación de ese rol manualmente, recomendamos utilizar el rol proporcionado.

Carga de datos de streaming desde Amazon CloudWatch

Puedes cargar datos de streaming desde CloudWatch Logs a tu dominio OpenSearch de servicio mediante una suscripción a CloudWatch Logs. Para obtener información sobre CloudWatch las suscripciones de Amazon, consulta Procesamiento en tiempo real de datos de registro con

suscripciones. Para obtener información sobre la configuración, consulte Transmisión de datos de CloudWatch registros a Amazon OpenSearch Service en la Guía para CloudWatch desarrolladores de Amazon.

Carga de datos de streaming desde AWS IoT

Puede enviar datos mediante el AWS IoT uso de reglas. Para obtener más información, consulta la OpenSearchacción en la Guía paraAWS IoT desarrolladores.

Carga de datos en Amazon OpenSearch Service con Logstash

La versión de código abierto de Logstash (Logstash OSS) proporciona una forma conveniente de utilizar la API masiva para cargar datos en un dominio de Amazon OpenSearch Service. El servicio admite todos los complementos de entrada de Logstash estándar, incluido el complemento de entrada de Amazon S3. OpenSearch Service soporta el complemento de salida logstash-output-opensearch, que soporta autenticación básica y credenciales de IAM. El complemento funciona con la versión 8.1 y versiones inferiores de Logstash OSS.

Configuración

La configuración de Logstash varía en función del tipo de autenticación que utiliza su dominio.

Independientemente del método de autenticación que utilice, debe configurar `ecs_compatibility` en `disabled` en la sección de salida del archivo de configuración. Logstash 8.0 introdujo un cambio revolucionario en el que se ejecutan todos los complementos en Modo de compatibilidad ECS de forma predeterminada. Debe anular el valor predeterminado para mantener el comportamiento heredado.

Configuración de control de acceso detallado

Si el dominio de OpenSearch Service utiliza un control de acceso detallado con autenticación HTTP básica, la configuración es similar a cualquier otro clúster de OpenSearch. Este archivo de configuración de ejemplo toma su entrada de la versión de código abierto de Filebeat (Filebeat OSS):

```
input {
  beats  {
    port => 5044
  }
}
```

```
output {
  opensearch {
    hosts       => "https://domain-endpoint:443"
    user        => "my-username"
    password    => "my-password"
    index       => "logstash-logs-%{+YYYY.MM.dd}"
    ecs_compatibility => disabled
    ssl_certificate_verification => false
  }
}
```

La configuración varía según la aplicación de Beats y el caso de uso, pero la configuración de Filebeat OSS podría verse así:

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    - /path/to/logs/dir/*.log
filebeat.config.modules:
  path: ${path.config}/modules.d/*.yml
  reload.enabled: false
setup.ilm.enabled: false
setup.ilm.check_exists: false
setup.template.settings:
  index.number_of_shards: 1
output.logstash:
  hosts: ["logstash-host:5044"]
```

Configuración de IAM

Si el dominio utiliza una política de acceso de dominio basada en IAM o un control de acceso detallado con un usuario maestro, debe firmar todas las solicitudes de OpenSearch Service con las credenciales de IAM. La siguiente política basada en identidades concede todas las solicitudes HTTP a los subrecursos de su dominio.

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

```
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:aws-account-id:domain/domain-name/*"
    }
  ]
}
```

Para configurar su configuración de Logstash, cambie su archivo de configuración para usar el complemento en su salida. Este ejemplo de archivo de configuración toma su entrada de archivos en un bucket de S3:

```
input {
  s3 {
    bucket => "my-s3-bucket"
    region => "us-east-1"
  }
}

output {
  opensearch {
    hosts => ["domain-endpoint:443"]
    auth_type => {
      type => 'aws_iam'
      aws_access_key_id => 'your-access-key'
      aws_secret_access_key => 'your-secret-key'
      region => 'us-east-1'
      }
      index  => "logstash-logs-%{+YYYY.MM.dd}"
      ecs_compatibility => disabled
  }
}
```

Si no desea proporcionar sus credenciales de IAM dentro del archivo de configuración, puede exportarlas (o ejecutarlas `aws configure`):

```
export AWS_ACCESS_KEY_ID="your-access-key"
export AWS_SECRET_ACCESS_KEY="your-secret-key"
export AWS_SESSION_TOKEN="your-session-token"
```

Si el dominio de OpenSearch Service está en una VPC, la máquina de Logstash OSS debe poder conectarse a la VPC y tener acceso al dominio a través de los grupos de seguridad de la VPC. Para

más información, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”.

Buscar datos en Amazon OpenSearch Service

Existen varios métodos habituales de búsqueda de documentos en Amazon OpenSearch Service, incluidas las búsquedas de URI y las búsquedas de cuerpos de la solicitud. OpenSearch Service ofrece funcionalidad adicional que mejora la experiencia de búsqueda, como paquetes personalizados, compatibilidad con SQL y búsqueda asincrónica. Para ver una referencia de la API de búsqueda de OpenSearch completa, consulte la documentación de OpenSearch.

> **Note**
>
> Las siguientes solicitudes de muestra funcionan con las API de OpenSearch. Algunas solicitudes podrían no funcionar con versiones anteriores de Elasticsearch.

Temas

Búsquedas de URI

Las búsquedas de identificador de recursos universal (URI) son la forma más sencilla de búsqueda. En una búsqueda de URI, hay que especificar la consulta como un parámetro de solicitud HTTP:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/_search?q=house
```

Una respuesta de muestra tendría el siguiente aspecto:


```
{
  "took": 25,
  "timed_out": false,
  "_shards": {
    "total": 10,
    "successful": 10,
    "skipped": 0,
    "failed": 0
  },
  "hits": {
    "total": {
      "value": 85,
      "relation": "eq",
    },
    "max_score": 6.6137657,
    "hits": [
      {
        "_index": "movies",
        "_type": "movie",
        "_id": "tt0077975",
        "_score": 6.6137657,
        "_source": {
          "directors": [
            "John Landis"
          ],
          "release_date": "1978-07-27T00:00:00Z",
          "rating": 7.5,
          "genres": [
            "Comedy",
            "Romance"
          ],
          "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTY2OTQxNTc1OF5BMl5BanBnXkFtZTYwNjA3NjI5._V1_SX400_.jpg",
          "plot": "At a 1962 College, Dean Vernon Wormer is determined to expel the
 entire Delta Tau Chi Fraternity, but those troublemakers have other plans for him.",
          "title": "Animal House",
          "rank": 527,
          "running_time_secs": 6540,
          "actors": [
```

```
            "John Belushi",
            "Karen Allen",
            "Tom Hulce"
          ],
          "year": 1978,
          "id": "tt0077975"
        }
      },
      ...
    ]
  }
}
```

De forma predeterminada, esta consulta realiza búsquedas en todos los campos de todos los índices para encontrar el término house. Para aportar más precisión a la búsqueda, especifique un índice (`movies`) y un campo de documento (`title`) en el URI:

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?q=title:house
```

Puede incluir parámetros adicionales en la solicitud, pero los parámetros compatibles proporcionan solo un pequeño subconjunto de opciones de búsqueda de OpenSearch. La siguiente solicitud devuelve 20 resultados (en vez de los 10 predeterminados) y los clasifica por año (en vez de clasificarlos por `_score`):

```
GET https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search?
q=title:house&size=20&sort=year:desc
```

Búsquedas de cuerpo de la solicitud

A fin de realizar búsquedas más complejas, utilice el cuerpo de la solicitud HTTP y el lenguaje específico de dominio (DSL) de OpenSearch para realizar las consultas. El DSL de la consulta permite especificar la gama completa de opciones de búsqueda de OpenSearch.

> **Note**
>
> No puede incluir caracteres especiales Unicode en el valor de un campo de texto, o el valor se analizará como varios valores separados por el carácter especial. Este análisis incorrecto puede provocar un filtrado involuntario de los documentos y comprometer potencialmente

el control sobre su acceso. Para más información, consulte Nota sobre los caracteres especiales Unicode en los campos de texto de la documentación de OpenSearch.

La siguiente consulta de `match` es similar al ejemplo de búsqueda de URI final:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "sort": {
    "year": {
      "order": "desc"
    }
  },
  "query": {
    "query_string": {
      "default_field": "title",
      "query": "house"
    }
  }
}
```

> **Note**
>
> La API de `_search` acepta `GET` y `POST` HTTP para búsquedas del cuerpo de la solicitud, pero no todos los clientes HTTP admiten la adición de un cuerpo de la solicitud a una solicitud `GET`. `POST` es la opción más universal.

En muchos casos, es posible que desee buscar varios campos, pero no todos los campos. Utilice la consulta `multi_match`:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title", "plot", "actors", "directors"]
    }
```

```
  }
}
```

Potenciar campos

Puede mejorar la relevancia de la búsqueda mediante la "potenciación" de ciertos campos. Los potenciadores son multiplicadores que dan mayor peso a las coincidencias en un campo que a las de otros campos. En el siguiente ejemplo, una coincidencia de john en el campo `title` tiene el doble de peso en `_score` que una coincidencia en el campo `plot` y cuatro veces más que otra en los campos `actors` o `directors`. El resultado es que películas como John Wick y John Carter están cerca de los primeros resultados de búsqueda y las películas protagonizadas por John Travolta están casi al final.

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "john",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Resaltado de resultados de búsqueda

La opción `highlight` indica a OpenSearch que devuelva un objeto adicional dentro de la matriz `hits` si la consulta coincide con uno o más campos:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
```

```
      "plot": {}
    }
  }
}
```

Si la consulta coincide con el contenido del campo `plot`, un acierto podría tener el siguiente aspecto:

```
{
  "_index": "movies",
  "_type": "movie",
  "_id": "tt0091541",
  "_score": 11.276199,
  "_source": {
    "directors": [
      "Richard Benjamin"
    ],
    "release_date": "1986-03-26T00:00:00Z",
    "rating": 6,
    "genres": [
      "Comedy",
      "Music"
    ],
    "image_url": "http://ia.media-imdb.com/images/M/
MV5BMTIzODEzODE2OF5BMl5BanBnXkFtZTcwNjQ3ODcyMQ@@._V1_SX400_.jpg",
    "plot": "A young couple struggles to repair a hopelessly dilapidated house.",
    "title": "The Money Pit",
    "rank": 4095,
    "running_time_secs": 5460,
    "actors": [
      "Tom Hanks",
      "Shelley Long",
      "Alexander Godunov"
    ],
    "year": 1986,
    "id": "tt0091541"
  },
  "highlight": {
    "plot": [
      "A young couple struggles to repair a hopelessly dilapidated <em>house</em>."
    ]
  }
}
```

De forma predeterminada, OpenSearch incluye la cadena coincidente entre etiquetas , proporciona hasta 100 caracteres de contexto en torno a la coincidencia y desglosa el contenido en frases mediante la identificación de signos de puntuación, espacios, tabulaciones y saltos de línea. Todas estas configuraciones son personalizables:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  },
  "highlight": {
    "fields": {
      "plot": {}
    },
    "pre_tags": "<strong>",
    "post_tags": "</strong>",
    "fragment_size": 200,
    "boundary_chars": ".,!? "
  }
}
```

API de recuento

Si no está interesado en el contenido de sus documentos y solo quiere saber el número de coincidencias, puede utilizar la API de `_count` en lugar de la API de `_search`. En la siguiente solicitud, se utiliza la consulta `query_string` para identificar comedias románticas:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_count
{
  "query": {
    "query_string": {
      "default_field": "genres",
      "query": "romance AND comedy"
    }
  }
}
```

Una respuesta de muestra tendría el siguiente aspecto:

```
{
  "count": 564,
  "_shards": {
    "total": 5,
    "successful": 5,
    "skipped": 0,
    "failed": 0
  }
}
```

Paginar los resultados de búsqueda

Si necesita mostrar un gran número de resultados de búsqueda, puede implementar la paginación usando varios métodos diferentes.

Punto en el tiempo

La característica de punto en el tiempo (PIT) es un tipo de búsqueda que permite ejecutar diferentes consultas en un conjunto de datos fijo en el tiempo. Este es el método de paginación preferido en OpenSearch, especialmente para la paginación profunda. Puede usar PIT con OpenSearch Service, versión 2.5 y versiones posteriores. Para más información sobre PITR, consulte ???.

Añada los parámetros **`from`** y **`size`**.

La forma más sencilla de paginar es con los parámetros `from` y `size`. La siguiente solicitud devuelve los resultados 20-39 de la lista de resultados de búsqueda indexada a cero:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/movies/_search
{
  "from": 20,
  "size": 20,
  "query": {
    "multi_match": {
      "query": "house",
      "fields": ["title^4", "plot^2", "actors", "directors"]
    }
  }
}
```

Para ver más información sobre la paginación de búsquedas, consulte Paginar los resultados en la documentación de OpenSearch.

Lenguaje de consulta de paneles

Puede utilizar el Lenguaje de consulta de paneles (DQL) para buscar datos y visualizaciones en los paneles de OpenSearch. DQL utiliza cuatro tipos de consultas principales: términos, booleano, fecha e intervalo y campo anidado.

Consulta de términos

Una consulta de términos requiere que se especifique el término que se busca.

Para llevar a cabo una consulta de términos, ingrese lo siguiente:

```
host:www.example.com
```

Consulta booleana

Puede utilizar los operadores booleanos `AND`, `or` y `not` para combinar varias consultas.

Para llevar a cabo una consulta booleana, pegue lo siguiente:

```
host.keyword:www.example.com and response.keyword:200
```

Consulta de fecha e intervalo

Puede utilizar una consulta de fecha e intervalo para buscar una fecha anterior o posterior a la consulta.

- > indica una búsqueda de una fecha posterior a la fecha especificada.
- < indica una búsqueda de una fecha anterior a la fecha especificada.

```
@timestamp > "2020-12-14T09:35:33"
```

Consulta de campo anidada

Si tiene un documento con campos anidados, debe especificar qué partes del documento desea recuperar. A continuación, se muestra un documento de muestra con campos anidados:

```
{"NBA players":[
    {"player-name": "Lebron James",
      "player-position": "Power forward",
      "points-per-game": "30.3"
    },
    {"player-name": "Kevin Durant",
      "player-position": "Power forward",
      "points-per-game": "27.1"
    },
    {"player-name": "Anthony Davis",
      "player-position": "Power forward",
      "points-per-game": "23.2"
    },
    {"player-name": "Giannis Antetokounmpo",
      "player-position": "Power forward",
      "points-per-game":"29.9"
    }
  ]
}
```

Para recuperar un campo específico con DQL, pegue lo siguiente:

```
NBA players: {player-name: Lebron James}
```

Para recuperar varios objetos del documento anidado, pegue lo siguiente:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo}
```

Para buscar dentro de un intervalo, pegue lo siguiente:

```
NBA players: {player-name: Lebron James} and NBA players: {player-name: Giannis
 Antetokounmpo and < 30}
```

Si el documento tiene un objeto anidado dentro de otro objeto, aún puede recuperar datos especificando todos los niveles. Para ello, pegue lo siguiente:

```
Top-Power-forwards.NBA players: {player-name:Lebron James}
```

Paquetes personalizados para Amazon OpenSearch Service

Amazon OpenSearch Service te permite cargar archivos de diccionarios personalizados, como palabras vacías y sinónimos, y también proporciona varios complementos opcionales preempaquetados que puedes asociar a tu dominio. El término genérico para referirse a ambos tipos de archivos es paquetes.

Los archivos de diccionario mejoran los resultados de búsqueda OpenSearch al indicar que hay que ignorar determinadas palabras muy frecuentes o tratar términos como «crema congelada», «helado» y «helado» como equivalentes. También pueden mejorar la derivación, como sucede en el complemento Japanese (kuromoji) Analysis.

Los complementos opcionales pueden proporcionar funciones adicionales a su dominio. Por ejemplo, puede usar el complemento Amazon Personalize para obtener resultados de búsqueda personalizados. Los complementos opcionales utilizan el tipo de paquete `ZIP-PLUGIN`. Para obtener más información sobre los complementos opcionales, consulte the section called “Complementos por versión de motor”.

Temas

Requisitos de permisos de paquetes

Los usuarios sin acceso de administrador requieren ciertas acciones AWS Identity and Access Management (IAM) para poder administrar los paquetes:

- `es:CreatePackage`- crear un paquete en una región de OpenSearch servicio
- `es:DeletePackage`- eliminar un paquete de una región OpenSearch de servicio
- `es:AssociatePackage`: asociar un paquete a un dominio
- `es:DissociatePackage`: disociar un paquete de un dominio

También necesita permisos en la ruta del bucket de Amazon S3 u objeto donde reside el paquete personalizado.

Otorgue todos los permisos en IAM, no en la política de acceso al dominio. Para más información, consulte the section called “Identity and Access Management”.

Carga de paquetes en Amazon S3

En esta sección se explica cómo cargar paquetes de diccionarios personalizados, ya que los paquetes de complementos opcionales ya vienen preinstalados. Antes de poder asociar un diccionario personalizado a un dominio, debe cargarlo en un bucket de Amazon S3. Para ver las instrucciones, consulte Carga de objetos en la Guía del usuario de Amazon Simple Storage Service. No es necesario cargar los complementos admitidos.

Si su diccionario contiene información confidencial, especifique el cifrado del lado del servidor con claves gestionadas por S3 cuando lo cargue. OpenSearch El servicio no puede acceder a los archivos de S3 que protejas con una clave. AWS KMS

Después de cargar el archivo, tome nota de su ruta de S3. El formato de la ruta es `s3://`*`bucket-name`*`/`*`file-path`*`/`*`file-name`*.

Puede utilizar el siguiente archivo de sinónimos para fines de prueba. Guárdelo como `synonyms.txt`.

```
danish, croissant, pastry
ice cream, gelato, frozen custard
sneaker, tennis shoe, running shoe
basketball shoe, hightop
```

Algunos diccionarios, como los diccionarios Hunspell, utilizan varios archivos y requieren sus propios directorios en el sistema de archivos. En este momento, el OpenSearch servicio solo admite diccionarios de un solo archivo.

Importación y asociación de paquetes

La consola es la forma más sencilla de importar un diccionario personalizado a OpenSearch Service. Al importar un diccionario de Amazon S3, OpenSearch Service almacena su propia copia del paquete y la cifra automáticamente mediante AES-256 con OpenSearch claves administradas por el servicio.

Los complementos opcionales ya vienen preinstalados en el OpenSearch Servicio, por lo que no es necesario que los cargue usted mismo, pero sí que tiene que asociar un complemento a un dominio. Los complementos disponibles aparecen en la pantalla Paquetes de la consola.

Importa y asocia un paquete a un dominio con el AWS Management Console

1. En la consola OpenSearch de Amazon Service, selecciona Paquetes.
2. Seleccione Importar paquete.
3. Asigne un nombre descriptivo al diccionario personalizado.
4. Proporcione la ruta de S3 al archivo y, a continuación, seleccione Enviar.
5. Vuelva a la pantalla Paquetes.
6. Cuando el estado del paquete sea Disponible, elíjalo. Los complementos opcionales estarán Disponibles automáticamente.
7. Seleccione Asociar a un dominio.
8. Seleccione un dominio y, a continuación, seleccione Asociar.
9. En el panel de navegación, seleccione el dominio y, a continuación, vaya a la pestaña Paquetes.
10. Si el paquete es un diccionario personalizado, anote el ID cuando el paquete esté disponible. `analyzers/`*`id`*Utilízala como ruta del archivo en las solicitudes para OpenSearch.

Como alternativa, puede utilizar los AWS CLI SDK o la API de configuración para importar y asociar paquetes. Para obtener más información, consulta la Referencia de AWS CLI comandos y la Referencia de la API de Amazon OpenSearch Service.

Uso de paquetes con OpenSearch

En esta sección se explica cómo usar ambos tipos de paquetes: diccionarios personalizados y complementos opcionales.

Uso de diccionarios personalizados

Después de asociar un archivo a un dominio, puede usarlo en parámetros como `synonyms_path`, `stopwords_path` y `user_dictionary` al crear generadores de tokens y filtros de token. El parámetro exacto varía según el objeto. Varios objetos admiten `synonyms_path` y `stopwords_path`, pero `user_dictionary` es exclusivo del complemento kuromoji.

Para el complemento IK (chino) Analysis, puede cargar un archivo de diccionario personalizado en forma de paquete personalizado y asociarlo a un dominio, y el complemento lo recogerá

automáticamente sin necesidad de parámetro `user_dictionary`. Si se trata de un archivo de sinónimos, utilice el parámetro `synonyms_path`.

El siguiente ejemplo agrega un archivo de sinónimos a un nuevo índice:

```
PUT my-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "my_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["my_filter"]
          }
        },
        "filter": {
          "my_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F111111111",
            "updateable": true
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "standard",
        "search_analyzer": "my_analyzer"
      }
    }
  }
}
```

Esta solicitud crea un analizador personalizado para el índice que utiliza el generador de tokens estándar y un filtro de token de sinónimos.

- Los generadores de tokens dividen las secuencias de caracteres en tokens (normalmente palabras) en función de algún conjunto de reglas. El ejemplo más simple es el generador de tokens

de espacios en blanco, que divide los caracteres anteriores en un token cada vez que encuentra un carácter de espacio en blanco. Un ejemplo más complejo es el generador de tokens estándar, que utiliza un conjunto de reglas gramaticales para funcionar en muchos idiomas.

- Los filtros de tokens agregan, modifican o eliminan tokens. Por ejemplo, un filtro de token de sinónimos agrega tokens cuando encuentra una palabra en la lista de sinónimos. El filtro de tokens de palabras vacías elimina los tokens cuando encuentra una palabra en la lista de palabras vacías.

Esta solicitud también agrega un campo de texto (`description`) al mapeo e indica OpenSearch que se use el nuevo analizador como analizador de búsqueda. Puede ver que todavía utiliza el analizador estándar como analizador de índices.

Por último, tenga en cuenta la línea `"updateable": true` en el filtro de token. Este campo solo se aplica a los analizadores de búsqueda, no a los analizadores de índice, y es crítico si luego desea actualizar el analizador de búsqueda de forma automática.

Con fines de prueba, agregue algunos documentos al índice:

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "description": "ice cream" }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "description": "croissant" }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "description": "tennis shoe" }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "description": "hightop" }
```

A continuación, use un sinónimo para buscarlos:

```
GET my-index/_search
{
  "query": {
    "match": {
      "description": "gelato"
    }
  }
}
```

En este caso, OpenSearch devuelve la siguiente respuesta:

```
{
  "hits": {
    "total": {
      "value": 1,
      "relation": "eq"
    },
    "max_score": 0.99463606,
    "hits": [{
      "_index": "my-index",
      "_type": "_doc",
      "_id": "1",
      "_score": 0.99463606,
      "_source": {
        "description": "ice cream"
      }
    }]
  }
}
```

> **Tip**
>
> Los archivos de diccionario utilizan espacio de montón de Java proporcional a su tamaño. Por ejemplo, un archivo de diccionario de 2 GiB podría consumir 2 GiB de espacio de montón en un nodo. Si utiliza archivos de gran tamaño, asegúrese de que los nodos tengan suficiente espacio en el montón para acomodarlos. Monitoree la métrica `JVMMemoryPressure` y escale el clúster según sea necesario.

Uso de complementos opcionales

OpenSearch El servicio le permite asociar OpenSearch complementos opcionales preinstalados para usarlos con su dominio. Un paquete de complementos opcional es compatible con una OpenSearch versión específica y solo se puede asociar a los dominios con esa versión. La lista de paquetes disponibles para su dominio incluye todos los complementos compatibles con la versión de su dominio. Después de asociar un complemento a un dominio, comienza un proceso de instalación en el dominio. Luego, puedes hacer referencia al complemento y usarlo cuando realices solicitudes al OpenSearch Servicio.

Asociar y disociar un complemento requiere una implementación azul/verde. Para más información, consulte the section called “Cambios que suelen causar implementaciones azul/verde”.

Los complementos opcionales incluyen analizadores de idioma y resultados de búsqueda personalizados. Por ejemplo, el complemento Amazon Personalize Search Ranking utiliza machine learning para personalizar los resultados de búsqueda para sus clientes. Para obtener más información sobre este complemento, consulte Personalización de los resultados de búsqueda desde OpenSearch. Para ver una lista de todos los complementos admitidos, consulte the section called "Complementos por versión de motor".

Complemento Sudachi

En el caso del complemento Sudachi, al volver a asociar un archivo de diccionario, no se refleja inmediatamente en el dominio. El diccionario se actualiza cuando se ejecuta la siguiente implementación azul/verde en el dominio como parte de un cambio de configuración u otra actualización. Como alternativa, puedes crear un paquete nuevo con los datos actualizados, crear un índice nuevo con este paquete nuevo, volver a indexar el índice existente en el nuevo índice y, a continuación, eliminar el índice anterior. Si prefiere utilizar el enfoque de reindexación, utilice un alias de índice para que no se interrumpa el tráfico.

Además, el complemento Sudachi solo admite los diccionarios binarios de Sudachi, que se pueden cargar con la CreatePackageoperación de API. Para obtener información sobre el diccionario del sistema prediseñado y el proceso de compilación de diccionarios de usuario, consulte Documentación de Sudachi.

En el siguiente ejemplo, se muestra cómo utilizar los diccionarios de sistema y de usuario con el tokenizador de Sudachi. Debe cargar estos diccionarios como paquetes personalizados con el tipo `TXT-DICTIONARY` y proporcionar sus ID de paquete en la configuración adicional.

```
PUT sudachi_sample
{
  "settings": {
    "index": {
      "analysis": {
        "tokenizer": {
          "sudachi_tokenizer": {
            "type": "sudachi_tokenizer",
            "additional_settings": "{\"systemDict\": \"<system-dictionary-package-
id>\",\"userDict\": [\"<user-dictionary-package-id>\"]}"
        }
        },
        "analyzer": {
          "sudachi_analyzer": {
            "filter": ["my_searchfilter"],
```

```
            "tokenizer": "sudachi_tokenizer",
            "type": "custom"
          }
        },
        "filter":{
          "my_searchfilter": {
            "type": "sudachi_split",
            "mode": "search"
          }
        }
      }
    }
  }
}
```

Actualización de paquetes

En esta sección solo se explica cómo actualizar un paquete de diccionarios personalizados, ya que los paquetes de complementos opcionales ya están actualizados. Al cargar una nueva versión de un diccionario en Amazon S3, el paquete no se actualiza automáticamente en Amazon OpenSearch Service. OpenSearch El servicio almacena su propia copia del archivo, por lo que si subes una nueva versión a S3, tendrás que actualizarla manualmente.

Cada uno de los dominios asociados también almacena su propia copia del archivo. Para mantener el comportamiento de búsqueda predecible, los dominios siguen utilizando la versión actual del paquete hasta que los actualice explícitamente. Para actualizar un paquete personalizado, modifique el archivo Amazon S3 Control, actualice el paquete en OpenSearch Service y, a continuación, aplique la actualización.

Actualice un paquete con AWS Management Console

1. En la consola OpenSearch de servicio, elija Paquetes.
2. Seleccione un paquete y luego Actualizar.
3. Proporcione la ruta de S3 al archivo y, a continuación, seleccione Actualizar paquete.
4. Vuelva a la pantalla Paquetes.
5. Cuando el estado del paquete cambie a Disponible, selecciónelo. A continuación, seleccione uno o más dominios asociados, Aplicar actualización y confirme. Espere a que el estado de asociación cambie a Activo.
6. Los siguientes pasos variarán en función de cómo haya configurado los índices:

- Si tu dominio ejecuta OpenSearch Elasticsearch 7.8 o una versión posterior y solo usa analizadores de búsqueda con el campo actualizable establecido en true, no necesitas realizar ninguna otra acción. OpenSearch El servicio actualiza automáticamente tus índices mediante la API _plugins/_refresh_search_analyzers.
- Si tu dominio ejecuta Elasticsearch 7.7 o una versión anterior, usa analizadores de índices o no usa el campo, consulta. `updateable` the section called “Actualizaciones manuales de índices para diccionarios”

Aunque la consola es el método más sencillo, también puedes usar los SDK o la AWS CLI API de configuración para actualizar los paquetes de servicios. OpenSearch Para obtener más información, consulta la Referencia de AWS CLI comandos y la Referencia de la API de Amazon OpenSearch Service.

Actualiza un paquete con el AWS SDK

En lugar de actualizar de forma manual un paquete en la consola, puede utilizar los SDK para automatizar el proceso de actualización. El siguiente script de Python de ejemplo carga un nuevo archivo de paquete en Amazon S3, actualiza el paquete en OpenSearch Service y aplica el nuevo paquete al dominio especificado. Tras confirmar que la actualización se ha realizado correctamente, realiza un ejemplo de llamada para OpenSearch demostrar que se han aplicado los nuevos sinónimos.

Debe proporcionar valores para `host`, `region`, `file_name`, `bucket_name`, `s3_key`, `package_id`, `domain_name` y `query`.

```
from requests_aws4auth import AWS4Auth
import boto3
import requests
import time
import json
import sys

host = ''  # The OpenSearch domain endpoint with https:// and a trailing slash. For
 example, https://my-test-domain.us-east-1.es.amazonaws.com/
region = ''  # For example, us-east-1
file_name = ''  # The path to the file to upload
bucket_name = ''  # The name of the S3 bucket to upload to
s3_key = ''  # The name of the S3 key (file name) to upload to
package_id = ''  # The unique identifier of the OpenSearch package to update
```

```
domain_name = ''  # The domain to associate the package with
query = ''  # A test query to confirm the package has been successfully updated

service = 'es'
credentials = boto3.Session().get_credentials()
client = boto3.client('opensearch')
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key,
                   region, service, session_token=credentials.token)


def upload_to_s3(file_name, bucket_name, s3_key):
    """Uploads file to S3"""
    s3 = boto3.client('s3')
    try:
        s3.upload_file(file_name, bucket_name, s3_key)
        print('Upload successful')
        return True
    except FileNotFoundError:
        sys.exit('File not found. Make sure you specified the correct file path.')


def update_package(package_id, bucket_name, s3_key):
    """Updates the package in OpenSearch Service"""
    print(package_id, bucket_name, s3_key)
    response = client.update_package(
        PackageID=package_id,
        PackageSource={
            'S3BucketName': bucket_name,
            'S3Key': s3_key
        }
    )
    print(response)


def associate_package(package_id, domain_name):
    """Associates the package to the domain"""
    response = client.associate_package(
        PackageID=package_id, DomainName=domain_name)
    print(response)
    print('Associating...')


def wait_for_update(domain_name, package_id):
    """Waits for the package to be updated"""
```

```
    response = client.list_packages_for_domain(DomainName=domain_name)
    package_details = response['DomainPackageDetailsList']
    for package in package_details:
        if package['PackageID'] == package_id:
            status = package['DomainPackageStatus']
            if status == 'ACTIVE':
                print('Association successful.')
                return
            elif status == 'ASSOCIATION_FAILED':
                sys.exit('Association failed. Please try again.')
            else:
                time.sleep(10)  # Wait 10 seconds before rechecking the status
                wait_for_update(domain_name, package_id)


def sample_search(query):
    """Makes a sample search call to OpenSearch"""
    path = '_search'
    params = {'q': query}
    url = host + path
    response = requests.get(url, params=params, auth=awsauth)
    print('Searching for ' + '"' + query + '"')
    print(response.text)
```

> **Note**
>
> Si recibes un error que indica que no se ha encontrado el paquete al ejecutar el script AWS CLI, es probable que Boto3 esté utilizando la región especificada en ~/.aws/config, que no es la región en la que se encuentra tu bucket de S3. Puede ejecutar `aws configure` y especificar la región correcta o agregar explícitamente la región al cliente:
>
> ```
> client = boto3.client('opensearch', region_name='us-east-1')
> ```

Actualizaciones manuales de índices para diccionarios

Las actualizaciones manuales de índices solo se aplican a los diccionarios personalizados, no a los complementos opcionales. Para utilizar un diccionario actualizado, debe actualizar de forma manual los índices, si cumple alguna de las siguientes condiciones:

- El dominio ejecuta Elasticsearch 7.7 o anterior.

- Utiliza paquetes personalizados como analizadores de índices.
- Utiliza paquetes personalizados como analizadores de búsqueda, pero no incluye el campo actualizable.

Para actualizar los analizadores con los nuevos archivos de paquete, dispone de dos opciones:

- Cierre y abra los índices que desee actualizar:

```
POST my-index/_close
POST my-index/_open
```

- Vuelva a indexar los índices. Primero, cree un índice que utilice el archivo de sinónimos actualizado (o un archivo completamente nuevo). Tenga en cuenta que solo se admite UTF-8.

```
PUT my-new-index
{
  "settings": {
    "index": {
      "analysis": {
        "analyzer": {
          "synonym_analyzer": {
            "type": "custom",
            "tokenizer": "standard",
            "filter": ["synonym_filter"]
          }
        },
        "filter": {
          "synonym_filter": {
            "type": "synonym",
            "synonyms_path": "analyzers/F222222222"
          }
        }
      }
    }
  },
  "mappings": {
    "properties": {
      "description": {
        "type": "text",
        "analyzer": "synonym_analyzer"
      }
    }
```

```
  }
}
```

Luego vuelva a indexar el índice anterior con ese nuevo índice:

```
POST _reindex
{
  "source": {
    "index": "my-index"
  },
  "dest": {
    "index": "my-new-index"
  }
}
```

Si actualiza con frecuencia los analizadores de índices, utilice alias de índice para mantener una ruta coherente al índice más reciente:

```
POST _aliases
{
  "actions": [
    {
      "remove": {
        "index": "my-index",
        "alias": "latest-index"
      }
    },
    {
      "add": {
        "index": "my-new-index",
        "alias": "latest-index"
      }
    }
  ]
}
```

Si no necesita el índice anterior, elimínelo:

```
DELETE my-index
```

Disociación y eliminación de paquetes

Si disocia un paquete de un dominio, ya sea un diccionario personalizado o un complemento opcional, ya no podrá usar ese paquete cuando cree nuevos índices. Una vez disociado un paquete, los índices existentes que lo utilizaban ya no pueden usarlo. Debe eliminar el paquete de cualquier índice antes de poder disociarlo; de lo contrario, la disociación fallará.

La consola es la forma más sencilla de disociar un paquete de un dominio y eliminarlo del Servicio. OpenSearch Eliminar un paquete del OpenSearch Servicio no lo elimina de su ubicación original en Amazon S3.

Disociación de un paquete de un dominio con la AWS Management Console

1. Visite https://aws.amazon.com y, a continuación, seleccione Iniciar sesión en la consola.
2. En Analytics, selecciona Amazon OpenSearch Service.
3. En el panel de navegación, elija el dominio y, a continuación, elija la pestaña Paquetes.
4. Seleccione un paquete, Acciones y, a continuación, seleccione Disociar. Confirme su elección.
5. Espere a que el paquete desaparezca de la lista. Puede que tenga que actualizar el navegador.
6. Si desea utilizar el paquete con otros dominios, deténgase aquí. Para continuar con la eliminación del paquete (si es un diccionario personalizado), seleccione Paquetes en el panel de navegación.
7. Seleccione el paquete y elija Eliminar.

También puede utilizar los SDK o la AWS CLI API de configuración para disociar y eliminar los paquetes. Para obtener más información, consulta la Referencia de AWS CLI comandos y la Referencia de la API de Amazon OpenSearch Service.

Consultar los datos de Amazon OpenSearch Service con SQL

Puede utilizar SQL para consultar su Amazon OpenSearch Service, en lugar de utilizar la Consulta de OpenSearch DSL con base en JSON. Consultar con SQL es útil si ya está familiarizado con el lenguaje o si desea integrar su dominio en una aplicación que lo utilice.

Utilice la siguiente tabla para buscar la versión del complemento SQL compatible con cada versión de OpenSearch y Elasticsearch.

OpenSearch

Versión de OpenSearch	Versión del complemento de SQL	Características notables
2.11.0	2.11.0.0	Añada compatibilidad con el lenguaje y las consultas de PPL
2.9.0	2.9.0.0	Se añadió el conector Spark y admite funciones de tabla y ProMQL
2.7.0	2.7.0.0	Se añadió API `datasource`
2.5.0	2.5.0.0	
2.3.0	2.3.0.0	Se añadieron funciones de fecha y hora `maketime` y `makedate`
1.3.0	1.3.0.0	Admite tamaño límite de consulta predeterminado y cláusula IN al seleccionar de una lista de valores
1.2.0	1.2.0.0	Se añadió nuevo protocolo para el formato de respuesta de visualización
1.1.0	1.1.0.0	Admite la función de coincidencia como filtro en SQL y PPL
1.0.0	1.0.0.0	Admite la consulta de un flujo de datos

Open Distro para Elasticsearch

Versión de Elasticsearch	Versión del complemento de SQL	Características notables
7.10	1.13.0	NULL FIRST y LAST para funciones de ventana, función CAST(), comandos SHOW y DESCRIBE

Versión de Elasticsearch	Versión del complemento de SQL	Características notables
7.9	1.11.0	Se añadieron funciones de fecha/hora adicionales, palabra clave ORDER BY
7.8	1.9.0	
7.7	1.8.0	
7.3	1.3.0	Varios operadores de cadena y número
7.1	1.1.0	

La compatibilidad con SQL está disponible en los dominios que ejecutan OpenSearch o Elasticsearch 6.5 o versiones posteriores. La documentación completa del complemento SQL está disponible en la Documentación de OpenSearch.

Ejemplo de llamada

Para consultar los datos con SQL, envíe solicitudes HTTP a `_sql` con el formato siguiente:

```
POST domain-endpoint/_plugins/_sql
{
  "query": "SELECT * FROM my-index LIMIT 50"
}
```

> **Note**
>
> Si el dominio ejecuta Elasticsearch en lugar de OpenSearch, el formato es `_opendistro/_sql`.

Notas y diferencias

Las llamadas a `_plugins/_sql` incluyen los nombres de índice en el cuerpo de la solicitud y, por lo tanto, se aplican las mismas consideraciones de política de acceso que en las operaciones bulk,

mget y msearch. Como siempre, siga el principio de privilegios mínimos cuando conceda permisos a las operaciones de API.

Para consideraciones de seguridad relacionadas con la utilización de SQL con el control de acceso detallado, consulte the section called “Control de acceso detallado”.

El complemento SQL de OpenSearch incluye muchas opciones de configuración ajustables. En OpenSearch Service, utilice la ruta `_cluster/settings`, en lugar de la ruta de configuración del complemento (`_plugins/_query/settings`):

```
PUT _cluster/settings
{
  "transient" : {
    "plugins.sql.enabled" : true
  }
}
```

En los dominios de Elasticsearch heredados, reemplace `plugins` con `opendistro`:

```
PUT _cluster/settings
{
  "transient" : {
    "opendistro.sql.enabled" : true
  }
}
```

SQL Workbench

SQL Workbench es una interfaz de usuario de OpenSearch Dashboards que permite ejecutar consultas SQL bajo demanda, traducir SQL en su equivalente REST y ver y guardar resultados como texto, JSON, JDBC o CSV. Para más información, consulte Query Workbench.

CLI SQL

La CLI SQL es una aplicación Python independiente que se puede iniciar con el comando `opensearchsql`. Para obtener información sobre los pasos para instalar, configurar y utilizar, consulte SQL CLI.

Controlador JDBC

El controlador de Java Database Connectivity (JDBC) permite integrar dominios de OpenSearch Service en sus aplicaciones favoritas de inteligencia empresarial (BI). Para descargar el controlador, haga clic aquí. Para más información, consulte el repositorio de GitHub.

En las tablas siguientes, se resume la compatibilidad de las versiones para el controlador.

OpenSearch

Versión de OpenSearch	Versión del controlador JDBC
2.11	1.1.0.1
2.9	1.1.0.1
2.7	1.1.0.1
2,5	1.1.0.1
2.3	1.1.0.1
1.3	1.1.0.1
1.2	1.1.0.1
1.1	1.1.0.1
1.0	1.1.0.1

Open Distro para Elasticsearch

Versión de Elasticsearch	Versión del controlador JDBC
7.10	1.13.0
7.9	1.11.0
7.8	1.9.0
7.7	1.8.0

Versión de Elasticsearch	Versión del controlador JDBC
7.4	1.4.0
7.1	1.0.0
6.8	0.9.0
6.7	0.9.0
6.5	0.9.0

Controlador ODBC

El controlador de Open Database Connectivity (ODBC) es un controlador de ODBC de solo lectura para Windows y macOS que permite conectar aplicaciones de inteligencia empresarial y visualización de datos como Microsoft Excel al complemento SQL.

Puede descargar un ejemplo de archivo de controlador que funcione en la página de artefactos de OpenSearch. Para obtener más información sobre cómo instalar el controlador, consulte el Repositorio SQL en GitHub.

Búsqueda k-Nearest Neighbor (k-NN) en Amazon OpenSearch Service

Con la sigla en inglés de su algoritmo asociado vecinos más cercanos de k, k-NN para Amazon OpenSearch Service permite buscar puntos en un espacio vectorial y encontrar los “vecinos más cercanos” de esos puntos por distancia euclidiana o similitud de coseno. Los casos de uso incluyen recomendaciones (por ejemplo, una función de “otras canciones que podrían gustarte” en una aplicación de música), reconocimiento de imágenes y detección de fraude.

Utilice las siguientes tablas para encontrar la versión del complemento k-NN que se ejecuta en un dominio de Amazon OpenSearch Service. Cada versión del complemento k-NN corresponde a una versión de OpenSearch o Elasticsearch.

OpenSearch

Versión de OpenSearch	Versión del complemento k-NN	Características notables
2.11	2.11.0.0	Se agregó soporte para consultas `ignore_unmapped` en k-NN
2.9	2.9.0.0	Se implementaron vectores de bytes k-NN y un filtrado eficiente con el motor Faiss
2.7	2.7.0.0	
2,5	2.5.0.0	Se amplió SystemIndexPlugin para el índice de sistema del modelo k-NN. Se añadieron extensiones de archivo específicas de Lucene al núcleo de HybridFS
2.3	2.3.0.0	
1.3	1.3.0.0	
1.2	1.2.0.0	Se agregó compatibilidad con la biblioteca Faiss
1.1	1.1.0.0	
1.0	1.0.0.0	API de REST renombradas mientras admite la compatibilidad con versiones anteriores, espacio de nombres renombrado de `opendistro` a `opensearch`

Elasticsearch

Versión de Elasticsearch	Versión del complemento k-NN	Características notables
7.1	1.3.0.0	Distancia euclidiana
7.4	1.4.0.0	

Versión de Elasticsearch	Versión del complemento k-NN	Características notables
7.7	1.8.0.0	Similitud coseno
7.8	1.9.0.0	
7.9	1.11.0.0	Periodo de preparación de la API, puntuación personalizada
7.10	1.13.0.0	Distancia de Hamming, distancia de norma L1, scripting Painless

La documentación completa sobre el complemento k-NN está disponible en la documentación de OpenSearch. Para obtener información de fondo sobre el algoritmo de k vecinos más cercanos, consulte Wikipedia.

Introducción a k-NN

Para utilizar k-NN, debe crear un índice con la configuración `index.knn` y agregar uno o más campos del tipo de datos `knn_vector`.

```
PUT my-index
{
  "settings": {
    "index.knn": true
  },
  "mappings": {
    "properties": {
      "my_vector1": {
        "type": "knn_vector",
        "dimension": 2
      },
      "my_vector2": {
        "type": "knn_vector",
        "dimension": 4
      }
    }
  }
```

```
}
```

El tipo de datos `knn_vector` admite una sola lista de hasta 10 000 flotadores, con el número de flotadores definido por el parámetro `dimension` requerido. Después de crear el índice, agregue algunos datos.

```
POST _bulk
{ "index": { "_index": "my-index", "_id": "1" } }
{ "my_vector1": [1.5, 2.5], "price": 12.2 }
{ "index": { "_index": "my-index", "_id": "2" } }
{ "my_vector1": [2.5, 3.5], "price": 7.1 }
{ "index": { "_index": "my-index", "_id": "3" } }
{ "my_vector1": [3.5, 4.5], "price": 12.9 }
{ "index": { "_index": "my-index", "_id": "4" } }
{ "my_vector1": [5.5, 6.5], "price": 1.2 }
{ "index": { "_index": "my-index", "_id": "5" } }
{ "my_vector1": [4.5, 5.5], "price": 3.7 }
{ "index": { "_index": "my-index", "_id": "6" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 10.3 }
{ "index": { "_index": "my-index", "_id": "7" } }
{ "my_vector2": [2.5, 3.5, 5.6, 6.7], "price": 5.5 }
{ "index": { "_index": "my-index", "_id": "8" } }
{ "my_vector2": [4.5, 5.5, 6.7, 3.7], "price": 4.4 }
{ "index": { "_index": "my-index", "_id": "9" } }
{ "my_vector2": [1.5, 5.5, 4.5, 6.4], "price": 8.9 }
```

A continuación, puede buscar los datos mediante el tipo de consulta `knn`.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  }
}
```

En este caso, k es el número de vecinos que desea que devuelva la consulta, pero también debe incluir la opción `size`. De lo contrario, obtendrá k resultados para cada partición (y cada segmento) en lugar de k resultados para toda la consulta. k-NN admite un valor de k máximo de 10 000.

Si mezcla la consulta knn con otras cláusulas, es posible que reciba menos resultados k. En este ejemplo, la cláusula `post_filter` reduce el número de resultados de 2 a 1.

```
GET my-index/_search
{
  "size": 2,
  "query": {
    "knn": {
      "my_vector2": {
        "vector": [2, 3, 5, 6],
        "k": 2
      }
    }
  },
  "post_filter": {
    "range": {
      "price": {
        "gte": 6,
        "lte": 10
      }
    }
  }
}
```

Si necesita gestionar un gran volumen de consultas y, al mismo tiempo, mantener un rendimiento óptimo, puede utilizar la API `_msearch` para crear una búsqueda masiva con JSON y enviar una única solicitud para realizar varias búsquedas:

```
GET _msearch
{ "index": "my-index"}
{ "query": { "knn": {"my_vector2":{"vector": [2, 3, 5, 6],"k":2 }} } }
{ "index": "my-index", "search_type": "dfs_query_then_fetch"}
{ "query": { "knn": {"my_vector1":{"vector": [2, 3],"k":2 }} } }
```

En el siguiente video se muestra cómo configurar búsquedas vectoriales masivas para consultas K-NN.

Diferencias, ajuste y limitaciones de k-NN

OpenSearch permite modificar todas las configuraciones de k-NN mediante la API `_cluster/settings`. En OpenSearch Service, puede cambiar todas las configuraciones, excepto `knn.memory.circuit_breaker.enabled` y `knn.circuit_breaker.triggered`. Las estadísticas k-NN se incluyen como Métricas de Amazon CloudWatch.

En particular, verifique la métrica `KNNGraphMemoryUsage` en cada nodo de datos con respecto a la estadística `knn.memory.circuit_breaker.limit` y la RAM disponible para el tipo de instancia. OpenSearch Service utiliza la mitad de la RAM de una instancia para la pila de Java (hasta un tamaño de pila de 32 GiB). De forma predeterminada, k-NN utiliza hasta el 50 % de la mitad restante, por lo que un tipo de instancia con 32 GiB de RAM puede acomodar 8 GiB de gráficos (32 * 0,5 * 0,5). El rendimiento puede verse afectado si el uso de la memoria gráfica supera este valor.

No puede migrar un índice k-NN a un almacenamiento UltraWarm o almacenamiento en frío si el índice utiliza k-NN aproximado (`"index.knn": true`). Si `index.knn` está configurado en `false` (k-NN exacto), aún puede mover el índice a otros niveles de almacenamiento.

Búsqueda entre clústeres en Amazon Service OpenSearch

La búsqueda entre clústeres en Amazon OpenSearch Service te permite realizar consultas y agregaciones en varios dominios conectados. A menudo tiene más sentido usar varios dominios más pequeños en lugar de un solo dominio grande, especialmente cuando se ejecutan distintos tipos de cargas de trabajo.

Los dominios específicos de la carga de trabajo permiten realizar las siguientes tareas:

- Optimice cada dominio mediante la elección de tipos de instancia para cargas de trabajo específicas.
- Establezca límites de aislamiento de fallas entre cargas de trabajo. Esto significa que si una de las cargas de trabajo devuelve un error, el error queda contenido dentro de ese dominio específico y no afecta a las demás cargas de trabajo.
- Escale más fácilmente entre dominios.

La búsqueda entre clústeres es compatible con OpenSearch los paneles, por lo que puede crear visualizaciones y paneles en todos sus dominios. Pagas las tarifas estándar de transferencia AWS de datos por los resultados de búsqueda transferidos entre dominios.

Temas

Limitaciones

La búsqueda en clústeres tiene varias limitaciones importantes:

- No puedes conectar un dominio de Elasticsearch a un OpenSearch dominio.
- No puedes conectarte a clústeres de /Elasticsearch autogestionados OpenSearch.
- Para conectar dominios entre regiones, ambos dominios deben estar en Elasticsearch 7.10 o una versión posterior o. OpenSearch
- Un dominio puede tener un máximo de 20 conexiones salientes. Del mismo modo, un dominio puede tener un máximo de 20 conexiones entrantes. En otras palabras, un dominio puede conectarse a un máximo de 20 dominios.
- El dominio de origen debe estar en la misma versión o superior a la del dominio de destino. Si configura una conexión bidireccional entre dos dominios y desea actualizar uno o ambos, primero debe eliminar una de las conexiones.
- No puede usar diccionarios personalizados o SQL con la búsqueda en clústeres.
- No se puede usar AWS CloudFormation para conectar dominios.
- No se puede utilizar la búsqueda entre clústeres en instancias M3 o bursátiles (T2 y T3).

Requisitos previos de búsqueda entre clústeres

Antes de configurar la búsqueda en clústeres, asegúrese de que los dominios cumplan los siguientes requisitos:

- Dos OpenSearch dominios, o dominios de Elasticsearch en la versión 6.7 o posterior
- Control de acceso detallado habilitado

- No ode-to-node hay cifrado activado

Precio de búsqueda entre clústeres

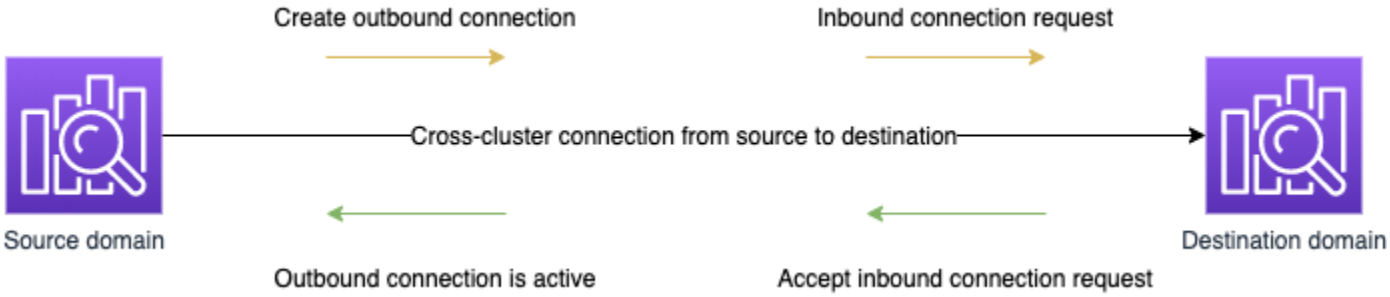
No hay ningún cargo adicional por buscar entre dominios.

Configuración de una conexión

El dominio de “origen” hace referencia al dominio desde el que se origina una petición de búsqueda en clústeres. En otras palabras, el dominio de origen es al que envía la petición de búsqueda inicial.

El dominio “destino” es el dominio que consulta el dominio de origen.

Una conexión entre clústeres es unidireccional desde el dominio de origen hasta el dominio de destino. Esto significa que el dominio de destino no puede consultar el dominio de origen. Sin embargo, puede configurar otra conexión en la dirección opuesta.



El dominio de origen crea una conexión “saliente” al dominio de destino. El dominio de destino recibe una solicitud de conexión “entrante” del dominio de origen.

Para configurar una conexión

1. En el panel del dominio, seleccione un dominio y vaya a la pestaña Conexiones.
2. En la sección Conexiones de salida, seleccione Solicitar.
3. En Alias de conexión, ingrese un nombre para la conexión.
4. Elige entre conectarte a un dominio de tu Cuenta de AWS región o a otra cuenta o región.

    - Para conectarte a un clúster de tu Cuenta de AWS región, selecciona el dominio en el menú desplegable y selecciona Solicitar.
    - Para conectarse a un clúster de otra región Cuenta de AWS o región, seleccione el ARN del dominio remoto y elija Solicitar. Para conectar dominios entre regiones, ambos dominios deben ejecutar Elasticsearch versión 7.10 o posterior o. OpenSearch

5. Para omitir los clústeres no disponibles para las consultas de clústeres, seleccione Omitir los no disponibles. Esta configuración garantiza que las consultas entre clústeres devuelvan resultados parciales a pesar de que se produzcan errores en uno o más clústeres remotos.
6. La búsqueda entre clústeres valida primero la solicitud de conexión para asegurarse de que se cumplen los requisitos previos. Si los dominios son incompatibles, la solicitud de conexión entra en el estado `Validation failed`.
7. Una vez correctamente validada la solicitud de conexión, se envía al dominio de destino, donde tiene que aprobarse. Mientras no se obtenga la aprobación, la conexión permanecerá en el estado de `Pending acceptance`. Cuando se acepta la solicitud de conexión en el dominio de destino, el estado cambia a `Active` y el dominio de destino se vuelve disponible para consultas.

    - La página de dominio muestra el estado general del dominio y los detalles del estado de la instancia del dominio de destino. Los propietarios de dominios tienen la flexibilidad de crear, visualizar, eliminar y monitorear conexiones desde o hacia sus dominios.

Una vez establecida la conexión, se cifra todo el tráfico que circule entre los nodos de los dominios conectados. Si conecta un dominio de VPC a un dominio que no es VPC y el dominio que no es VPC es un punto de enlace público que puede recibir tráfico de Internet, el tráfico entre clústeres entre los dominios sigue cifrado y seguro.

Eliminación de una conexión

La eliminación de una conexión detiene cualquier operación entre clústeres en sus índices.

1. En el panel del dominio, vaya a la pestaña Conexiones.
2. Seleccione las conexiones de dominio que desea eliminar, luego elija Eliminar y, a continuación, confirme la eliminación.

Puede realizar estos pasos en el dominio fuente o de destino para eliminar la conexión. Una vez quitada la conexión, seguirá visible con el estado `Deleted` durante un periodo de 15 días.

No se puede eliminar un dominio con conexiones activas entre clústeres. Para eliminar un dominio, primero quite todas las conexiones entrantes y salientes de ese dominio. Esto es para asegurarse de tener en cuenta a los usuarios del dominio entre clústeres antes de eliminar el dominio.

Configuración de seguridad y explicación de ejemplo

1. Envíe una petición de búsqueda en clústeres al dominio de origen.
2. El dominio de origen evalúa esa solicitud en comparación con la política de acceso al dominio. Dado que la búsqueda en clústeres requiere un control de acceso detallado, recomendamos una política de acceso abierto en el dominio de origen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

> **Note**
>
> Si incluye índices remotos en la ruta, debe codificar la URL del URI en el ARN del dominio. Por ejemplo, use `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst%3Aremote_index` en lugar de `arn:aws:es:us-east-1:123456789012:domain/my-domain/local_index,dst:remote_index`.

Si elige utilizar una política de acceso restrictivo además de un control de acceso detallado, la política debe permitir el acceso a `es:ESHttpGet` como mínimo.

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

```
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::123456789012:user/test-user"
        ]
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:region:account:domain/src-domain/*"
    }
  ]
}
```

3. El control de acceso detallado en el dominio de origen evalúa la solicitud:

   - ¿La solicitud está firmada con credenciales básicas IAM o HTTP válidas?
   - Si es así, ¿tiene el usuario permiso para realizar la búsqueda y acceder a los datos?

   Si la solicitud solo busca datos en el dominio de destino (por ejemplo, `dest-alias:dest-index/_search`), solo necesitará permisos en el dominio de destino.

   Si la solicitud busca datos en ambos dominios (por ejemplo, `source-index,dest-alias:dest-index/_search`), necesita permisos en ambos dominios.

   En el control de acceso detallado, los usuarios deben tener el permiso `indices:admin/shards/search_shards` además del permisos `read` o `search` estándar para los índices pertinentes.

4. El dominio de origen pasa la solicitud al dominio de destino. El dominio de destino evalúa esta solicitud frente a su política de acceso al dominio. Debe incluir el permiso `es:ESCrossClusterGet` en el dominio de destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
```

```
  ]
}
```

Asegúrese de que el permiso `es:ESCrossClusterGet` se aplica para `/dst-domain` y no `/dst-domain/*`.

Sin embargo, esta política mínima solo permite búsquedas en clústeres. Para realizar otras operaciones, como indexar documentos y realizar búsquedas estándar, necesita permisos adicionales. Recomendamos la siguiente política en el dominio de destino:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/dst-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/dst-domain"
    }
  ]
}
```

> **Note**
>
> Todas las solicitudes de búsqueda entre clústeres entre dominios se cifran en tránsito de forma predeterminada como parte del cifrado. node-to-node

5. El dominio de destino realiza la búsqueda y devuelve los resultados al dominio de origen.
6. El dominio de origen combina sus propios resultados (si los hay) con los resultados del dominio de destino y los devuelve.
7. Recomendamos Postman para probar las solicitudes:

   - En el dominio de destino, indexe un documento:

   ```
   POST https://dst-domain.us-east-1.es.amazonaws.com/books/_doc/1

   {
     "Dracula": "Bram Stoker"
   }
   ```

   - Para consultar este índice desde el dominio de origen, incluya el alias de conexión del dominio de destino dentro de la consulta.

   ```
   GET https://src-domain.us-east-1.es.amazonaws.com/<connection_alias>:books/
   _search

   {
       ...
     "hits": [
       {
         "_index": "source-destination:books",
         "_type": "_doc",
         "_id": "1",
         "_score": 1,
         "_source": {
           "Dracula": "Bram Stoker"
         }
       }
     ]
   }
   ```

   Puede encontrar el alias de conexión en la pestaña Conexiones del panel de control del dominio.

   - Si configura una conexión entre `domain-a -> domain-b` con alias de conexión `cluster_b` y `domain-a -> domain-c` con alias de conexión `cluster_c`, busque `domain-a`, `domain-b` y `domain-c` de la siguiente manera:

```
GET https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_search
{
  "query": {
    "match": {
      "user": "domino"
    }
  }
}
```

Respuesta

```
{
  "took": 150,
  "timed_out": false,
  "_shards": {
    "total": 3,
    "successful": 3,
    "failed": 0,
    "skipped": 0
  },
  "_clusters": {
    "total": 3,
    "successful": 3,
    "skipped": 0
  },
  "hits": {
    "total": 3,
    "max_score": 1,
    "hits": [
      {
        "_index": "local_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 1,
        "_source": {
          "user": "domino",
          "message": "Lets unite the new mutants",
          "likes": 0
        }
      },
      {
```

```
        "_index": "cluster_b:b_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 2,
        "_source": {
          "user": "domino",
          "message": "I'm different",
          "likes": 0
        }
      },
      {
        "_index": "cluster_c:c_index",
        "_type": "_doc",
        "_id": "0",
        "_score": 3,
        "_source": {
          "user": "domino",
          "message": "So am I",
          "likes": 0
        }
      }
    ]
  }
}
```

Si no eligió omitir los clústeres no disponibles en la configuración de la conexión, todos los clústeres de destino que busca tienen que estar disponibles para que la petición de búsqueda se ejecute correctamente. De lo contrario, se produce un error en toda la solicitud; incluso si uno de los dominios no está disponible, la búsqueda no devuelve ningún resultado.

OpenSearch Cuadros de mando

Puede visualizar datos de varios dominios conectados de la misma manera que desde un solo dominio, excepto que debe acceder a los índices remotos mediante `connection-alias:index`. Por lo tanto, su patrón de índice debe coincidir `connection-alias:index`.

Aprender a clasificar para Amazon OpenSearch Service

OpenSearch utiliza un marco de clasificación probabilístico llamado BM-25 para calcular las puntuaciones de relevancia. Si una palabra clave distintiva aparece con más frecuencia en un

documento, BM-25 asigna una puntuación de relevancia más alta a ese documento. Este marco, sin embargo, no tiene en cuenta el comportamiento del usuario, como los datos de clics, lo que puede mejorar aún más la relevancia.

Learning to Rank es un complemento de código abierto que permite utilizar machine learning y los datos de comportamiento para ajustar la relevancia de los documentos. El complemento utiliza modelos de las bibliotecas XGBoost y Ranklib para volver a puntuar los resultados de búsqueda. El complemento de Elasticsearch LTR fue desarrollado inicialmente por OpenSource Connections, con importantes contribuciones de Wikimedia Foundation, Snagajob Engineering, Bonsai y Yelp Engineering. La versión de OpenSearch del plugin se deriva del complemento Elasticsearch LTR. La documentación completa, incluidos los pasos detallados y las descripciones de la API, está disponible en la documentación de Learning to Rank (Aprender a clasificar).

Aprender a clasificar requiere OpenSearch o Elasticsearch 7.7 o posterior.

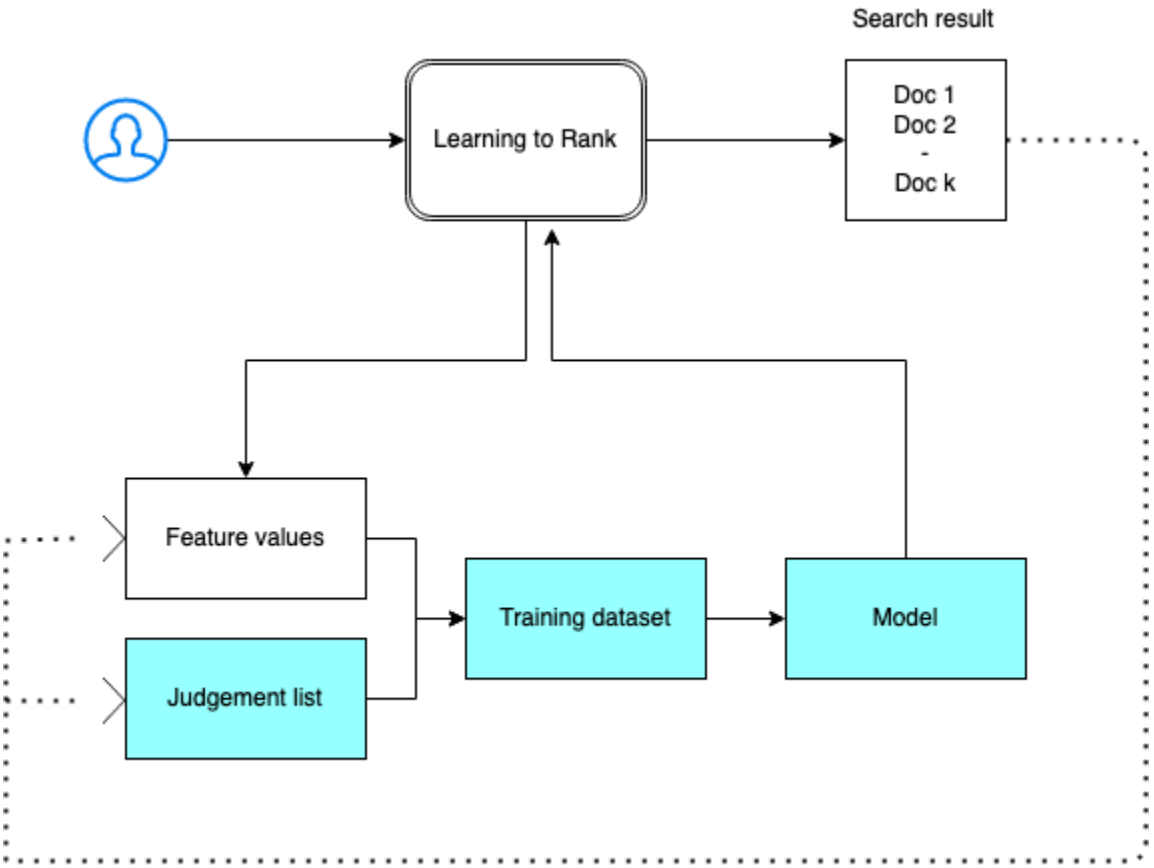
> **Note**
>
> Para utilizar el complemento Aprender a clasificar, debe tener permisos de administrador completos. Para obtener más información, consulte the section called “Modificar el usuario maestro”.

Temas

- Introducción a Aprender a clasificar
- API de Aprender a clasificar

Introducción a Aprender a clasificar

Debe proporcionar una lista de criterios, preparar un conjunto de datos de entrenamiento y entrenar el modelo fuera de Amazon OpenSearch Service. Las partes en azul se producen fuera de OpenSearch Service:



Paso 1: inicializar el complemento

Para inicializar el complemento Aprender a clasificar, envíe la siguiente solicitud a su dominio de OpenSearch Service:

```
PUT _ltr
```

```
{
  "acknowledged" : true,
  "shards_acknowledged" : true,
  "index" : ".ltrstore"
}
```

Este comando crea un índice `.ltrstore` oculto que almacena información de metadatos, como conjuntos de características y modelos.

Paso 2: crear una lista de criterios

> **Note**
>
> Debe realizar este paso fuera de OpenSearch Service.

Una lista de criterios es un conjunto de ejemplos de los cuales aprende un modelo de machine learning. La lista de criterios debe incluir palabras clave importantes para usted y un conjunto de documentos calificados para cada palabra clave.

En este ejemplo, tenemos una lista de criterios para un conjunto de datos de películas. Un grado de 4 indica una coincidencia perfecta. Un grado de 0 indica la peor coincidencia.

Grado	Palabra clave	ID del documento	Nombre de la película
4	rambo	7555	Rambo
3	rambo	1370	Rambo III
3	rambo	1369	Rambo: First Blood Part II
3	rambo	1368	First Blood

Prepare la lista de criterios con el siguiente formato:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood

where qid:1 represents "rambo"
```

Para ver un ejemplo más completo de una lista de criterios, consulte Criterios sobre películas.

Puede crear esta lista de criterios de forma manual con la ayuda de anotadores humanos o inferirla de manera programática a partir de datos de análisis.

Paso 3: crear un conjunto de características

Una característica es un campo que corresponde a la relevancia de un documento, por ejemplo, `title`, `overview`, `popularity score` (número de vistas) y así sucesivamente.

Cree un conjunto de características con una plantilla de Mustache para cada característica. Para obtener más información acerca de las características, consulte Trabajo con características.

En este ejemplo, crearemos un conjunto de características `movie_features` con los campos `title` y `overview`:

```
POST _ltr/_featureset/movie_features
{
  "featureset" : {
      "name" : "movie_features",
      "features" : [
        {
          "name" : "1",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "title" : "{{keywords}}"
            }
          }
        },
        {
          "name" : "2",
          "params" : [
            "keywords"
          ],
          "template_language" : "mustache",
          "template" : {
            "match" : {
              "overview" : "{{keywords}}"
            }
          }
        }
      ]
    }
}
```

Si consulta el índice `.ltrstore` original, recupera el conjunto de características:

```
GET _ltr/_featureset
```

Paso 4: registrar los valores de la característica

Los valores de la característica son las puntuaciones de relevancia calculadas por BM-25 para cada característica.

Combine el conjunto de características y la lista de sentencias para registrar los valores de la característica. Para obtener más información acerca de las características de registro, consulte Puntuaciones de características.

En este ejemplo, la consulta `bool` recupera los documentos calificados con el filtro y, a continuación, elige el conjunto de características con la consulta `sltr`. La consulta `ltr_log` combina los documentos y las características para registrar los valores de característica correspondientes:

```
POST tmdb/_search
{
  "_source": {
    "includes": [
      "title",
      "overview"
    ]
  },
  "query": {
    "bool": {
      "filter": [
        {
          "terms": {
            "_id": [
              "7555",
              "1370",
              "1369",
              "1368"
            ]
          }
        },
        {
          "sltr": {
            "_name": "logged_featureset",
            "featureset": "movie_features",
```

```
            "params": {
              "keywords": "rambo"
            }
          }
        }
      ]
    }
  },
  "ext": {
    "ltr_log": {
      "log_specs": {
        "name": "log_entry1",
        "named_query": "logged_featureset"
      }
    }
  }
}
```

Un ejemplo de respuesta se vería así:

```
{
  "took" : 7,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 4,
      "relation" : "eq"
    },
    "max_score" : 0.0,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 0.0,
        "_source" : {
```

```
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1"
              },
              {
                "name" : "2",
                "value" : 10.558305
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "7555",
      "_score" : 0.0,
      "_source" : {
        "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1",
```

```
                "value" : 11.2569065
              },
              {
                "name" : "2",
                "value" : 9.936821
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
      ]
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 0.0,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
        "title" : "Rambo: First Blood Part II"
      },
      "fields" : {
        "_ltrlog" : [
          {
            "log_entry1" : [
              {
                "name" : "1",
                "value" : 6.334839
              },
              {
                "name" : "2",
                "value" : 10.558305
              }
            ]
          }
        ]
      },
      "matched_queries" : [
        "logged_featureset"
```

```
        ]
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 0.0,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
 find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
 his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
 when Trautman is captured.",
          "title" : "Rambo III"
        },
        "fields" : {
          "_ltrlog" : [
            {
              "log_entry1" : [
                {
                  "name" : "1",
                  "value" : 9.425955
                },
                {
                  "name" : "2",
                  "value" : 11.262714
                }
              ]
            }
          ]
        },
        "matched_queries" : [
          "logged_featureset"
        ]
      }
    ]
  }
}
```


En el ejemplo anterior, la primera característica no posee un valor de característica, ya que la palabra clave “rambo” no aparece en el campo de título del documento con un ID igual a 1368. Se trata de un valor de característica que falta en los datos de entrenamiento.

Paso 5: crear un conjunto de datos de entrenamiento

> **Note**
>
> Debe realizar este paso fuera de OpenSearch Service.

El siguiente paso es combinar la lista de sentencias y los valores de característica para crear un conjunto de datos de entrenamiento. Si la lista de criterios original se ve así:

```
4 qid:1 # 7555 Rambo
3 qid:1 # 1370 Rambo III
3 qid:1 # 1369 Rambo: First Blood Part II
3 qid:1 # 1368 First Blood
```

Conviértala en el conjunto de datos de entrenamiento final, que se ve así:

```
4 qid:1 1:12.318474 2:10.573917 # 7555 rambo
3 qid:1 1:10.357875 2:11.950391 # 1370 rambo
3 qid:1 1:7.010513 2:11.220095 # 1369 rambo
3 qid:1 1:0.0 2:11.220095 # 1368 rambo
```

Puede realizar este paso de forma manual o escribir un programa para automatizarlo.

Paso 6: elegir un algoritmo y crear el modelo

> **Note**
>
> Debe realizar este paso fuera de OpenSearch Service.

Con el conjunto de datos de entrenamiento en su lugar, el siguiente paso es utilizar las bibliotecas XGBoost o Ranklib para crear un modelo. Las bibliotecas XGBoost y Ranklib permiten crear modelos populares como LambdaMART, Random Forests, etc.

Para conocer los pasos para utilizar XGBoost y Ranklib para crear el modelo, consulte la documentación sobre XGBoost y RankLib, respectivamente. Para utilizar Amazon SageMaker para crear el modelo XGBoost, consulte el Algoritmo XGBoost.

Paso 7: implementar el modelo

Después de haber creado el modelo, impleméntelo en el complemento Learning to Rank (Aprender a clasificar). Para obtener más información acerca de la implementación de un modelo, consulte Carga de un modelo entrenado.

En este ejemplo, crearemos un modelo de `my_ranklib_model` con la biblioteca Ranklib:

```
POST _ltr/_featureset/movie_features/_createmodel?pretty
{
  "model": {
    "name": "my_ranklib_model",
    "model": {
      "type": "model/ranklib",
      "definition": """## LambdaMART
## No. of trees = 10
## No. of leaves = 10
## No. of threshold candidates = 256
## Learning rate = 0.1
## Stop early = 100

<ensemble>
   <tree id="1" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-2.0</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-2.0</output>
               </split>
               <split pos="right">
                  <output>-2.0</output>
               </split>
            </split>
         </split>
```

```
         <split pos="right">
            <output>2.0</output>
         </split>
      </split>
   </tree>
   <tree id="2" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.67031991481781</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.67031991481781</output>
               </split>
               <split pos="right">
                  <output>-1.6703200340270996</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.6703201532363892</output>
         </split>
      </split>
   </tree>
   <tree id="3" weight="0.1">
      <split>
         <feature>2</feature>
         <threshold>10.573917</threshold>
         <split pos="left">
            <output>1.479954481124878</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
```

```
            <split pos="left">
               <output>-1.4799546003341675</output>
            </split>
            <split pos="right">
               <output>-1.479954481124878</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.479954481124878</output>
         </split>
      </split>
   </split>
</tree>
<tree id="4" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
      <split pos="left">
         <feature>1</feature>
         <threshold>0.0</threshold>
         <split pos="left">
            <output>-1.3569872379302979</output>
         </split>
         <split pos="right">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <output>-1.3569872379302979</output>
            </split>
            <split pos="right">
               <output>-1.3569872379302979</output>
            </split>
         </split>
      </split>
      <split pos="right">
         <output>1.3569873571395874</output>
      </split>
   </split>
</tree>
<tree id="5" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
      <split pos="left">
```

```
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.2721362113952637</output>
            </split>
            <split pos="right">
               <feature>1</feature>
               <threshold>7.010513</threshold>
               <split pos="left">
                  <output>-1.2721363306045532</output>
               </split>
               <split pos="right">
                  <output>-1.2721363306045532</output>
               </split>
            </split>
         </split>
         <split pos="right">
            <output>1.2721362113952637</output>
         </split>
      </split>
   </tree>
   <tree id="6" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.2110036611557007</output>
               </split>
               <split pos="right">
                  <output>-1.2110036611557007</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.2110037803649902</output>
            </split>
         </split>
         <split pos="right">
            <output>1.2110037803649902</output>
```

```
         </split>
      </split>
   </tree>
   <tree id="7" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.165616512298584</output>
               </split>
               <split pos="right">
                  <output>-1.165616512298584</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.165616512298584</output>
            </split>
         </split>
         <split pos="right">
            <output>1.165616512298584</output>
         </split>
      </split>
   </tree>
   <tree id="8" weight="0.1">
      <split>
         <feature>1</feature>
         <threshold>10.357875</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>7.010513</threshold>
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.131177544593811</output>
               </split>
               <split pos="right">
                  <output>-1.131177544593811</output>
```

```
            </split>
         </split>
         <split pos="right">
            <output>-1.131177544593811</output>
         </split>
      </split>
      <split pos="right">
         <output>1.131177544593811</output>
      </split>
   </split>
</tree>
<tree id="9" weight="0.1">
   <split>
      <feature>2</feature>
      <threshold>10.573917</threshold>
      <split pos="left">
         <output>1.1046180725097656</output>
      </split>
      <split pos="right">
         <feature>1</feature>
         <threshold>7.010513</threshold>
         <split pos="left">
            <feature>1</feature>
            <threshold>0.0</threshold>
            <split pos="left">
               <output>-1.1046180725097656</output>
            </split>
            <split pos="right">
               <output>-1.1046180725097656</output>
            </split>
         </split>
         <split pos="right">
            <output>-1.1046180725097656</output>
         </split>
      </split>
   </split>
</tree>
<tree id="10" weight="0.1">
   <split>
      <feature>1</feature>
      <threshold>10.357875</threshold>
      <split pos="left">
         <feature>1</feature>
         <threshold>7.010513</threshold>
```

```
            <split pos="left">
               <feature>1</feature>
               <threshold>0.0</threshold>
               <split pos="left">
                  <output>-1.0838804244995117</output>
               </split>
               <split pos="right">
                  <output>-1.0838804244995117</output>
               </split>
            </split>
            <split pos="right">
               <output>-1.0838804244995117</output>
            </split>
         </split>
         <split pos="right">
            <output>1.0838804244995117</output>
         </split>
      </split>
   </tree>
</ensemble>
"""
    }
  }
}
```

Para ver el modelo, envíe la siguiente solicitud:

```
GET _ltr/_model/my_ranklib_model
```

Paso 8: buscar con Aprender a clasificar

Después de implementar el modelo, estará listo para realizar la búsqueda.

Realice la consulta `sltr` con las características que utiliza y el nombre del modelo que desea ejecutar:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
```

```
    "multi_match": {
      "query": "rambo",
      "fields": ["title", "overview"]
    }
  },
  "rescore": {
    "query": {
      "rescore_query": {
        "sltr": {
          "params": {
            "keywords": "rambo"
          },
          "model": "my_ranklib_model"
        }
      }
    }
  }
}
```

Con Aprender a clasificar, usted ve “Rambo” como el primer resultado porque le asignamos la calificación más alta en la lista de criterios:

```
{
  "took" : 12,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 7,
      "relation" : "eq"
    },
    "max_score" : 13.096414,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 13.096414,
```

```
      "_source" : {
        "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
        "title" : "Rambo"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1370",
      "_score" : 11.17245,
      "_source" : {
        "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
        "title" : "Rambo III"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1368",
      "_score" : 10.442155,
      "_source" : {
        "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
        "title" : "First Blood"
      }
    },
    {
      "_index" : "tmdb",
      "_type" : "movie",
      "_id" : "1369",
      "_score" : 10.442155,
      "_source" : {
        "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
```

```
rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "31362",
        "_score" : 7.424202,
        "_source" : {
          "overview" : "It is 1985, and a small, tranquil Florida town is being rocked
by a wave of vicious serial murders and bank robberies. Particularly sickening to the
authorities is the gratuitous use of violence by two “Rambo” like killers who dress
themselves in military garb. Based on actual events taken from FBI files, the movie
depicts the Bureau’s efforts to track down these renegades.",
          "title" : "In the Line of Duty: The F.B.I. Murders"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.43182,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
his family's stifling home life when he encounters Lee Carter (Will Poulter), the
school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
to make cinematic history by filming his own action-packed video epic. Together, these
two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
– and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
own!""",
          "title" : "Son of Rambow"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "61410",
        "_score" : 3.9719706,
        "_source" : {
          "overview" : "It's South Africa 1990. Two major events are about to happen:
The release of Nelson Mandela and, more importantly, it's Spud Milton's first year
at an elite boys only private boarding school. John Milton is a boy from an ordinary
```

```
 background who wins a scholarship to a private school in Kwazulu-Natal, South Africa.
 Surrounded by boys with nicknames like Gecko, Rambo, Rain Man and Mad Dog, Spud has
 his hands full trying to adapt to his new home. Along the way Spud takes his first
 tentative steps along the path to manhood. (The path it seems could be a rather long
 road). Spud is an only child. He is cursed with parents from well beyond the lunatic
 fringe and a senile granny. His dad is a fervent anti-communist who is paranoid that
 the family domestic worker is running a shebeen from her room at the back of the
 family home. His mom is a free spirit and a teenager's worst nightmare, whether it's
 shopping for Spud's underwear in the local supermarket",
          "title" : "Spud"
        }
      }
    ]
  }
}
```

Si realiza la búsqueda sin utilizar el complemento Aprender a clasificar, OpenSearch devuelve resultados diferentes:

```
POST tmdb/_search
{
  "_source": {
    "includes": ["title", "overview"]
  },
  "query": {
    "multi_match": {
      "query": "Rambo",
      "fields": ["title", "overview"]
    }
  }
}
```

```
{
  "took" : 5,
  "timed_out" : false,
  "_shards" : {
    "total" : 1,
    "successful" : 1,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
```

```
      "value" : 5,
      "relation" : "eq"
    },
    "max_score" : 11.262714,
    "hits" : [
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1370",
        "_score" : 11.262714,
        "_source" : {
          "overview" : "Combat has taken its toll on Rambo, but he's finally begun to
find inner peace in a monastery. When Rambo's friend and mentor Col. Trautman asks for
his help on a top secret mission to Afghanistan, Rambo declines but must reconsider
when Trautman is captured.",
          "title" : "Rambo III"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "7555",
        "_score" : 11.2569065,
        "_source" : {
          "overview" : "When governments fail to act on behalf of captive missionaries,
ex-Green Beret John James Rambo sets aside his peaceful existence along the Salween
River in a war-torn region of Thailand to take action.  Although he's still haunted
by violent memories of his time as a U.S. soldier during the Vietnam War, Rambo can
hardly turn his back on the aid workers who so desperately need his help.",
          "title" : "Rambo"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1368",
        "_score" : 10.558305,
        "_source" : {
          "overview" : "When former Green Beret John Rambo is harassed by local law
enforcement and arrested for vagrancy, the Vietnam vet snaps, runs for the hills and
rat-a-tat-tats his way into the action-movie hall of fame. Hounded by a relentless
sheriff, Rambo employs heavy-handed guerilla tactics to shake the cops off his tail.",
          "title" : "First Blood"
        }
```

```
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "1369",
        "_score" : 10.558305,
        "_source" : {
          "overview" : "Col. Troutman recruits ex-Green Beret John Rambo for a highly
 secret and dangerous mission. Teamed with Co Bao, Rambo goes deep into Vietnam to
 rescue POWs. Deserted by his own team, he's left in a hostile jungle to fight for his
 life, avenge the death of a woman and bring corrupt officials to justice.",
          "title" : "Rambo: First Blood Part II"
        }
      },
      {
        "_index" : "tmdb",
        "_type" : "movie",
        "_id" : "13258",
        "_score" : 6.4600153,
        "_source" : {
          "overview" : """Will Proudfoot (Bill Milner) is looking for an escape from
 his family's stifling home life when he encounters Lee Carter (Will Poulter), the
 school bully. Armed with a video camera and a copy of "Rambo: First Blood", Lee plans
 to make cinematic history by filming his own action-packed video epic. Together, these
 two newfound friends-turned-budding-filmmakers quickly discover that their imaginative
 – and sometimes mishap-filled – cinematic adventure has begun to take on a life of its
 own!""",
          "title" : "Son of Rambow"
        }
      }
    ]
  }
}
```

En función de cuán bien considere que el modelo funciona, ajuste la lista de criterios y las características. A continuación, repita los pasos 2 a 8 para mejorar los resultados de la clasificación a lo largo del tiempo.

API de Aprender a clasificar

Utilice las operaciones de Aprender a clasificar para trabajar de manera programática con conjuntos de características y modelos.

Crear tienda

Crea un índice `.ltrstore` oculto que almacena información sobre metadatos, como conjuntos de características y modelos.

```
PUT _ltr
```

Eliminar tienda

Elimina el índice `.ltrstore` oculto y restablece el complemento.

```
DELETE _ltr
```

Crear conjunto de características

Crea un conjunto de características.

```
POST _ltr/_featureset/<name_of_features>
```

Eliminar un conjunto de características

Elimina un conjunto de características.

```
DELETE _ltr/_featureset/<name_of_feature_set>
```

Obtener un conjunto de características

Recupera un conjunto de características.

```
GET _ltr/_featureset/<name_of_feature_set>
```

Crear un modelo

Crea un modelo.

```
POST _ltr/_featureset/<name_of_feature_set>/_createmodel
```

Eliminar modelo

Elimina un modelo.

```
DELETE _ltr/_model/<name_of_model>
```

Obtener modelo

Recupera un modelo.

```
GET _ltr/_model/<name_of_model>
```

Obtener estadísticas

Proporciona información acerca de cómo se comporta el complemento.

```
GET _ltr/_stats
```

También puede usar filtros para recuperar una sola estadística:

```
GET _ltr/_stats/<stat>
```

Además, puede limitar la información a un único nodo del clúster:

```
GET _ltr/_stats/<stat>/nodes/<nodeId>

{
  "_nodes" : {
    "total" : 1,
    "successful" : 1,
    "failed" : 0
  },
  "cluster_name" : "873043598401:ltr-77",
  "stores" : {
    ".ltrstore" : {
      "model_count" : 1,
      "featureset_count" : 1,
      "feature_count" : 2,
      "status" : "green"
    }
  },
  "status" : "green",
  "nodes" : {
    "DjelK-_ZSfyzstO5dhGGQA" : {
```

```
      "cache" : {
        "feature" : {
          "eviction_count" : 0,
          "miss_count" : 0,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "featureset" : {
          "eviction_count" : 2,
          "miss_count" : 2,
          "entry_count" : 0,
          "memory_usage_in_bytes" : 0,
          "hit_count" : 0
        },
        "model" : {
          "eviction_count" : 2,
          "miss_count" : 3,
          "entry_count" : 1,
          "memory_usage_in_bytes" : 3204,
          "hit_count" : 1
        }
      },
      "request_total_count" : 6,
      "request_error_count" : 0
    }
  }
}
```

Las estadísticas se proporcionan en dos niveles, nodo y clúster, como se especifica en las siguientes tablas:

Estadísticas a nivel de nodo

Nombre del campo	Descripción
request_total_count	Recuento total de solicitudes de clasificación.
request_error_count	Recuento total de solicitudes fallidas.
cache	Estadísticas de todas las cachés (caracter ísticas, conjuntos de características, modelos). Se produce un acierto de caché cuando un

Nombre del campo	Descripción
	usuario consulta el complemento y el modelo ya está cargado en la memoria.
cache.eviction_count	Número de expulsiones de caché.
cache.hit_count	Número de aciertos de caché.
cache.miss_count	Número de errores de caché. Se produce un error de caché cuando un usuario consulta el complemento y el modelo aún no se cargó en la memoria.
cache.entry_count	Número de entradas en la caché.
cache.memory_usage_in_bytes	Memoria total utilizada en bytes.
cache.cache_capacity_reached	Indica si se alcanza el límite de caché.

Estadísticas de nivel de clúster

Nombre del campo	Descripción
tiendas	Indica dónde se almacenan los conjuntos de características y los metadatos del modelo. (El valor predeterminado es “.ltrstore”. De lo contrario, tiene el prefijo “.ltrstore_”, con un nombre proporcionado por el usuario).
stores.status	Estado del índice.
stores.feature_sets	Número de conjuntos de características.
stores.features_count	Número de características.
stores.model_count	Número de modelos.
estado	Estado del complemento basado en el estado de los índices del almacén de características

Nombre del campo	Descripción
	(rojo, amarillo o verde) y el estado del interrupt or de circuito (abierto o cerrado).
cache.cache_capacity_reached	Indica si se alcanza el límite de caché.

Obtener estadísticas de caché

Devuelve estadísticas sobre el uso de la memoria y la caché.

```
GET _ltr/_cachestats

{
    "_nodes": {
        "total": 2,
        "successful": 2,
        "failed": 0
    },
    "cluster_name": "opensearch-cluster",
    "all": {
        "total": {
            "ram": 612,
            "count": 1
        },
        "features": {
            "ram": 0,
            "count": 0
        },
        "featuresets": {
            "ram": 612,
            "count": 1
        },
        "models": {
            "ram": 0,
            "count": 0
        }
    },
    "stores": {
        ".ltrstore": {
            "total": {
                "ram": 612,
```

```
                "count": 1
            },
            "features": {
                "ram": 0,
                "count": 0
            },
            "featuresets": {
                "ram": 612,
                "count": 1
            },
            "models": {
                "ram": 0,
                "count": 0
            }
        }
    },
    "nodes": {
        "ejF6uutERF20wOFNOXB61A": {
            "name": "opensearch1",
            "hostname": "172.18.0.4",
            "stats": {
                "total": {
                    "ram": 612,
                    "count": 1
                },
                "features": {
                    "ram": 0,
                    "count": 0
                },
                "featuresets": {
                    "ram": 612,
                    "count": 1
                },
                "models": {
                    "ram": 0,
                    "count": 0
                }
            }
        },
        "Z2RZNWRLSveVcz2c6lHf5A": {
            "name": "opensearch2",
            "hostname": "172.18.0.2",
            "stats": {
                ...
```

```
            }
        }
    }
}
```

Borrar caché

Borra la caché del complemento. Utilice esta opción para actualizar el modelo.

```
POST _ltr/_clearcache
```

Búsqueda asíncrona en Amazon OpenSearch Service

Con la búsqueda asíncrona de Amazon OpenSearch Service, puede enviar una consulta de búsqueda que se ejecute en segundo plano, monitorear el progreso de la solicitud y recuperar los resultados en una etapa posterior. Puede recuperar resultados parciales, a medida que estén disponibles, antes de que se complete la búsqueda. Una vez finalizada la búsqueda, guarde los resultados para una posterior recuperación y análisis.

La búsqueda asíncrona requiere OpenSearch 1.0 o posterior o Elasticsearch 7.10 o posterior. La documentación completa de la búsqueda asíncrona, incluidos los pasos detallados y las descripciones de la API, está disponible en la Documentación de OpenSearch.

Ejemplo de llamada de búsqueda

Para realizar una búsqueda asíncrona, envíe solicitudes HTTP a `_plugins/_asynchronous_search` con el siguiente formato:

```
POST opensearch-domain/_plugins/_asynchronous_search
```

> **Note**
>
> Si utiliza Elasticsearch 7.10 en lugar de una versión de OpenSearch, reemplace `_plugins` con `_opendistro` en todas las solicitudes de búsqueda asíncronas.

Puede especificar las siguientes opciones de búsqueda asíncrona:

Opciones	Descripción	Valor predeterminado	Obligatorio
`wait_for_completion_timeout`	Especifica la cantidad de tiempo durante la cual planea esperar los resultados. Puede ver los resultados que obtiene dentro de este tiempo, igual que en una búsqueda normal. Puede sondear los resultados restantes en función de un ID. El valor máximo es 300 segundos.	1 segundos	No
`keep_on_completion`	Especifica si desea guardar los resultados en el clúster una vez finalizada la búsqueda. Puede examinar los resultados almacenados más adelante.	`false`	No
`keep_alive`	Especifica la cantidad de tiempo que se guarda el resultado en el clúster. Por ejemplo, `2d` significa que los resultados se almacenan en el clúster durante 48 horas. Los resultados de búsqueda guardados se eliminan después de este periodo o si se cancela la búsqueda. Tenga en cuenta que esto incluye el tiempo de ejecución de la consulta. Si la consulta sobrepasa este tiempo, el proceso cancela esta consulta automáticamente.	12 horas	No

Solicitud de ejemplo

```
POST _plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=1ms&keep_on_completion=true&request_cache=false
{
  "aggs": {
    "city": {
      "terms": {
        "field": "city",
        "size": 10
      }
```

```
    }
  }
}
```

> **Note**
>
> Todos los parámetros de solicitud que se aplican a una consulta `_search` estándar son compatibles. Si utiliza Elasticsearch 7.10 en lugar de una versión de OpenSearch, reemplace `_plugins` con `_opendistro`.

Permisos de búsqueda asíncrona

La búsqueda asíncrona admite el control de acceso detallado. Para obtener más información sobre la combinación y la coincidencia de permisos para adaptarlos al caso de uso, consulteSeguridad de búsqueda asíncrona.

Para los dominios con control de acceso detallado habilitado, necesita los siguientes permisos mínimos para un rol:

```
# Allows users to use all asynchronous search functionality
asynchronous_search_full_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/*'
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - 'indices:data/read/search*'

# Allows users to read stored asynchronous search results
asynchronous_search_read_access:
  reserved: true
  cluster_permissions:
    - 'cluster:admin/opensearch/asynchronous-search/get'
```

Para dominios con control de acceso detallado deshabilitado, utilice el acceso de IAM y la clave secreta para firmar todas las solicitudes. Puede acceder a los resultados con el ID de búsqueda asíncrona.

Configuración de búsqueda asincrónica

OpenSearch permite cambiar todas las configuraciones de búsqueda asincrónica mediante la API de `_cluster/settings`. En OpenSearch Service, solo puede cambiar la configuración siguiente:

- `plugins.asynchronous_search.node_concurrent_running_searches`
- `plugins.asynchronous_search.persist_search_failures`

Búsqueda en clústeres

Puede realizar una búsqueda asíncrona entre clústeres con las siguientes limitaciones menores:

- Puede ejecutar una búsqueda asíncrona solo en el dominio fuente.
- No puede minimizar los viajes de ida y vuelta de la red como parte de una consulta de búsqueda entre clústeres.

Si configura una conexión entre `domain-a -> domain-b`, con alias de conexión `cluster_b`, y `domain-a -> domain-c`, con alias de conexión `cluster_c`, realice una búsqueda asíncrona de `domain-a`, `domain-b` y `domain-c`, de la siguiente manera:

```
POST https://src-domain.us-east-1.es.amazonaws.com/
local_index,cluster_b:b_index,cluster_c:c_index/_plugins/_asynchronous_search/?
pretty&size=10&wait_for_completion_timeout=500ms&keep_on_completion=true&request_cache=false
{
  "size": 0,
  "_source": {
    "excludes": []
  },
  "aggs": {
    "2": {
      "terms": {
        "field": "clientip",
        "size": 50,
        "order": {
          "_count": "desc"
        }
      }
    }
  },
  "stored_fields": [
```

```
    "*"
  ],
  "script_fields": {},
  "docvalue_fields": [
    "@timestamp"
  ],
  "query": {
    "bool": {
      "must": [
        {
          "query_string": {
            "query": "status:404",
            "analyze_wildcard": true,
            "default_field": "*"
          }
        },
        {
          "range": {
            "@timestamp": {
              "gte": 1483747200000,
              "lte": 1488326400000,
              "format": "epoch_millis"
            }
          }
        }
      ],
      "filter": [],
      "should": [],
      "must_not": []
    }
  }
}
```

Respuesta

```
{
  "id" :
 "Fm9pYzJyVG91U19xb0hIQUJnMHJfRFEAAAAAAAknghQ1OWVBczNZQjVEa2dMYTBXaTdEagAAAAAAAAAB",
  "state" : "RUNNING",
  "start_time_in_millis" : 1609329314796,
  "expiration_time_in_millis" : 1609761314796
}
```

Para obtener más información, consulte the section called “Búsqueda en clústeres”.

UltraWarm

Las búsquedas asíncronas con índices de UltraWarm siguen en funcionamiento. Para obtener más información, consulte the section called “UltraWarm almacenamiento”.

> **Note**
>
> Puede monitorear las estadísticas de búsqueda asíncrona en CloudWatch. Para obtener una lista completa de las métricas, consulte the section called “Métricas de búsqueda asíncrona”.

Punto en el tiempo en Amazon OpenSearch Service

La característica de punto en el tiempo (PIT) es un tipo de búsqueda que permite ejecutar diferentes consultas en un conjunto de datos fijo en el tiempo. Normalmente, cuando ejecuta la misma consulta en el mismo índice en distintos puntos en el tiempo, recibe resultados diferentes porque los documentos se indexan, actualizan y eliminan constantemente. Con PIT, puede realizar consultas en función de un estado constante de su conjunto de datos.

El uso principal de la función PIT es combinarla con la funcionalidad `search_after`. Este es el método de paginación preferido en OpenSearch, especialmente para la paginación profunda, porque funciona en un conjunto de datos que está congelado en el tiempo, no está vinculado a una consulta y admite una paginación coherente hacia adelante y hacia atrás. Puede usar PIT con la versión 2.5 y versiones posteriores de OpenSearch Service.

Para obtener más información sobre PIT, consulte Punto en el tiempo en la documentación de OpenSearch.

Consideraciones

Al configurar las búsquedas PIT, tenga en cuenta lo siguiente:

- Si va a realizar una actualización desde un dominio 2.3 y necesita un control de acceso detallado para las acciones PIT, tendrá que añadir esas acciones y funciones manualmente.
- El PIT no tiene capacidad de recuperación. El reinicio de los nodos, la terminación de nodos, las implementaciones azul/verde y los reinicios de los procesos ES provocan la pérdida de todos los datos de PIT.

- Si una partición se reubica durante la implementación azul/verde, solo los segmentos de datos activos se transfieren al nuevo nodo. Los segmentos de particiones retenidos por PIT (tanto de forma exclusiva como el que se comparte con los datos activos) permanecen en el nodo anterior.
- Actualmente, las búsquedas PIT no funcionan con la búsqueda asíncrona.

Crear un PIT

Para crear un PIT, envíe solicitudes HTTP a `_search/point_in_time` con el siguiente formato:

```
POST opensearch-domain/my-index/_search/point_in_time?keep_alive=time
```

Puede especificar las siguientes opciones PIT:

Opciones	Descripción	Valor predeterminado	Obligatorio
`keep_alive`	La cantidad de tiempo que debe durar la conservación del PIT. Cada vez que se accede a un PIT con una solicitud de búsqueda, la vida útil del PIT se prolonga en un tiempo igual al parámetro `keep_alive` . Este parámetro de consulta es obligatorio cuando se crea un PIT, pero es opcional en una solicitud de búsqueda.		Sí
`preference`	Una cadena que especifica el nodo o la partición utilizados para realizar la búsqueda.	Random	No
`routing`	Una cadena que especifica que las solicitudes de búsqueda se dirijan a una partición específica.	El `_id` del documento	No
`expand_wildcards`	Una cadena que especifica el tipo de índice que puede coincidir con el patrón comodín. Admite valores separados por comas. Los valores válidos son los siguientes:	`open`	No

Opciones	Descripción	Valor predeterminado	Obligatorio
	• `all`: Coincide con cualquier índice o flujo de datos, incluidos los ocultos. • `open`: Coincide índices abiertos, no ocultos o flujos de datos no ocultos. • `closed`: Coincide índices cerrados, no ocultos o flujos de datos no ocultos. • `hidden`: Coincide índices o flujos de datos ocultos. Debe combinarse con índices abiertos, cerrados o tanto abiertos como cerrados. • `none`: No se aceptan patrones comodín.		
`allow_partial_pit_creation`	Un valor booleano que especifica si se debe crear un PIT con errores parciales.	`true`	No

Respuesta de ejemplo

```
{
    "pit_id":
 "o463QQEPbXktaW5kZXgtMDAwMDAxFnNOWU43ckt3U3IyaFVpbGE1UWEtMncAFjFyeXBsRGJmVFM2RTB6eVg1aVVqQncAA
    "_shards": {
        "total": 1,
        "successful": 1,
        "skipped": 0,
        "failed": 0
    },
    "creation_time": 1658146050064
}
```

Al crear un PIT, recibirá un ID de PIT en la respuesta. Este es el ID que se utiliza para realizar búsquedas con el PIT.

Permisos de puntos en el tiempo

Los PIT admiten el control de acceso detallado. Si va a actualizar a un dominio 2.5 y necesita un control de acceso detallado, debe crear roles manualmente con los siguientes permisos:

```
# Allows users to use all point in time search search functionality
point_in_time_full_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - '*'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/point_in_time/readall"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"


# Allows users to use point in time search search functionality for specific index
# All type operations like list all PITs, delete all PITs are not supported in this
 case

point_in_time_index_access:
  reserved: true
  index_permissions:
    - index_patterns:
        - 'my-index-1'
      allowed_actions:
        - "indices:data/read/point_in_time/create"
        - "indices:data/read/point_in_time/delete"
        - "indices:data/read/search"
        - "indices:monitor/point_in_time/segments"
```

Para los dominios con la versión 2.5 o superior, puede usar el rol integrado `point_in_time_full_access`. Para obtener más información, consulte Security model en la documentación de OpenSearch.

Configuración de PIT

OpenSearch permite cambiar todas las configuraciones de PIT disponibles mediante la API de `_cluster/settings`. En OpenSearch Service, actualmente no es posible modificar la configuración.

Búsqueda en clústeres

Puede crear PIT, buscarlas con identificadores de PIT, enumerarlas y eliminarlas de todos los clústeres con las siguientes limitaciones menores:

- Puede enumerar todos los PIT y eliminarlos solo en el dominio origen.
- No puede minimizar los viajes de ida y vuelta de la red como parte de una consulta de búsqueda entre clústeres.

Para obtener más información, consulte the section called “Búsqueda en clústeres”.

UltraWarm

Las búsquedas PIT con índices de UltraWarm siguen en funcionamiento. Para obtener más información, consulte the section called “UltraWarm almacenamiento”.

> **Note**
>
> Puede monitorear las estadísticas de búsqueda PIT en CloudWatch. Para obtener una lista completa de las métricas, consulte the section called “Métricas de un momento dado”.

Búsqueda semántica en Amazon Service OpenSearch

A partir de la versión 2.9 del OpenSearch Servicio, puede utilizar la búsqueda semántica para comprender las consultas de búsqueda y mejorar la relevancia de las búsquedas. Puede usar la búsqueda semántica de dos maneras: con la búsqueda neuronal y con k-NN.

Con OpenSearch Service, puede configurar conectores de IA para servicios externos Servicios de AWS y para ellos. Con la consola, también puede crear un modelo de ML con una plantilla AWS CloudFormation. Para más información, consulte the section called “CloudFormation integraciones de plantillas”.

Uso de OpenSearch cuadros de mando con Amazon Service OpenSearch

OpenSearch Dashboards es una herramienta de visualización de código abierto diseñada para funcionar con. OpenSearch Amazon OpenSearch Service proporciona una instalación de OpenSearch paneles de control con cada dominio OpenSearch de servicio.

Encontrarás un enlace a los OpenSearch paneles en el panel de control de tu dominio, en la consola de OpenSearch servicio. Para los dominios en ejecución OpenSearch, la URL es*domain-endpoint*`/_dashboards/`. Para los dominios que ejecutan la versión antigua de Elasticsearch, la URL es. *domain-endpoint*`/_plugin/kibana`

Las consultas que utilizan esta instalación predeterminada de OpenSearch Dashboards tienen un tiempo de espera de 300 segundos.

En las siguientes secciones se abordan algunos casos de uso comunes de los paneles: OpenSearch

- the section called “Controlar el acceso a los paneles OpenSearch ”
- the section called “Configuración de los OpenSearch paneles de control para utilizar un servidor de mapas WMS”
- the section called “Conexión de un servidor de Dashboards local a Service OpenSearch ”

Controlar el acceso a los paneles OpenSearch

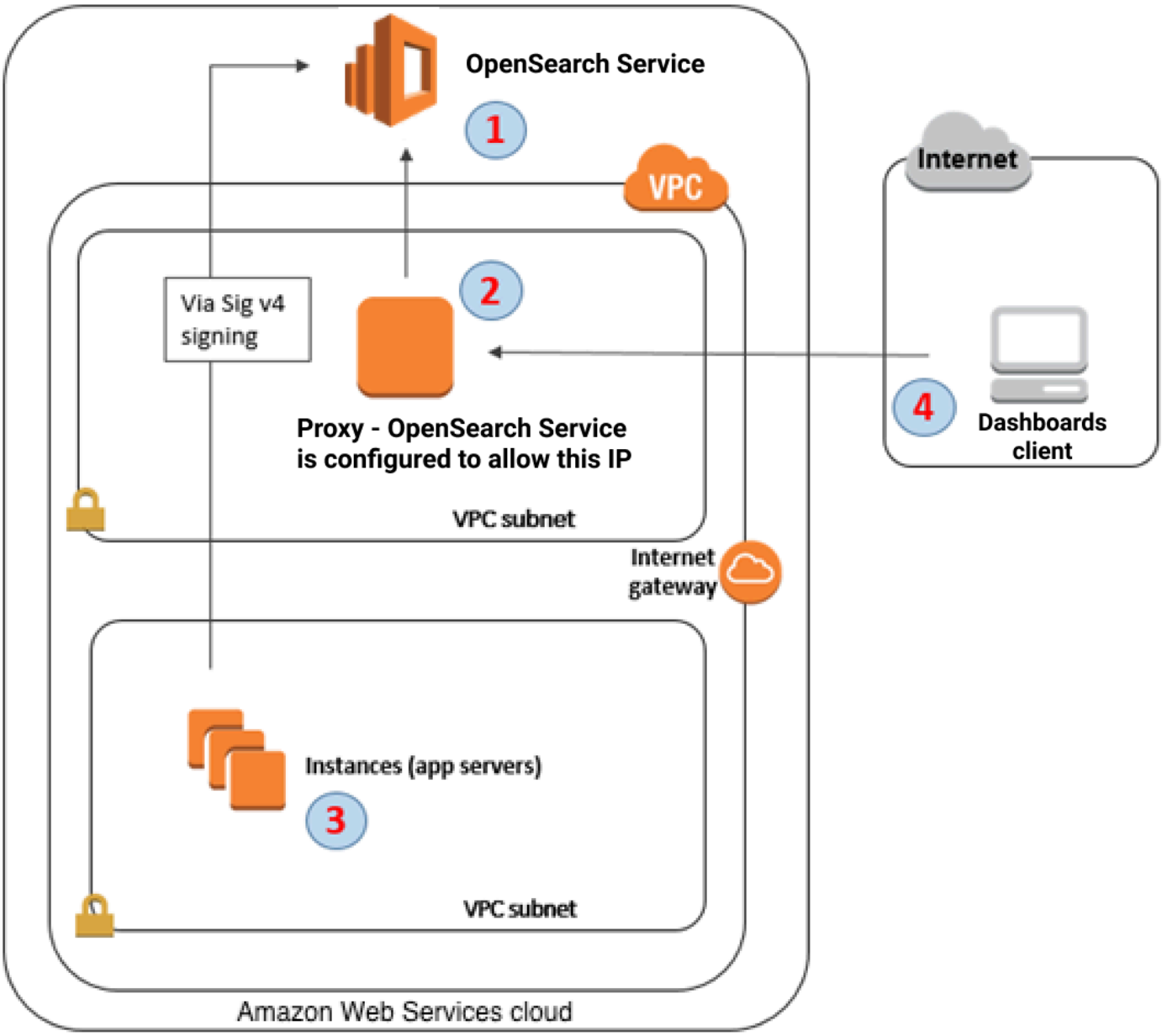
Los paneles no admiten de forma nativa los usuarios y funciones de IAM, pero OpenSearch Service ofrece varias soluciones para controlar el acceso a los paneles:

- Habilite SAML authentication for Dashboards (Autenticación SAML para Dashboards).
- Utilice el control de acceso detallado con autenticación básica de HTTP.
- Configure la autenticación de Cognito para Dashboards.
- Para los dominios de acceso público, configure una política de acceso basada en IP que utilice o no un servidor proxy.
- Para los dominios de acceso a la VPC, configure una política de acceso abierto que utilice o no un servidor proxy, y grupos de seguridad para controlar el acceso. Para obtener más información, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC”.

Uso de un proxy para acceder al servicio desde los paneles OpenSearch OpenSearch

> **Note**
>
> Este proceso solo es de aplicación si el dominio utiliza acceso público y no se desea emplear la autenticación de Cognito. Consulte the section called “Controlar el acceso a los paneles OpenSearch ”.

Como Dashboards es una JavaScript aplicación, las solicitudes se originan en la dirección IP del usuario. El control de acceso basado en IP podría resultar poco práctico debido al gran número de direcciones IP a las que sería necesario brindar acceso para que cada usuario tenga acceso a Dashboards. Una solución alternativa consiste en colocar un servidor proxy entre los OpenSearch paneles y el servicio. OpenSearch A continuación, puede agregar una política de acceso basada en IP que permita solicitudes desde solo una única dirección IP, la del proxy. En el siguiente diagrama se muestra esta configuración.



1. Este es su dominio de OpenSearch servicio. IAM proporciona acceso autorizado a este dominio. Otra política de acceso basada en IP proporciona acceso al servidor proxy.
2. Este es el servidor proxy que se ejecuta en una instancia de Amazon EC2.
3. Otras aplicaciones pueden usar el proceso de firma de la versión 4 de Signature para enviar solicitudes autenticadas al OpenSearch Servicio.
4. OpenSearch Los clientes de Dashboards se conectan a su dominio OpenSearch de servicio a través del proxy.

Para habilitar esta clase de configuración, necesita una política basada en recursos que especifica funciones y direcciones IP. A continuación, mostramos un ejemplo de política:

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Resource": "arn:aws:es:us-west-2:111111111111:domain/my-domain/*",
      "Principal": {
        "AWS": "arn:aws:iam::111111111111:role/allowedrole1"
      },
      "Action": [
        "es:ESHttpGet"
      ],
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": [
            "123.456.789.123"
          ]
        }
      },
      "Resource": "arn:aws:es:us-west-2:111111111111:domain/my-domain/*"
    }
  ]
}
```

Recomendamos configurar la instancia EC2 mediante la ejecución del el servidor proxy con una dirección IP elástica. De esta forma, puede sustituir la instancia cuando sea necesario y continuar adjuntando la misma dirección IP pública a la misma. Para obtener más información, consulte Direcciones IP elásticas en la Guía del usuario de Amazon EC2 para instancias de Linux.

Si utiliza un servidor proxy y la autenticación de Cognito, es posible que tenga que agregar parámetros de configuración para Dashboards y Amazon Cognito con el fin de evitar errores de tipo `redirect_mismatch`. Consulte el siguiente ejemplo de `nginx.conf`:

```
server {
    listen 443;
    server_name $host;
    rewrite ^/$ https://$host/_plugin/_dashboards redirect;

    ssl_certificate           /etc/nginx/cert.crt;
    ssl_certificate_key       /etc/nginx/cert.key;

    ssl on;
    ssl_session_cache  builtin:1000  shared:SSL:10m;
    ssl_protocols  TLSv1 TLSv1.1 TLSv1.2;
    ssl_ciphers HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
    ssl_prefer_server_ciphers on;

    location /_plugin/_dashboards {
        # Forward requests to Dashboards
        proxy_pass https://$dashboards_host/_plugin/_dashboards;

        # Handle redirects to Cognito
        proxy_redirect https://$cognito_host https://$host;

        # Update cookie domain and path
        proxy_cookie_domain $dashboards_host $host;
        proxy_cookie_path / /_plugin/_dashboards/;

        # Response buffer settings
        proxy_buffer_size 128k;
        proxy_buffers 4 256k;
        proxy_busy_buffers_size 256k;
    }

    location ~ \/(log|sign|fav|forgot|change|saml|oauth2) {
        # Forward requests to Cognito
        proxy_pass https://$cognito_host;

        # Handle redirects to Dashboards
        proxy_redirect https://$dashboards_host https://$host;

        # Update cookie domain
        proxy_cookie_domain $cognito_host $host;
    }
}
```

Configuración de los OpenSearch paneles de control para utilizar un servidor de mapas WMS

La instalación predeterminada de OpenSearch Dashboards for OpenSearch Service incluye un servicio de mapas, excepto para los dominios de las regiones de India y China. El servicio de mapas admite hasta 10 niveles de acercamiento/alejamiento.

Con independencia de la región, puede configurar Dashboards para que utilice un servidor de Web Map Service (WMS) diferente para las visualizaciones de mapas de coordenadas. Las visualizaciones de mapas de región solo admiten el servicio de mapas predeterminado.

Para configurar Dashboards para que utilice un servidor de mapas de WMS:

1. Abra Dashboards.
2. Seleccione Stack Management (Gestión de pilas).
3. Seleccione Advanced Settings (Configuración avanzada).
4. Localice visualization:tileMap:WMSdefaults.
5. Cambie `enabled` a `true` y `url` a la URL de un servidor de mapas WMS válido.

```
{
  "enabled": true,
  "url": "wms-server-url",
  "options": {
    "format": "image/png",
    "transparent": true
  }
}
```

6. Seleccione Save changes (Guardar cambios).

Para aplicar el nuevo valor predeterminado a las visualizaciones, es posible que deba volver a cargar Dashboards. Si guardó visualizaciones, elija Options (Opciones) después de abrir la visualización. Verifique que el Servidor de mapas WMS esté habilitado y que la URL de WMS contenga el servidor de mapas preferido y, a continuación, elija Apply changes (Aplicar cambios).

> **Note**
>
> Los servicios de mapa suelen estar sujetos a restricciones o cuotas de licencias. El usuario es responsable de todas estas consideraciones en cualquier servidor de mapas que especifique. Los servicios de mapa de U.S. Geological Survey podrían resultarle útiles para hacer pruebas.

Conexión de un servidor de Dashboards local a Service OpenSearch

Si ya ha invertido una cantidad considerable de tiempo en configurar su propia instancia de OpenSearch Dashboards, puede utilizarla en lugar de (o además de) la instancia de Dashboards predeterminada que OpenSearch proporciona Service. El siguiente procedimiento sirve para dominios que utilicen el control de acceso detallado con una política de acceso abierto.

Para conectar un servidor de OpenSearch Dashboards local a Service OpenSearch

1. En su dominio OpenSearch de servicio, cree un usuario con los permisos adecuados:
   a. En Dashboards, vaya a Security (Seguridad), Internal users (Usuarios internos) y elija Create internal user (Crear usuario interno).
   b. Proporcione un nombre de usuario y una contraseña y elija Create (Crear).
   c. Vaya a Roles (Roles) y elija un rol.
   d. Seleccione Mapped users (Usuarios asignados) y Seleccione Manage mapping (Gestión de mapas).
   e. En Users (Usuarios), agregue el nombre de usuario y elija Map (Asignar).
2. Descargue e instale la versión adecuada del complemento de OpenSearch seguridad en su instalación autogestionada de Dashboards OSS.
3. En su servidor de Dashboards local, abra el `config/opensearch_dashboards.yml` archivo y añada su terminal de OpenSearch servicio con el nombre de usuario y la contraseña que creó anteriormente:

```
opensearch.hosts: ['https://domain-endpoint']
opensearch.username: 'username'
opensearch.password: 'password'
```

Puede utilizar el siguiente ejemplo de archivo `opensearch_dashboards.yml`:

```
server.host: '0.0.0.0'

opensearch.hosts: ['https://domain-endpoint']

opensearch_dashboards.index: ".username"

opensearch.ssl.verificationMode: none # if not using HTTPS

opensearch_security.auth.type: basicauth
opensearch_security.auth.anonymous_auth_enabled: false
opensearch_security.cookie.secure: false # set to true when using HTTPS
opensearch_security.cookie.ttl: 3600000
opensearch_security.session.ttl: 3600000
opensearch_security.session.keepalive: false
opensearch_security.multitenancy.enabled: false
opensearch_security.readonly_mode.roles: ['opensearch_dashboards_read_only']
opensearch_security.auth.unauthenticated_routes: []
opensearch_security.basicauth.login.title: 'Please log in using your username and
 password'

opensearch.username: 'username'
opensearch.password: 'password'
opensearch.requestHeadersWhitelist:
[
authorization,
securitytenant,
security_tenant,
]
```

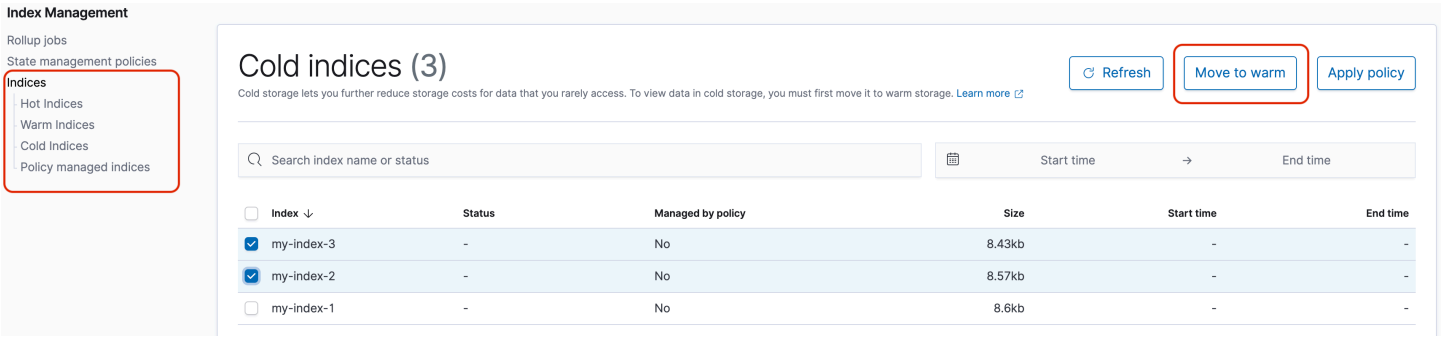
Para ver sus índices OpenSearch de servicio, inicie su servidor de Dashboards local, vaya a Dev Tools y ejecute el siguiente comando:

```
GET _cat/indices
```

Administrar los índices en los paneles OpenSearch

La instalación de OpenSearch Dashboards en su dominio de OpenSearch servicio proporciona una interfaz de usuario útil para administrar los índices en los diferentes niveles de almacenamiento de

su dominio. Seleccione Administración de índices en el menú principal de los paneles para ver todos los índices almacenados en caliente y en frío UltraWarm, así como los índices gestionados por las políticas de Index State Management (ISM). Utilice la administración de índices para mover índices entre el almacenamiento en frío y el almacenamiento en caliente y para monitorear las migraciones entre los tres niveles.



Tenga en cuenta que no verá las opciones de índice de calor, calor y frío a menos que tenga activado el almacenamiento en frío UltraWarm o esté activado.

Características adicionales

La instalación predeterminada de OpenSearch Dashboards en cada dominio OpenSearch de servicio tiene algunas funciones adicionales:

- Interfaces de usuario para los distintos complementos OpenSearch
- Inquilinos
- Informes

  Utilice Reporting (Informes) para generar informes CSV bajo demanda desde la página Discover e informes PDF o PNG de paneles o visualizaciones. Los informes CSV tienen un límite de 10 000 filas.
- Diagramas de Gantt
- Cuadernos

Administración de índices en Amazon OpenSearch Service

Después de agregar datos a Amazon OpenSearch Service, a menudo necesita reindexarlos, trabajar con alias de índice, trasladar un índice a un almacenamiento más rentable o eliminarlo por completo. Este capítulo trata sobre el almacenamiento UltraWarm, el almacenamiento en frío y la administración de estados de índice. Para obtener información sobre las API de índice de OpenSearch, consulte la documentación de OpenSearch.

Temas

UltraWarm almacenamiento para Amazon OpenSearch Service

UltraWarm proporciona una forma rentable de almacenar grandes cantidades de datos de solo lectura en Amazon OpenSearch Service. Los nodos de datos estándar utilizan almacenamiento "en caliente", que adopta la forma de almacenes de instancias o volúmenes de Amazon EBS asociados a cada nodo. El almacenamiento en caliente proporciona el rendimiento más rápido posible para indexar y buscar nuevos datos.

En lugar de almacenamiento adjunto, UltraWarm los nodos utilizan Amazon S3 y una sofisticada solución de almacenamiento en caché para mejorar el rendimiento. En el caso de los índices en los que no está escribiendo activamente, que consultan con menos frecuencia y que no necesitan el mismo rendimiento, UltraWarm ofrecen costes significativamente más bajos por GiB de datos. Dado que los índices calientes son de solo lectura, a menos que se devuelvan al almacenamiento activo, UltraWarm es ideal para datos inmutables, como los registros.

En OpenSearch, los índices cálidos se comportan igual que cualquier otro índice. Puede consultarlos mediante las mismas API o utilizarlos para crear visualizaciones en OpenSearch los paneles de control.

Temas

Requisitos previos

UltraWarm tiene algunos requisitos previos importantes:

- UltraWarm requiere Elasticsearch 6.8 OpenSearch o superior.
- Para utilizar el almacenamiento "warm", los dominios deben tener nodos maestros dedicados.
- Si su dominio utiliza un tipo de instancia T2 o T3 para los nodos de datos, no puede utilizar el almacenamiento templado.
- Si su índice usa códecs de compresión Zstandard (`"index.codec": "zstd"o"index.codec": "zstd_no_dict"`), no puede moverlo a un almacenamiento en caliente.
- Si su índice usa k-NN aproximado (`"index.knn": true`), no puede moverlo al almacenamiento en caliente.

- Si el dominio usa un control de acceso detallado, los usuarios deben estar asignados al `ultrawarm_manager` rol en OpenSearch los paneles para poder realizar llamadas a la API. UltraWarm

> **Note**
>
> Es posible que la `ultrawarm_manager` función no esté definida en algunos dominios de servicio preexistentes. OpenSearch Si no ve el rol en el panel, debe crearlo de forma manual.

Configuración de permisos

Si lo habilita UltraWarm en un dominio de OpenSearch servicio preexistente, es posible que el `ultrawarm_manager` rol no esté definido en el dominio. Los usuarios que no sean administradores deben estar asignados a este rol para poder administrar índices templados en los dominios mediante un control de acceso detallado. Para crear el rol `ultrawarm_manager` de forma manual, siga estos pasos:

1. En los OpenSearch paneles, vaya a Seguridad y elija Permisos.
2. Elija Crear grupo de acciones y configure los siguientes grupos:

Nombre del grupo	Permisos
`ultrawarm_cluster`	• `cluster:admin/ultrawarm/migration/list` • `cluster:monitor/nodes/stats`
`ultrawarm_index_read`	• `indices:admin/ultrawarm/migration/get` • `indices:admin/get`
`ultrawarm_index_write`	• `indices:admin/ultrawarm/migration/warm` • `indices:admin/ultrawarm/migration/hot` • `indices:monitor/stats` • `indices:admin/ultrawarm/migration/cancel`

3. Elija Roles y Crear rol.
4. Asigne al rol el nombre ultrawarm_manager.

5. Para Permisos de clúster, seleccione `ultrawarm_cluster` y `cluster_monitor`.
6. Para Índice, escriba `*`.
7. Para Permisos de índice, seleccione `ultrawarm_index_read`, `ultrawarm_index_write`, y `indices_monitor`.
8. Seleccione Crear.
9. Después de crear el rol, asígnelo a cualquier rol de usuario o backend que UltraWarm administre los índices.

UltraWarm requisitos de almacenamiento y consideraciones de rendimiento

Como se explica en el the section called “Cálculo de requisitos de almacenamiento” apartado anterior, los datos almacenados en caliente suponen una sobrecarga importante: réplicas, espacio reservado en Linux y espacio reservado en el OpenSearch servicio. Por ejemplo, una partición principal de 20 GiB con una partición de réplica requiere aproximadamente 58 GiB de almacenamiento en caliente.

Como utiliza Amazon S3, no UltraWarm incurre en ninguna de estas sobrecargas. Al calcular los requisitos UltraWarm de almacenamiento, solo se tiene en cuenta el tamaño de las particiones principales. La durabilidad de los datos en S3 elimina la necesidad de mantener réplicas y S3 abstrae (y hace innecesarias) las consideraciones de sistemas operativos o de servicio. Esa misma partición de 20 GiB requiere solo 20 GiB de almacenamiento templado. Si aprovisiona una instancia `ultrawarm1.large.search`, puede usar los 20 TiB de su almacenamiento máximo para particiones principales. Consulte the section called “UltraWarm cuotas de almacenamiento” para obtener un resumen de los tipos de instancia y la cantidad máxima de almacenamiento que puede abordar cada uno.

Con UltraWarm, seguimos recomendando un tamaño de fragmento máximo de 50 GiB. El número de núcleos de CPU y la cantidad de RAM asignados a cada tipo de UltraWarm instancia te dan una idea del número de fragmentos que pueden buscar simultáneamente. Tenga en cuenta que, si bien solo los fragmentos principales cuentan para el UltraWarm almacenamiento en S3, los OpenSearch cuadros de mando indican `_cat/indices` el tamaño del UltraWarm índice como el total de todos los fragmentos principales y de réplica.

Por ejemplo, cada instancia de `ultrawarm1.medium.search` tiene dos núcleos de CPU y puede abordar hasta 1,5 TiB de almacenamiento en S3. Dos de estas instancias tienen una combinación de 3 TiB de almacenamiento, que funciona en aproximadamente 62 particiones si cada partición es

de 50 GiB. Si una solicitud al clúster solo busca cuatro de estas particiones, el rendimiento puede ser excelente. Si la solicitud es amplia y busca los 62, es posible que los cuatro núcleos de CPU tengan dificultades para realizar la operación. Supervise las `WarmJVMMemoryPressure` UltraWarm métricas `WarmCPUUtilization` y las métricas para comprender cómo gestionan las instancias sus cargas de trabajo.

Si realiza búsquedas amplias o frecuentes, considere dejar los índices en el almacenamiento caliente. Al igual que cualquier otra OpenSearch carga de trabajo, el paso más importante para determinar si UltraWarm cumple con tus necesidades es realizar pruebas representativas con los clientes utilizando un conjunto de datos realista.

UltraWarm precios

Con el almacenamiento en caliente, se paga lo que se aprovisiona. Algunas instancias requieren un volumen de Amazon EBS asociado, mientras que otras incluyen un almacén de instancias. Tanto si el almacenamiento está vacío como si está lleno, se paga el mismo precio.

Con el UltraWarm almacenamiento, pagas por lo que usas. Una instancia `ultrawarm1.large.search` puede poner a disposición hasta 20 TiB de almacenamiento en S3. Sin embargo, si únicamente se almacena 1 TiB de datos, solo se le facturará 1 TiB de datos. Como todos los demás tipos de nodos, también pagas una tarifa por hora por cada UltraWarm nodo. Para obtener más información, consulte the section called “Precios de Amazon OpenSearch Service”.

Habilitando UltraWarm

La consola es la forma más sencilla de crear un dominio que utiliza almacenamiento templado. Al crear el dominio, elija Habilitar nodos de UltraWarm datos y el número de nodos calientes que desee. El mismo proceso básico funciona en dominios existentes, siempre que cumplan los requisitos previos. Incluso después de que el estado del dominio cambie de Procesado a Activo, es UltraWarm posible que no esté disponible para su uso durante varias horas.

También puedes usar la API de configuración AWS CLIo la API para habilitar UltraWarm`WarmEnabled`, específicamente`WarmCount`, `WarmType` las opciones y`ClusterConfig`.

> **Note**
>
> Los dominios admiten un número máximo de nodos templados. Para más información, consulte the section called “Cuotas”.

Ejemplo de comando de la CLI

El siguiente comando de la AWS CLI crea un dominio con tres nodos de datos, tres nodos maestros dedicados, seis nodos calientes y control de acceso detallado habilitado:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-config
 InstanceCount=3,InstanceType=r6g.large.search,DedicatedMasterEnabled=true,DedicatedMasterType=
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["123456789012"]},"Action":
["es:*"],"Resource":"arn:aws:es:us-west-1:123456789012:domain/my-domain/*"}]}' \
  --region us-east-1
```

Para obtener información detallada, consulte la Referencia de comandos de AWS CLI.

Ejemplo de solicitud a la API de configuración

La siguiente solicitud a la API de configuración crea un dominio con tres nodos de datos, tres nodos maestros dedicados y seis nodos templados con control de acceso detallado habilitado y una política de acceso restrictiva:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
```

```
      "AvailabilityZoneCount": 3
    },
    "WarmEnabled": true,
    "WarmCount": 6,
    "WarmType": "ultrawarm1.medium.search"
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain",
  "AccessPolicies": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":[\"123456789012\"]},\"Action\":[\"es:*\"],\"Resource\":
\"arn:aws:es:us-east-1:123456789012:domain/my-domain/*\"}]}"
}
```

Para obtener información detallada, consulta la referencia de la API OpenSearch de Amazon Service.

Migración de índices al almacenamiento UltraWarm

Si ha terminado de escribir en un índice y ya no necesita el rendimiento de búsqueda más rápido posible, migre el índice a: UltraWarm

```
POST _ultrawarm/migration/my-index/_warm
```

A continuación, verifique el estado de la migración:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_SHARD_RELOCATION",
    "migration_type": "HOT_TO_WARM",
    "shard_level_status": {
      "running": 0,
      "total": 5,
      "pending": 3,
      "failed": 0,
      "succeeded": 2
    }
  }
}
```

El estado del índice debe ser verde para realizar una migración. Si migra varios índices en una sucesión rápida, puede obtener un resumen de todas las migraciones en texto sin formato, similar a la API `_cat`:

```
GET _ultrawarm/migration/_status?v

index    migration_type state
my-index HOT_TO_WARM    RUNNING_SHARD_RELOCATION
```

OpenSearch El servicio migra un índice a la vez a UltraWarm. Se pueden tener hasta 200 migraciones en la cola. Cualquier solicitud que supere el límite será rechazada. Para comprobar el número actual de migraciones en la cola, supervise la métrica de `HotToWarmMigrationQueueSize`. Los índices permanecen disponibles durante todo el proceso de migración, sin tiempo de inactividad.

El proceso de migración tiene los siguientes estados:

```
PENDING_INCREMENTAL_SNAPSHOT
RUNNING_INCREMENTAL_SNAPSHOT
FAILED_INCREMENTAL_SNAPSHOT
```

```
PENDING_FORCE_MERGE
RUNNING_FORCE_MERGE
FAILED_FORCE_MERGE
PENDING_FULL_SNAPSHOT
RUNNING_FULL_SNAPSHOT
FAILED_FULL_SNAPSHOT
PENDING_SHARD_RELOCATION
RUNNING_SHARD_RELOCATION
FINISHED_SHARD_RELOCATION
```

Como indican estos estados, se pueden producir errores en las migraciones si se realizan durante instantáneas, reubicaciones de particiones o fusiones forzosas. Los errores durante las instantáneas o las reubicaciones de particiones suelen deberse a errores de nodo o problemas de conectividad de S3. La falta de espacio en el disco suele ser la causa subyacente de los errores en las fusiones forzosas.

Una vez finalizada la migración, la misma solicitud `_status` devuelve un error. Si comprueba el índice en ese momento, verá algunos parámetros de configuración que son exclusivos de los índices templados:

```
GET my-index/_settings

{
  "my-index": {
    "settings": {
      "index": {
        "refresh_interval": "-1",
        "auto_expand_replicas": "false",
        "provided_name": "my-index",
        "creation_date": "1599241458998",
        "unassigned": {
          "node_left": {
            "delayed_timeout": "5m"
          }
        },
        "number_of_replicas": "1",
        "uuid": "GswyCdR0RSq0SJYmzsIpiw",
        "version": {
          "created": "7070099"
        },
        "routing": {
          "allocation": {
```

```
            "require": {
              "box_type": "warm"
            }
          }
        },
        "number_of_shards": "5",
        "merge": {
          "policy": {
            "max_merge_at_once_explicit": "50"
          }
        }
      }
    }
  }
}
```

- `number_of_replicas`, en este caso, es el número de réplicas pasivas, que no consumen espacio en disco.
- `routing.allocation.require.box_type` especifica que el índice debe usar nodos templados en lugar de nodos de datos estándar.
- `merge.policy.max_merge_at_once_explicit` especifica el número de segmentos que se van a fusionar simultáneamente durante la migración.

Los índices almacenados en caliente son de solo lectura, a menos que se devuelvan al almacenamiento activo, lo que los hace UltraWarm más adecuados para datos inmutables, como los registros. Puede consultar los índices y eliminarlos, pero no puede agregar, actualizar ni eliminar documentos individuales. Si lo intenta, podría encontrarse con el siguiente error:

```
{
  "error" : {
    "root_cause" : [
      {
        "type" : "cluster_block_exception",
        "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage
 exceeded flood-stage watermark, index has read-only-allow-delete block];"
      }
    ],
    "type" : "cluster_block_exception",
    "reason" : "index [indexname] blocked by: [TOO_MANY_REQUESTS/12/disk usage exceeded
 flood-stage watermark, index has read-only-allow-delete block];"
```

```
  },
  "status" : 429
}
```

Automatizar migraciones

Se recomienda utilizar the section called “Index State Management” para automatizar el proceso de migración después de que un índice alcance cierta antigüedad o cumpla otras condiciones. Consulte la política de ejemplo que muestra este flujo de trabajo.

Ajuste de migración

Las migraciones de índices al almacenamiento requieren una fusión forzada. UltraWarm Cada OpenSearch índice se compone de un número determinado de fragmentos y cada fragmento se compone de un número determinado de segmentos de Lucene. La operación de fusión forzada purga los documentos marcados para su eliminación y conserva espacio en disco. De forma predeterminada, UltraWarm fusiona los índices en un segmento.

Puede cambiar este valor hasta 1000 segmentos utilizando la configuración de `index.ultrawarm.migration.force_merge.max_num_segments`. Los valores más altos aceleran el proceso de migración, pero aumentan la latencia de consulta para el índice activo una vez finalizada la migración. Para cambiar la configuración, realice la siguiente solicitud:

```
PUT my-index/_settings
{
  "index": {
    "ultrawarm": {
      "migration": {
        "force_merge": {
          "max_num_segments": 1
        }
      }
    }
  }
}
```

Para comprobar cuánto tiempo tarda esta etapa del proceso de migración, monitoree la métrica de `HotToWarmMigrationForceMergeLatency`.

Cancelación de migraciones

UltraWarm gestiona las migraciones de forma secuencial, en una cola. Si una migración está en la cola, pero aún no se ha iniciado, puede eliminarla de la cola mediante la siguiente solicitud:

```
POST _ultrawarm/migration/_cancel/my-index
```

Si el dominio utiliza un control de acceso detallado, debe tener el permiso de `indices:admin/ultrawarm/migration/cancel` para realizar esta solicitud.

Listado de índices calientes y templados

UltraWarm añade dos opciones adicionales, similares a`_all`, para ayudar a gestionar los índices calientes y cálidos. Para obtener una lista de todos los índices calientes o templados, realice las siguientes solicitudes:

```
GET _warm
GET _hot
```

Puede utilizar estas opciones en otras solicitudes que especifican índices, por ejemplo:

```
_cat/indices/_warm
_cluster/state/_all/_hot
```

Devolución de índices templados al almacenamiento caliente

Si necesita volver a escribir en un índice, vuelva a migrarlo al almacenamiento en caliente:

```
POST _ultrawarm/migration/my-index/_hot
```

Puede tener hasta 10 migraciones en cola de almacenamiento caliente a almacenamiento en caliente a la vez. OpenSearch El servicio procesa las solicitudes de migración de una en una, en el orden en que se pusieron en cola. Para comprobar el número actual, monitoree la métrica de `WarmToHotMigrationQueueSize`.

Una vez finalizada la migración, compruebe la configuración del índice para asegurarse de que satisfaga sus necesidades. Los índices vuelven al almacenamiento caliente con una réplica.

Restauración de índices templados a partir de instantáneas

Además del repositorio estándar para instantáneas automatizadas, UltraWarm añade un segundo repositorio para índices calientes,. `cs-ultrawarm` Cada instantánea de este repositorio contiene solo un índice. Si elimina un índice caliente, su instantánea permanece en el repositorio de `cs-ultrawarm` durante 14 días, al igual que cualquier otra instantánea automatizada.

Cuando restaura una instantánea desde `cs-ultrawarm`, se restaura en el almacenamiento "warm", no en el almacenamiento en caliente. Las instantáneas de los repositorios `cs-automated` y `cs-automated-enc` restauran el almacenamiento en caliente.

Para restaurar una UltraWarm instantánea en un almacenamiento en caliente

1. Identifique la instantánea más reciente que contiene el índice que desea restaurar:

```
GET _snapshot/cs-ultrawarm/_all?verbose=false

{
  "snapshots": [{
    "snapshot": "snapshot-name",
    "version": "1.0",
    "indices": [
      "my-index"
    ]
  }]
}
```

> **Note**
>
> De forma predeterminada, la `GET _snapshot/<repo>` operación muestra información detallada sobre los datos, como la hora de inicio, la hora de finalización y la duración de cada instantánea de un repositorio. La `GET _snapshot/<repo>` operación recupera información de los archivos de cada instantánea contenidos en un repositorio. Si no necesita la hora de inicio, la hora de finalización y la duración y solo necesita el nombre y la información de índice de una instantánea, le recomendamos que utilice el `verbose=false` parámetro al enumerar las instantáneas para minimizar el tiempo de procesamiento y evitar que se agote el tiempo de espera.

2. Si el índice ya existe, elimínelo:

```
DELETE my-index
```

Si no quiere eliminar el índice, debe devolverlo al almacenamiento en caliente y reindexarlo.

3. Restaurar la instantánea:

```
POST _snapshot/cs-ultrawarm/snapshot-name/_restore
```

UltraWarm ignora cualquier configuración de índice que especifique en esta solicitud de restauración, pero puede especificar opciones como `rename_pattern` `yrename_replacement`. Para ver un resumen de las opciones de restauración de OpenSearch instantáneas, consulte la OpenSearch documentación.

Instantáneas manuales de índices templados

Usted puede tomar instantáneas manuales de índices templados, pero no lo recomendamos. El repositorio de automatización `cs-ultrawarm` ya contiene una instantánea para cada índice activo, tomada durante la migración, sin cargo adicional.

De forma predeterminada, el OpenSearch servicio no incluye índices calientes en las instantáneas manuales. Por ejemplo, la siguiente llamada solo incluye índices calientes:

```
PUT _snapshot/my-repository/my-snapshot
```

Si elige tomar instantáneas manuales de índices templados, se aplican varias consideraciones importantes.

- No puede mezclar índices calientes y templados. Por ejemplo, la siguiente solicitud devuelve un error:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,hot-index-1",
  "include_global_state": false
}
```

Si incluyen una mezcla de índices calientes y cálidos, comodín (*) también devuelven un error.

- Solo se puede incluir un índice templado por instantánea. Por ejemplo, la siguiente solicitud devuelve un error:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1,warm-index-2,other-warm-indices-*",
  "include_global_state": false
}
```

  Esta solicitud se realiza correctamente:

```
PUT _snapshot/my-repository/my-snapshot
{
  "indices": "warm-index-1",
  "include_global_state": false
}
```

- Las instantáneas manuales siempre se restauran al almacenamiento en caliente, incluso si originalmente incluían un índice templado.

Migración de índices templados al almacenamiento frío

Si tiene datos UltraWarm que consulta con poca frecuencia, considere la posibilidad de migrarlos a un almacenamiento en frío. El almacenamiento frío está diseñado para los datos a los que solo se accede ocasionalmente o que ya no están en uso activo. No puede leer ni escribir en índices fríos, pero puede migrarlos de nuevo al almacenamiento templado sin costo cada vez que necesite consultarlos. Para obtener instrucciones, consulte the section called “Migración de índices al almacenamiento frío”.

Deshabilitar UltraWarm

La consola es la forma más sencilla de deshabilitar UltraWarm. Elija el dominio, Acciones y Editar la configuración del clúster. Deseleccione Activar nodos de UltraWarm datos y elija Guardar cambios. También puede usar la opción `WarmEnabled` en la API de configuración y en la AWS CLI.

Antes de desactivarlos UltraWarm, debe eliminar todos los índices calientes o migrarlos de nuevo al almacenamiento activo. Cuando el almacenamiento en caliente esté vacío, espere cinco minutos antes de intentar UltraWarm desactivarlo.

Almacenamiento en frío para Amazon OpenSearch Service

El almacenamiento en frío permite almacenar cualquier cantidad de datos históricos o datos a los que se accede con poca frecuencia en el dominio de Amazon OpenSearch Service y analizarlos bajo demanda, a un costo menor que en otros niveles de almacenamiento. El almacenamiento en frío es apropiado si necesita realizar investigaciones periódicas o análisis forenses sobre datos antiguos. Algunos ejemplos prácticos de datos apropiados para el almacenamiento en frío son los registros a los que se accede con poca frecuencia, los datos que se deben conservar para cumplir con los requisitos de conformidad o los registros que tienen valor histórico.

De la misma forma que el almacenamiento UltraWarm, el almacenamiento en frío está respaldado por Amazon S3. Cuando necesite consultar datos almacenados en frío, puede adjuntarlos de forma selectiva a los nodos UltraWarm existentes. Puede administrar la migración y el ciclo de vida de los datos almacenados en frío manualmente o mediante políticas de administración de estados de índice.

Temas

Requisitos previos

El almacenamiento en frío tiene los siguientes requisitos previos:

- El almacenamiento en frío requiere la versión 7.9 o pesterior de OpenSearch o Elasticsearch.
- Para habilitar el almacenamiento en frío en un dominio de OpenSearch Service, también debe habilitar UltraWarm en el mismo dominio.
- Para utilizar el almacenamiento en frío, los dominios deben tener nodos maestros dedicados.
- Si un dominio utiliza un tipo de instancia T2 o T3 para los nodos de datos, no puede utilizar el almacenamiento en frío.
- Si su índice usa códecs de compresión Zstandard (`"index.codec": "zstd"` o `"index.codec": "zstd_no_dict"`), no puede moverlos a un almacenamiento en frío.
- Si su índice usa k-NN aproximado (`"index.knn": true`), no puede moverlo al almacenamiento en frío.
- Si el dominio utiliza el control de acceso detallado, los usuarios no administradores deben estar asignados al rol `cold_manager` en OpenSearch Dashboards para poder administrar índices almacenados en frío.

> **Note**
>
> El rol `cold_manager` puede no existir en algunos dominios de OpenSearch Service preexistentes. Si no ve el rol en el panel, debe crearlo de forma manual.

Configuración de permisos

Si habilita el almacenamiento en frío en un dominio de OpenSearch Service preexistente, el rol `cold_manager` podría no estar definido en el dominio. Si el dominio utiliza el control de acceso detallado, los usuarios que no sean administradores deben estar asignados a este rol para poder administrar índices almacenados en frío. Para crear el rol `cold_manager` de forma manual, siga estos pasos:

1. En OpenSearch Dashboards, vaya a Seguridad y elija Permisos.
2. Elija Crear grupo de acciones y configure los siguientes grupos:

Nombre del grupo	Permisos
`cold_cluster`	• `cluster:monitor/nodes/stats` • `cluster:admin/ultrawarm*` • `cluster:admin/cold/*`
`cold_index`	• `indices:monitor/stats` • `indices:data/read/minmax` • `indices:admin/ultrawarm/migration/get` • `indices:admin/ultrawarm/migration/cancel`

3. Elija Roles y, a continuación, elija Crear rol.
4. Nombre el rol cold_manager.
5. En Permisos de clúster, elija el grupo `cold_cluster` que creó.
6. En Índice, ingrese `*`.
7. En Permisos de índice, elija el grupo `cold_index` que creó.
8. Seleccione Crear.
9. Después de crear el rol, asígnelo a cualquier rol de usuario o backend que administre índices almacenados en frío.

Requisitos de almacenamiento en frío y consideraciones de rendimiento

Dado que el almacenamiento frío utiliza Amazon S3, no conlleva ninguno de los gastos del almacenamiento caliente, tales como réplicas, espacio reservado de Linux y espacio reservado de OpenSearch Service. El almacenamiento en frío no tiene tipos de instancias específicos porque no tiene ninguna capacidad informática asociada a él. Puede almacenar cualquier cantidad de datos en el almacenamiento en frío. Monitoree la métrica `ColdStorageSpaceUtilization` en Amazon CloudWatch para ver cuánto espacio de almacenamiento en frío utiliza.

Precio del almacenamiento en frío

Como sucede con el almacenamiento UltraWarm, con el almacenamiento en frío solo paga por el almacenamiento de datos. No hay ningún costo informático para los datos en frío y no incurrirá en gastos si no hay datos en el almacenamiento en frío.

No incurrirá en cargos de transferencia al mover datos entre los almacenamientos en frío y templado. Mientras se realiza la migración de los índices entre el almacenamiento templado y el frío, sigue pagando por una sola copia del índice. Una vez finalizada la migración, el índice se factura de acuerdo con el nivel de almacenamiento al que se migró. Para obtener más información sobre los precios del almacenamiento frío, consulte Precios de Amazon OpenSearch Service.

Habilitación del almacenamiento en frío

La consola es la forma más sencilla de crear un dominio que utiliza el almacenamiento en frío. Al crear el dominio, elija Habilitación del almacenamiento en frío. El mismo proceso funciona en dominios existentes, siempre que cumplan los requisitos previos. Incluso después de que el estado del dominio cambie de En proceso a Activo, es posible que el almacenamiento en frío no esté disponible para su utilización por varias horas.

También puede utilizar AWS CLI o la API de configuración para habilitar el almacenamiento en frío.

Ejemplo de comando de la CLI

El comando AWS CLI crea un dominio con tres nodos de datos, tres nodos maestros dedicados, almacenamiento en frío habilitado y control de acceso detallado habilitado:

```
aws opensearch create-domain \
  --domain-name my-domain \
  --engine-version Opensearch_1.0 \
  --cluster-
config ColdStorageOptions={Enabled=true},WarmEnabled=true,WarmCount=4,WarmType=ultrawarm1.mediu
 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=11 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-password}' \
  --region us-east-2
```

Para obtener más información, consulte la Referencia de comandos de la AWS CLI.

Ejemplo de solicitud a la API de configuración

La siguiente solicitud a la API de configuración crea un dominio con tres nodos de datos, tres nodos maestros dedicados, almacenamiento en frío habilitado y control de acceso detallado habilitado:

```
POST https://es.us-east-2.amazonaws.com/2021-01-01/opensearch/domain
{
  "ClusterConfig": {
    "InstanceCount": 3,
    "InstanceType": "r6g.large.search",
    "DedicatedMasterEnabled": true,
    "DedicatedMasterType": "r6g.large.search",
    "DedicatedMasterCount": 3,
    "ZoneAwarenessEnabled": true,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 3
     },
    "WarmEnabled": true,
    "WarmCount": 4,
    "WarmType": "ultrawarm1.medium.search",
    "ColdStorageOptions": {
       "Enabled": true
     }
  },
  "EBSOptions": {
    "EBSEnabled": true,
    "VolumeType": "gp2",
    "VolumeSize": 11
  },
  "EncryptionAtRestOptions": {
    "Enabled": true
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": true
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": true,
    "TLSSecurityPolicy": "Policy-Min-TLS-1-2-2019-07"
  },
   "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
```

```
      "MasterUserName": "master-user",
      "MasterUserPassword": "master-password"
    }
  },
  "EngineVersion": "Opensearch_1.0",
  "DomainName": "my-domain"
}
```

Para obtener información detallada, consulte la Referencia de API de Amazon OpenSearch Service.

Administración de índices fríos en OpenSearch Dashboards

Puede administrar índices calientes, templados y fríos con la interfaz de Dashboards existente en el dominio de OpenSearch Service. Dashboards permite migrar índices entre el almacenamiento frío y el templado, así como supervisar el estado de la migración de los índices, sin utilizar la CLI ni la API de configuración. Para obtener más información, consulte Administración de índices en OpenSearch Dashboards.

Migración de índices al almacenamiento frío

Cuando se migran índices al almacenamiento frío, se debe proporcionar un intervalo de tiempo a los datos para facilitar el descubrimiento. Puede elegir un campo de marca temporal basado en los datos del índice, proporcionar de forma manual una marca temporal inicial y final o elegir no especificar una.

Parámetro	Valor admitido	Descripción
`timestamp_field`	Campo de fecha/hora del mapeo de índices.	Los valores mínimo y máximo del campo proporcionado se calculan y almacenan como metadatos `start_time` y `end_time` para el índice almacenado en frío.
`start_time` y `end_time`	Utilice uno de los siguientes formatos: • strict_date_optional_time. Por ejemplo, `yyyy-MM-d`	Los valores proporcionados se almacenan como metadatos `start_time` y `end_time` para el índice almacenado en frío.

Parámetro	Valor admitido	Descripción
	`d'T'HH:mm:ss.SSSZ` o `yyyy-MM-dd` • Fecha de inicio en milisegundos	

Si no desea especificar una marca temporal, agregue `?ignore=timestamp` a la solicitud en su lugar.

La siguiente solicitud migra un índice del almacenamiento templado al almacenamiento en frío y proporciona horas de inicio y finalización para los datos de ese índice:

```
POST _ultrawarm/migration/my-index/_cold
  {
    "start_time": "2020-03-09",
    "end_time": "2020-03-09T23:00:00Z"
  }
```

A continuación, verifique el estado de la migración:

```
GET _ultrawarm/migration/my-index/_status

{
  "migration_status": {
    "index": "my-index",
    "state": "RUNNING_METADATA_RELOCATION",
    "migration_type": "WARM_TO_COLD"
  }
}
```

OpenSearch Service migra un índice por vez al almacenamiento en frío. Se pueden tener hasta 100 migraciones en la cola. Cualquier solicitud que supere el límite será rechazada. Para comprobar el número actual de migraciones en la cola, supervise la métrica de `WarmToColdMigrationQueueSize`. El proceso de migración tiene los siguientes estados:

```
ACCEPTED_COLD_MIGRATION - Migration request is accepted and queued.
RUNNING_METADATA_MIGRATION - The migration request was selected for execution and
 metadata is migrating to cold storage.
```

```
FAILED_METADATA_MIGRATION - The attempt to add index metadata has failed and all
 retries are exhausted.
PENDING_INDEX_DETACH - Index metadata migration to cold storage is completed. Preparing
 to detach the warm index state from the local cluster.
RUNNING_INDEX_DETACH - Local warm index state from the cluster is being removed. Upon
 success, the migration request will be completed.
FAILED_INDEX_DETACH - The index detach process failed and all retries are exhausted.
```

Automatización de las migraciones al almacenamiento en frío

Se recomienda utilizar la Administración de estados de índice para automatizar el proceso de migración después de que un índice alcance cierta antigüedad o cumpla otras condiciones. Consulte el ejemplo de política, que muestra cómo migrar automáticamente los índices del almacenamiento caliente al almacenamiento UltraWarm y luego al almacenamiento frío.

> **Note**
>
> Es necesario un `timestamp_field` explícito para mover los índices al almacenamiento frío mediante una política de administración de estados de índice.

Cancelación de migraciones al almacenamiento en frío

Si una migración al almacenamiento en frío está en cola o con un estado de error, puede cancelar la migración mediante la siguiente solicitud:

```
POST _ultrawarm/migration/_cancel/my-index

{
  "acknowledged" : true
}
```

Si el dominio utiliza un control de acceso detallado, necesita el permiso `indices:admin/ultrawarm/migration/cancel` para realizar esta solicitud.

Listado de índices almacenados en frío

Antes de realizar consultas, puede ver una lista de los índices del almacenamiento frío para decidir cuáles se deben migrar a al almacenamiento UltraWarm con el fin de realizar más análisis. La siguiente solicitud enumera todos los índices almacenados en frío, ordenados por nombre de índice:

```
GET _cold/indices/_search
```

Respuesta de ejemplo

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 3,
  "indices" : [
    {
      "index" : "my-index-1",
      "index_cold_uuid" : "hjEoh26mRRCFxRIMdgvLmg",
      "size" : 10339,
      "creation_date" : "2021-06-28T20:23:31.206Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-2",
      "index_cold_uuid" : "0vIS2n-oROmOWDFmwFIgdw",
      "size" : 6068,
      "creation_date" : "2021-07-15T19:41:18.046Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-3",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Filtrado

Puede filtrar los índices fríos según un patrón de índice basado en prefijos y variaciones del intervalo de tiempo.

La siguiente solicitud presenta una lista de los índices que coinciden con el patrón de prefijo `event-*`:

```
GET _cold/indices/_search
 {
   "filters":{
      "index_pattern": "event-*"
   }
 }
```

Respuesta de ejemplo

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 1,
  "indices" : [
    {
      "index" : "events-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

La siguiente solicitud devuelve índices cuyos campos de metadatos `start_time` y `end_time` están comprendidos entre `2019-03-01` y `2020-03-01`:

```
GET _cold/indices/_search
{
  "filters": {
    "time_range": {
      "start_time": "2019-03-01",
      "end_time": "2020-03-01"
    }
  }
}
```

Respuesta de ejemplo

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
```

```
  "total_results" : 1,
  "indices" : [
    {
      "index" : "my-index",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2019-05-09T00:00Z",
      "end_time" : "2019-09-09T23:00Z"
    }
  ]
}
```

Ordenar

Puede ordenar los índices fríos por campos de metadatos, como el nombre del índice o su tamaño. La siguiente solicitud presenta una lista de todos los índices ordenados por tamaño en orden descendente:

```
GET _cold/indices/_search
 {
 "sort_key": "size:desc"
 }
```

Respuesta de ejemplo

```
{
  "pagination_id" : "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
  "total_results" : 5,
  "indices" : [
    {
      "index" : "my-index-6",
      "index_cold_uuid" : "4eFiab7rRfSvp3slrIsIKA",
      "size" : 32263273,
      "creation_date" : "2021-08-18T18:25:31.845Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-9",
      "index_cold_uuid" : "mbD3ZRVDRI6ONqgEOsJyUA",
      "size" : 57922,
```

```
      "creation_date" : "2021-07-07T23:41:35.640Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    },
    {
      "index" : "my-index-5",
      "index_cold_uuid" : "EaeXOBodTLiDYcivKsXVLQ",
      "size" : 32403,
      "creation_date" : "2021-07-08T00:12:01.523Z",
      "start_time" : "2020-03-09T00:00Z",
      "end_time" : "2020-03-09T23:00Z"
    }
  ]
}
```

Otras claves de ordenamiento válidas son `start_time:asc/desc`, `end_time:asc/desc` y `index_name:asc/desc`.

Paginación

Puede paginar una lista de índices almacenados en frío. Configure el número de índices que se deben devolver por página con el parámetro `page_size` (el valor predeterminado es 10). Cada solicitud `_search` aplicada a los índices fríos devuelve un `pagination_id` que se puede utilizar para llamadas posteriores.

La siguiente solicitud realiza la paginación de los resultados de una solicitud `_search` de los índices fríos y muestra los siguientes 100 resultados:

```
GET _cold/indices/_search?page_size=100
{
"pagination_id": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY"
}
```

Migración de índices fríos al almacenamiento templado

Después de reducir la lista de índices fríos con los criterios de filtrado de la sección anterior, vuelva a migrarlos a UltraWarm, donde puede consultar los datos y utilizarlos para crear visualizaciones.

La siguiente solicitud vuelve a migrar dos índices fríos al almacenamiento templado:

```
POST _cold/migration/_warm
```

```
 {
 "indices": "my-index1,my-index2"
 }


{
  "acknowledged" : true
}
```

Para verificar el estado de la migración y recuperar el ID de migración, envíe la siguiente solicitud:

```
GET _cold/migration/_status
```

Respuesta de ejemplo

```
{
  "cold_to_warm_migration_status" : [
    {
      "migration_id" : "tyLjXCA-S76zPQbPVHkOKA",
      "indices" : [
        "my-index1,my-index2"
      ],
      "state" : "RUNNING_INDEX_CREATION"
    }
  ]
}
```

Para obtener información de migración específica del índice, incluya el nombre del índice:

```
GET _cold/migration/my-index/_status
```

En lugar de especificar un índice, puede ver una lista de los índices por su estado de migración actual. Los valores válidos son `_failed`, `_accepted` y `_all`.

El siguiente comando obtiene el estado de todos los índices de una única solicitud de migración:

```
GET _cold/migration/_status?migration_id=my-migration-id
```

Recupere el ID de migración mediante la solicitud de estado. Para obtener información detallada sobre la migración, agregue `&verbose=true`.

Puede migrar índices del almacenamiento de frío al almacenamiento templado en lotes de 10 o menos, con un máximo de 100 solicitudes que se migran en forma simultánea. Cualquier solicitud que supere el límite será rechazada. Para comprobar el número actual de migraciones que se están llevando a cabo actualmente, supervise la métrica de `ColdToWarmMigrationQueueSize`. El proceso de migración tiene los siguientes estados:

```
ACCEPTED_MIGRATION_REQUEST - Migration request is accepted and queued.
RUNNING_INDEX_CREATION - Migration request is picked up for processing and will create
 warm indexes in the cluster.
PENDING_COLD_METADATA_CLEANUP - Warm index is created and the migration service will
 attempt to clean up cold metadata.
RUNNING_COLD_METADATA_CLEANUP - Cleaning up cold metadata from the indexes migrated to
 warm storage.
FAILED_COLD_METADATA_CLEANUP - Failed to clean up metadata in the cold tier.
FAILED_INDEX_CREATION - Failed to create an index in the warm tier.
```

Restauración de índices fríos a partir de instantáneas

Si necesita restaurar un índice en frío eliminado, puede restaurarlo de nuevo en el nivel cálido siguiendo las instrucciones que aparecen en el documento the section called “Restauración de índices templados a partir de instantáneas” y, a continuación, migrando de nuevo el índice al nivel frío. No puede restaurar un índice en frío eliminado directamente al nivel frío. OpenSearch Service conserva los índices fríos durante 14 días después de que se hayan eliminado.

Cancelación de migraciones del almacenamiento en frío al templado

Si se pone en cola una migración de índice del almacenamiento en frío al templado o si presenta un estado de error, puede cancelarla mediante la siguiente solicitud:

```
POST _cold/migration/my-index/_cancel

{
  "acknowledged" : true
}
```

Para cancelar la migración de un lote de índices (máximo 10 a la vez), especifique el ID de migración:

```
POST _cold/migration/_cancel?migration_id=my-migration-id
```

```
{
  "acknowledged" : true
}
```

Recupere el ID de migración mediante la solicitud de estado.

Actualización de metadatos de índices almacenados en frío

Puede actualizar los campos `start_time` y `end_time` de un índice almacenado en frío:

```
PATCH _cold/my-index
 {
 "start_time": "2020-01-01",
 "end_time": "2020-02-01"
 }
```

No puede actualizar el `timestamp_field` de un índice de almacenamiento en frío.

> **Note**
>
> OpenSearch Dashboards no admite el método PATCH. Utilice curl, Postman o algún otro método para actualizar metadatos almacenados en frío.

Eliminación de índices almacenados en frío

Si no utiliza una política de ISM, puede eliminar los índices fríos de forma manual. La siguiente solicitud elimina un índice almacenado en frío:

```
DELETE _cold/my-index

{
  "acknowledged" : true
}
```

Deshabilitar el almacenamiento en frío

La consola de OpenSearch Service es la forma más sencilla de deshabilitar el almacenamiento en frío. Seleccione el dominio y elija Acciones, Editar la configuración del clúster, luego anule la selección de Habilitar el almacenamiento en frío).

Para utilizar la AWSCLI o la API de configuración, en `ColdStorageOptions`, establezca `"Enabled"="false"`.

Antes de desactivar el almacenamiento frío, debe eliminar todos los índices fríos o volver a migrarlos al almacenamiento templado; de lo contrario, la acción de desactivación no funcionará.

Almacenamiento OR1 para Amazon Service OpenSearch

OR1 es una familia de instancias para Amazon OpenSearch Service que proporciona una forma rentable de almacenar grandes cantidades de datos. Un dominio con instancias OR1 utiliza Amazon Elastic Block Store (Amazon EBS) `gp3` o `io1` volúmenes como almacenamiento principal, y los datos se copian de forma sincrónica a Amazon S3 a medida que llegan. Esta estructura de almacenamiento proporciona un mayor rendimiento de indexación con una alta durabilidad. La familia de instancias OR1 también admite la recuperación automática de datos en caso de error. Para obtener más información acerca de las opciones del tipo de instancia OR1, consulte the section called “Tipos de instancias de generación actual”.

Si está indexando cargas de trabajo de análisis operativo pesadas, como el análisis de registros, la observabilidad o el análisis de seguridad, puede beneficiarse de la mejora del rendimiento y la eficiencia informática de las instancias OR1. Además, la recuperación automática de datos que ofrecen las instancias OR1 mejora la fiabilidad general del dominio.

OpenSearch El servicio envía las métricas OR1 relacionadas con el almacenamiento a Amazon. CloudWatch Para ver una lista de las métricas disponibles, consulte ???.

Las instancias OR1 están disponibles bajo demanda o con precios de instancias reservadas, con una tarifa por hora para las instancias y el almacenamiento aprovisionados en Amazon EBS y Amazon S3.

Temas

- Limitaciones
- En qué se diferencia OR1 del almacenamiento UltraWarm
- Uso de instancias OR1

Limitaciones

Tenga en cuenta las siguientes limitaciones cuando utilice instancias OR1 para su dominio.

- Tu dominio debe ejecutar la OpenSearch versión 2.11 o superior.
- Tu dominio debe tener activado el cifrado en reposo. Para obtener más información, consulte ???.
- Tu dominio debe ser un dominio nuevo. No puedes modificar un dominio existente para usar instancias OR1.
- Si tu dominio usa nodos maestros dedicados, deben usar instancias de Graviton. Para obtener más información sobre los nodos maestros dedicados, consulte???.
- Los tamaños de los fragmentos en las instancias OR1 deben ser inferiores a 100 GiB. Los fragmentos de más de 100 GiB pueden ralentizar los tiempos de recuperación. Si creas fragmentos de más de 100 GiB en instancias OR1 OpenSearch , los bloques de servicio escriben solicitudes en el dominio. Si aún desea utilizar fragmentos de más de 100 GiB, AWS Supportpóngase en contacto con nosotros para solicitar un aumento de cuota.
- El intervalo de actualización de los índices de las instancias OR1 debe ser de 10 segundos o más. El intervalo de actualización predeterminado para las instancias OR1 es de 10 segundos.

En qué se diferencia OR1 del almacenamiento UltraWarm

OpenSearch El servicio proporciona UltraWarm instancias optimizadas para reducir el costo del almacenamiento de datos inactivos. Tanto el OR1 como las UltraWarm instancias almacenan los datos de forma local en Amazon EBS y de forma remota en Amazon S3. Sin embargo, OR1 y UltraWarm las instancias difieren en varios aspectos importantes:

- Las instancias OR1 guardan una copia de los datos en el almacenamiento local y remoto. UltraWarm las instancias, para reducir los costos de almacenamiento, mantienen los datos principalmente en un almacenamiento remoto. Según los patrones de uso, es posible que los muevan al almacenamiento local.
- Las instancias OR1 están activas y pueden aceptar operaciones de lectura y escritura, mientras que los datos de las UltraWarm instancias son de solo lectura hasta que se devuelvan manualmente al almacenamiento activo.
- UltraWarm se basa en las instantáneas del índice para garantizar la durabilidad de los datos. En comparación, las instancias OR1 realizan la replicación y la recuperación entre bastidores. En caso de que aparezca un índice rojo, las instancias OR1 restauran automáticamente los fragmentos que faltan del almacenamiento remoto en Amazon S3. El tiempo de recuperación varía en función del volumen de datos que se van a recuperar.

Para obtener más información sobre el UltraWarm almacenamiento, consulte???.

Uso de instancias OR1

Puede seleccionar instancias OR1 para sus nodos de datos al crear un nuevo dominio con el AWS Management Console, el AWS Command Line Interface (AWS CLI) o el AWS SDK. A continuación, puede indexar y consultar los datos con las herramientas existentes.

Consola

1. Dirígete a la consola OpenSearch de Amazon Service enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios.
3. Seleccione Create domain (Crear un dominio).
4. Ingrese un nombre para el dominio junto con el resto de opciones preferidas. En Familia de instancias, elija OR1. Seleccione Crear para comenzar el proceso de creación del dominio.

AWS CLI

1. Navega hasta tu AWS CLI terminal. Si necesita instalar el AWS CLI, consulte Instalar o actualizar la última versión del AWS CLI.
2. Para utilizar el almacenamiento OR1, debe proporcionar el valor del tamaño del tipo de instancia OR1 específico en el `InstanceType` campo al crear un dominio. También debe habilitar el cifrado en reposo.

   En el siguiente ejemplo, se crea un dominio con instancias OR1 de tamaño `2xlarge`.

```
aws opensearch create-domain \
  --domain-name test-domain \
  --engine-version OpenSearch_2.11 \
  --cluster-config
 "InstanceType=or1.2xlarge.search,InstanceCount=3,DedicatedMasterEnabled=true,DedicatedMast
 \
  --ebs-options "EBSEnabled=true,VolumeType=gp3,VolumeSize=200" \
  --encryption-at-rest-options Enabled=true \
  --advanced-security-options
 "Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions={MasterUserName=test-
user,MasterUserPassword=test-password}" \
  --node-to-node-encryption-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":
```

```
{"AWS":"*"},"Action":"es:*","Resource":"arn:aws:es:us-east-1:account-
id:domain/test-domain/*"}]}'
```

Administración de estados de índice en Amazon OpenSearch Service

La administración de estados de índice (ISM) de Amazon OpenSearch Service permite definir políticas administradas personalizadas para automatizar tareas rutinarias y aplicarlas a índices y patrones de índices. Ya no es necesario configurar y administrar procesos externos para ejecutar las operaciones de índice.

Una política incluye un estado predeterminado y una lista de estados para que el índice pase de un estado al otro. Dentro de cada estado, se puede definir una lista de acciones para realizar y las condiciones que activan estas transiciones. Un caso de uso típico es eliminar periódicamente los índices antiguos después de un determinado periodo de tiempo. Por ejemplo, puede definir una política que mueva el índice a un estado `read_only` después de 30 días y, a continuación, lo elimine después de 90 días.

Después de adjuntar una política a un índice, ISM crea un trabajo que se ejecuta cada 5 a 8 minutos (o cada 30 a 48 minutos en los clústeres de la versión 1.3 y anteriores) para realizar acciones de políticas, verificar condiciones y pasar el índice a estados diferentes. El tiempo base para que este trabajo se ejecute es cada 5 minutos, además de una fluctuación aleatoria del 0 al 60 % para asegurarse de que no se produzca un aumento de la actividad de todos los índices al mismo tiempo. ISM no ejecuta trabajos si el estado del clúster es rojo.

ISM requiere OpenSearch o Elasticsearch 6.8 o posterior. La documentación completa se encuentra disponible en la documentación de OpenSearch.

> **Important**
>
> Ya no se pueden utilizar plantillas de índice para aplicar políticas de ISM a los índices recién creados. Puede seguir administrando automáticamente los índices recién creados con el campo de plantillas de ISM. Esta actualización presenta un cambio interrumpido que afecta a las plantillas existentes de CloudFormation mediante esta configuración.

Crear una política de ISM

Para empezar a utilizar la administración de estados de índice

1. Abra la consola de Amazon OpenSearch Service en https://console.aws.amazon.com/aos/home.
2. Seleccione el dominio para el que desea crear una política de ISM.
3. En el panel de control del dominio, navegue hasta la URL de OpenSearch Dashboards e inicie sesión con su nombre de usuario maestro y contraseña. La URL tiene este formato:

   ```
   domain-endpoint/_dashboards/
   ```

4. Abra el panel de navegación izquierdo en OpenSearch Dashboards y elija Administración de índices, luego Crear política.
5. Utilice el editor visual o el editor de JSON para crear políticas. Se recomienda utilizar el editor visual, ya que ofrece una forma más estructurada de definir las políticas. Para obtener ayuda para crear políticas, consulte las políticas de muestra a continuación.
6. Después de crear una política, puede adjuntarla a uno o más índices:

   ```
   POST _plugins/_ism/add/my-index
   {
     "policy_id": "my-policy-id"
   }
   ```

   > **Note**
   >
   > Si su dominio ejecuta una versión de Elasticsearch heredada, utilice `_opendistro` en lugar de `_plugins`.

   Como alternativa, puede elegir el índice en OpenSearch Dashboards y, a continuación, elegir Aplicar política.

Ejemplos de política

Los siguientes ejemplos de política muestran cómo automatizar los casos de uso comunes de ISM.

Traspaso de almacenamiento en caliente a templado y a frío

Este ejemplo de política mueve un índice del almacenamiento en caliente al almacenamiento UltraWarm y, finalmente, al almacenamiento en frío. A continuación, elimina el índice.

El índice se encuentra inicialmente en el estado `hot`. Transcurridos 10 días, ISM lo mueve al estado `warm`. 80 días más tarde, cuando el índice tiene 90 días, ISM lo mueve al estado `cold`. Luego de un año, el servicio envía una notificación a una sala de Amazon Chime que indica que el índice está siendo eliminado y, a continuación, lo elimina permanentemente.

Tenga en cuenta que los índices fríos requieren la operación `cold_delete`, en lugar de la operación `delete` normal. Tenga en cuenta también que es necesario un `timestamp_field` explícito en los datos para administrar índices fríos con ISM.

```
{
  "policy": {
    "description": "Demonstrate a hot-warm-cold-delete workflow.",
    "default_state": "hot",
    "schema_version": 1,
    "states": [{
        "name": "hot",
        "actions": [],
        "transitions": [{
          "state_name": "warm",
          "conditions": {
            "min_index_age": "10d"
          }
        }]
      },
      {
        "name": "warm",
        "actions": [{
          "warm_migration": {},
          "retry": {
            "count": 5,
            "delay": "1h"
          }
        }],
        "transitions": [{
          "state_name": "cold",
          "conditions": {
            "min_index_age": "90d"
          }
```

```
        }]
      },
      {
        "name": "cold",
        "actions": [{
            "cold_migration": {
              "timestamp_field": "<your timestamp field>"
            }
          }
        ],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
             "min_index_age": "365d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "notification": {
            "destination": {
              "chime": {
                "url": "<URL>"
              }
            },
            "message_template": {
              "source": "The index {{ctx.index}} is being deleted."
            }
          }
        },
        {
          "cold_delete": {}
        }]
      }
    ]
  }
}
```

Reducir el recuento de réplicas

Este ejemplo de política reduce el recuento de réplicas a cero, después de siete días, para conservar espacio en disco y, a continuación, elimina el índice después de 21 días. Esta política supone que su

índice no es crítico y ya no recibe solicitudes de escritura; tener cero réplicas conlleva cierto riesgo de pérdida de datos.

```
{
  "policy": {
    "description": "Changes replica count and deletes.",
    "schema_version": 1,
    "default_state": "current",
    "states": [{
        "name": "current",
        "actions": [],
        "transitions": [{
          "state_name": "old",
          "conditions": {
            "min_index_age": "7d"
          }
        }]
      },
      {
        "name": "old",
        "actions": [{
          "replica_count": {
            "number_of_replicas": 0
          }
        }],
        "transitions": [{
          "state_name": "delete",
          "conditions": {
            "min_index_age": "21d"
          }
        }]
      },
      {
        "name": "delete",
        "actions": [{
          "delete": {}
        }],
        "transitions": []
      }
    ]
  }
}
```

Tomar una instantánea de índice

Este ejemplo de política utiliza la operación `snapshot` para tomar una instantánea de un índice tan pronto como contenga al menos un documento. `repository` es el nombre del repositorio de instantáneas manual que registró en Amazon S3. `snapshot` es el nombre de la instantánea. Para obtener más información sobre los requisitos previos de una instantánea y los pasos para registrar un repositorio, consulte the section called “Crear instantáneas de índice”.

```
{
  "policy": {
    "description": "Takes an index snapshot.",
    "schema_version": 1,
    "default_state": "empty",
    "states": [{
        "name": "empty",
        "actions": [],
        "transitions": [{
          "state_name": "occupied",
          "conditions": {
            "min_doc_count": 1
          }
        }]
      },
      {
        "name": "occupied",
        "actions": [{
          "snapshot": {
            "repository": "<my-repository>",
            "snapshot": "<my-snapshot>"
            }
          }],
          "transitions": []
      }
    ]
  }
}
```

Plantillas de ISM

Puede configurar un campo `ism_template` en una política, de modo que cuando se cree un índice que coincida con el patrón de plantilla, la política se adjuntará automáticamente a ese índice. En

este ejemplo, cualquier índice que cree con un nombre que comience por “registro” se hace coincidir automáticamente con la política de ISM `my-policy-id`:

```
PUT _plugins/_ism/policies/my-policy-id
{
  "policy": {
    "description": "Example policy.",
    "default_state": "...",
    "states": [...],
    "ism_template": {
      "index_patterns": ["log*"],
      "priority": 100
    }
  }
}
```

Para ver un ejemplo más detallado, consulte Ejemplo de política con plantillas de ISM para reversión automática.

Diferencias

En comparación con OpenSearch y Elasticsearch, ISM para Amazon OpenSearch Service presenta varias diferencias.

Operaciones ISM

- OpenSearch Service es compatible con tres operaciones de ISM únicas, `warm_migration`, `cold_migration` y `cold_delete`:
  - Si su dominio tiene UltraWarm habilitado, la acción `warm_migration` pasa el índice al almacenamiento templado.
  - Si el dominio tiene habilitado el almacenamiento frío, la acción `cold_migration` pasa el índice al almacenamiento frío, y la acción `cold_delete` elimina el índice del almacenamiento frío.

  Aunque una de estas acciones no se complete dentro del periodo de tiempo de espera establecido, la migración o eliminación de los índices prosigue. Configuración de un error_notification de una de las acciones anteriores, le notificará que la acción falla por no haberse completado dentro del periodo de tiempo de espera, pero la notificación es solo para su propia referencia. La propia operación no tiene un tiempo de espera inherente, y continúa ejecutándose hasta que finalmente se completa correctamente o falla.

- Si el dominio ejecuta OpenSearch o Elasticsearch 7.4 o posterior, el servicio OpenSearch admite las operaciones `open` y `close` de ISM.

- Si el dominio ejecuta OpenSearch o Elasticsearch 7.7 o posterior, el servicio OpenSearch admite la operación `snapshot`.

Operaciones de ISM de almacenamiento en frío

Para índices almacenados en frío, debe especificar un parámetro `?type=_cold` cuando utilice las siguientes API de ISM:

- Agregar política
- Quitar política
- Actualizar política
- Reintentar índice fallido
- Explicar índice

Estas API para índices fríos tienen las siguientes diferencias adicionales:

- Los operadores comodín no son compatibles excepto cuando se utilizan al final. Por ejemplo, se admite `_plugins/_ism/<add, remove, change_policy, retry, explain>/logstash-*`, pero no `_plugins/_ism/<add, remove, change_policy, retry, explain>/iad-*-prod`.
- No se admiten varios nombres y patrones de índices. Por ejemplo, se admite `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs`, pero no `_plugins/_ism/<add, remove, change_policy, retry, explain>/app-logs,sample-data`.

Configuración de ISM

OpenSearch y Elasticsearch permite cambiar todas las configuraciones de ISM disponibles mediante la API `_cluster/settings`. En Amazon OpenSearch Service, solo puede cambiar la siguiente configuración de ISM:

- Configuración de nivel de clúster:
  - `plugins.index_state_management.enabled`

  - `plugins.index_state_management.history.enabled`
- Configuración de nivel de índice:
  - `plugins.index_state_management.rollover_alias`

Tutorial: Automatización de los procesos de administración del estado del índice

Este tutorial demuestra cómo implementar una política de ISM que automatiza tareas rutinarias de administración de índices y las aplica a índices y patrones de índices.

Administración de estados de índice (ISM) de Amazon OpenSearch Service le permite automatizar las actividades recurrentes de administración de índices para evitar el uso de herramientas adicionales para administrar los ciclos de vida de los índices. Puede crear una política que automatice estas operaciones en función de la antigüedad del índice, el tamaño y otras condiciones, todo desde su dominio de Amazon OpenSearch Service.

OpenSearch Service admite tres niveles de almacenamiento: el estado “activo” predeterminado para la escritura activa y el análisis de baja latencia, UltraWarm para datos de solo lectura de hasta tres petabytes y el almacenamiento en frío para el archivado ilimitado a largo plazo.

Este tutorial presenta un caso de uso de ejemplo del manejo de datos de serie temporal en índices diarios. En este tutorial, configurará una política que tome una instantánea automática de cada índice adjunto después de 24 horas. A continuación, la política cambia el índice del estado activo predeterminado al almacenamiento UltraWarm después de dos días, al almacenamiento en frío después de 30 días y, por último, elimina el índice después de 60 días.

Requisitos previos

- El dominio de OpenSearch Service debe ejecutar Elasticsearch 6.8 o versiones posteriores.
- Su dominio debe tener almacenamiento UltraWarm y en frío habilitados.
- Debe registrar un repositorio de instantáneas manuales para su dominio.
- Su rol de usuario necesita permisos suficientes para acceder a la consola de OpenSearch Service. Si es necesario, valide y configure el acceso a su dominio.

Paso 1: configurar la política de ISM

Primero, configure una política de ISM en OpenSearch Dashboards.

1. En el panel del dominio en la consola de OpenSearch Service, diríjase a la URL de paneles de OpenSearch Dashboards e inicie sesión con su nombre de usuario maestro y contraseña. La URL tiene este formato: *domain-endpoint*/_dashboards/.
2. En OpenSearch Dashboards, elija Agregar datos de ejemplo y agregue uno o más de los índices de muestra a su dominio.
3. Abra el panel de navegación izquierdo y elija Administración de índices y, luego, Crear política.
4. Llame `ism-policy-example` a la política.
5. Reemplace la política predeterminada con la siguiente política:

```
{
  "policy": {
    "description": "Move indexes between storage tiers",
    "default_state": "hot",
    "states": [
      {
        "name": "hot",
        "actions": [],
        "transitions": [
          {
            "state_name": "snapshot",
            "conditions": {
              "min_index_age": "24h"
            }
          }
        ]
      },
      {
        "name": "snapshot",
        "actions": [
          {
            "retry": {
              "count": 5,
              "backoff": "exponential",
              "delay": "30m"
            },
            "snapshot": {
              "repository": "snapshot-repo",
```

```
            "snapshot": "ism-snapshot"
          }
        }
      ],
      "transitions": [
        {
          "state_name": "warm",
          "conditions": {
            "min_index_age": "2d"
          }
        }
      ]
    },
    {
      "name": "warm",
      "actions": [
        {
          "retry": {
            "count": 5,
            "backoff": "exponential",
            "delay": "1h"
          },
          "warm_migration": {}
        }
      ],
      "transitions": [
        {
          "state_name": "cold",
          "conditions": {
            "min_index_age": "30d"
          }
        }
      ]
    },
    {
      "name": "cold",
      "actions": [
        {
          "retry": {
            "count": 5,
            "backoff": "exponential",
            "delay": "1h"
          },
          "cold_migration": {
```

```
              "start_time": null,
              "end_time": null,
              "timestamp_field": "@timestamp",
              "ignore": "none"
            }
          }
        ],
        "transitions": [
          {
            "state_name": "delete",
            "conditions": {
              "min_index_age": "60d"
            }
          }
        ]
      },
      {
        "name": "delete",
        "actions": [
          {
            "cold_delete": {}
          }
        ],
        "transitions": []
      }
    ],
    "ism_template": [
      {
        "index_patterns": [
          "index-*"
        ],
        "priority": 100
      }
    ]
  }
}
```

> **Note**
>
> El campo `ism_template` adjunta automáticamente la política a cualquier índice creado recientemente que coincida con uno de los valores `index_patterns` especificados. En este caso, todos los índices que comiencen por `index-`. Puede modificar este

campo para que coincida con un formato de índice de su entorno. Para más información, consulte Plantillas de ISM.

6. En la sección `snapshot` de la política, sustituya *`snapshot-repo`* por el nombre del repositorio de instantáneas que registró para su dominio. También puede optar por sustituir *`ism-snapshot`*, que será el nombre de la instantánea cuando se cree.
7. Seleccione Crear. La política se puede ver ahora en la página Políticas de administración de estados.

Paso 2: adjuntar la política a uno o más índices

Ya que creó la política, puede adjuntarla a uno o más índices de su clúster.

1. Vaya a la pestaña Índices activos y busque `opensearch_dashboards_sample`, donde se enumeran todos los índices de muestra que agregó en el paso 1.
2. Seleccione todos los índices y elija Aplicar política y, a continuación, elija la política ism-policy-example que acaba de crear.
3. Seleccione Aplicar.

Puede supervisar los índices a medida que pasan por los distintos estados de la página Índices administrados por políticas.

Resumen de índices en Amazon OpenSearch Service con acumulaciones de índices

Las acumulaciones de índices de Amazon OpenSearch Service permiten reducir los costos de almacenamiento mediante la acumulación periódica de datos antiguos en índices resumidos.

Elija los campos en los que está interesado y utilice una acumulación de índices para crear un nuevo índice con solo los campos agregados en buckets de tiempo más rigurosos. Puede almacenar meses o años de datos históricos a una fracción del costo con el mismo rendimiento de consulta.

Las acumulaciones de índices requieren OpenSearch o Elasticsearch 7.9 o versiones posteriores. Encontrará la documentación completa sobre esta característica en la documentación de OpenSearch.

Crear un trabajo acumulativo de índices

Para comenzar, elija Index Management (Gestión de índices) en OpenSearch Dashboards. Seleccione Rollup Jobs (Trabajos de acumulación) y elija Create rollup job (Creación de un trabajo de acumulación).

Paso 1: configurar índices

Configure los índices de fuente y destino. El índice de fuente es el que desea resumir. El índice de destino es donde se guardan los resultados de la acumulación de índices.

Después de crear un trabajo de acumulación de índices, no puede cambiar las selecciones de índices.

Paso 2: definir agregaciones y métricas

Seleccione los atributos con las agregaciones (términos e histogramas) y métricas (promedio, suma, máximo, mínimo y recuento de valores) que desea acumular. Asegúrese de no agregar muchos atributos altamente pormenorizados, ya que no ahorrará mucho espacio.

Paso 3: especificar las programaciones

Especifique una programación para acumular los índices a medida que se ingieren. El trabajo de acumulación de índices está habilitado de forma predeterminada.

Paso 4: revisar y crear

Revise su configuración y seleccione Create (Crear).

Paso 5: buscar en el índice objetivo

Puede utilizar la API `_search` estándar para buscar en el índice de destino. No se puede acceder a la estructura interna de los datos en el índice de destino porque el complemento vuelve a escribir automáticamente la consulta en segundo plano para adaptarse al índice de destino. Esto es para asegurarse de que puede utilizar la misma consulta para el índice de fuente y destino.

Para consultar el índice de destino, establezca `size` en 0:

```
GET target_index/_search
```

```
{
  "size": 0,
  "query": {
    "match_all": {}
  },
  "aggs": {
    "avg_cpu": {
      "avg": {
        "field": "cpu_usage"
      }
    }
  }
}
```

> **Note**
>
> Las versiones 2.2 y posteriores de OpenSearch admiten la búsqueda de varios índices acumulativos en una sola solicitud. Las versiones de OpenSearch anteriores a la 2.2 y las versiones de Elasticsearch OSS heredadas solo admiten un índice acumulativo por búsqueda.

Transformación de índices en Amazon OpenSearch Service

Mientras que los trabajos acumulativos de índices le permiten reducir la granularidad de los datos acumulando datos antiguos en índices condensados, los trabajos de transformación le permiten crear una vista resumida diferente de sus datos centrada en ciertos campos, de modo que pueda visualizar o analizar los datos de diferentes maneras.

Las transformaciones de índice tienen una interfaz de usuario de OpenSearch Dashboards y API REST. La función requiere OpenSearch 1.0 o posterior. La documentación completa Prepper se encuentra disponible en la documentación de OpenSearch.

Creación de un trabajo de transformación de índice

Si no tiene ningún dato en el clúster, use los datos de vuelo de ejemplo de los paneles de OpenSearch para probar trabajos de transformación. Después de agregar los datos, inicie OpenSearch Dashboards. A continuación, elija Administración de índices, Trabajos de transformación, y Crear trabajo de transformación.

Paso 1: Elegir índices

En la sección Índices, seleccione el índice de origen y destino. Puede seleccionar un índice de destino existente o crear uno nuevo introduciendo un nombre para él.

Si desea transformar solo un subconjunto de su índice fuente, elija Agregar filtro de datos, y utilice la herramienta de OpenSearch consulta de DSL para especificar un subconjunto de su índice de origen.

Paso 2: Elegir los campos

Después de elegir los índices, elija los campos que desea utilizar en el trabajo de transformación, así como si desea utilizar agrupaciones o agregaciones.

- Puede utilizar agrupaciones para colocar los datos en depósitos separados en el índice transformado. Por ejemplo, si desea agrupar todos los destinos de aeropuerto dentro de los datos de vuelo de muestra, agrupe el `DestAirportID` en un campo de destino de `DestAirportID_terms` y puede encontrar los ID de aeropuerto agrupados en el índice transformado una vez finalizado el trabajo de transformación.
- Por otro lado, las agregaciones le permiten realizar cálculos simples. Por ejemplo, puede incluir una agregación en el trabajo de transformación para definir un nuevo campo de `sum_of_total_ticket_price` que calcula la suma de todos los billetes de avión. A continuación, puede analizar los nuevos datos en su índice transformado.

Paso 3: Especificar un programa

Los trabajos de transformación están habilitados de forma predeterminada y se ejecutan en programaciones. Para transform execution interval (intervalo de ejecución de transformación), especifique un intervalo en minutos, horas o días.

Paso 4: Revisar y supervisar

Revise su configuración y seleccione Crear. A continuación, monitoree la columna Estado del trabajo de transformación.

Paso 5: Buscar en el índice objetivo

Una vez finalizado el trabajo, puede usar la API `_search` para buscar en el índice de destino.

Por ejemplo, después de ejecutar un trabajo de transformación que transforma los datos de vuelo basados en el campo `DestAirportID`, puede ejecutar la siguiente solicitud para devolver todos los campos que tienen un valor de `SFO`:

```
GET target_index/_search
{
  "query": {
    "match": {
      "DestAirportID_terms" : "SFO"
    }
  }
}
```

Replicación entre clústeres de Amazon OpenSearch Service

Con la replicación entre clústeres de Amazon OpenSearch Service, se pueden replicar índices de usuario, asignaciones y metadatos de un dominio de OpenSearch Service a otro. Utilizar la replicación entre clústeres contribuye a garantizar la posibilidad de recuperación de desastres en caso de interrupción, y permite replicar datos entre centros de datos lejanos geográficamente para reducir la latencia. Usted paga los cargos de estándar de translerencia de datos AWS para los datos transferidos entre dominios.

La replicación entre clústeres sigue un modelo de replicación activa-pasiva en el que el índice local o seguidor extrae datos del índice remoto o principal. El índice líder hace referencia al origen de los datos o al índice desde el que desea replicar los datos. El índice seguidor hace referencia al destino de los datos o al índice en donde desea replicar los datos.

La replicación entre clústeres está disponible en los dominios que ejecutan Elasticsearch 7.10 o OpenSearch 1.1 o posterior. La documentación completa sobre la replicación entre clústeres se encuentra disponible en la documentación de OpenSearch.

Temas

- Confirmación de replicación
- Pausa y reanudación de la replicación
- Detención de la replicación
- Seguimiento automático
- Actualización de los dominios conectados

Limitaciones

La replicación entre clústeres tiene las siguientes limitaciones:

- No se pueden replicar datos entre dominios de Amazon OpenSearch Service y clústeres de OpenSearch o Elasticsearch autoadministrados.
- No puede replicar un índice de un dominio seguidor a otro dominio seguidor. Si desea replicar un índice en varios dominios seguidores, solo puede replicarlo desde el dominio líder único.
- Se puede conectar un dominio, mediante una combinación de conexiones de entrada y salida, a un máximo de 20 dominios más.
- Al configurar inicialmente una conexión entre clústeres, el dominio principal debe estar en la misma versión o en una versión superior a la del dominio seguidor.
- No puede usar AWS CloudFormation para conectar dominios.
- No se puede utilizar la replicación entre clústeres en instancias M3 o bursátiles (T2 y T3).
- No puede replicar datos entre índices UltraWarm o frío. Ambos índices deben estar almacenados en caliente.
- Al eliminar un índice del dominio principal, el índice correspondiente en el dominio seguidor no se elimina automáticamente.

Requisitos previos

Antes de configurar la replicación entre clústeres, asegúrese de que los dominios cumplan los siguientes requisitos:

- Elasticsearch 7.10 u OpenSearch 1.1 o posterior
- Control de acceso detallado habilitado
- Cifrado de nodo a nodo habilitado

Requisitos de los permisos

Para iniciar la replicación, debe incluir el permiso `es:ESCrossClusterGet` en el dominio remoto (líder). Recomendamos la siguiente política de IAM en el dominio remoto. Esta política también permite realizar otras operaciones, como indexar documentos y efectuar búsquedas estándar:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "*"
        ]
      },
      "Action": [
        "es:ESHttp*"
      ],
      "Resource": "arn:aws:es:region:account:domain/leader-domain/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:ESCrossClusterGet",
      "Resource": "arn:aws:es:region:account:domain/leader-domain"
    }
  ]
}
```

Asegúrese de que el permiso `es:ESCrossClusterGet` se aplica para `/leader-domain` y no `/leader-domain/*`.

Para que los usuarios que no son administradores puedan realizar actividades de replicación, también se les deben asignar los permisos adecuados. La mayoría de los permisos corresponden a operaciones de API REST específicas. Por ejemplo, el permiso `indices:admin/plugins/replication/index/_resume` permite reanudar la replicación de un índice. Para obtener una lista completa de permisos, consulte Permisos de replicación en la documentación de OpenSearch.

> **Note**
>
> Los comandos para iniciar la replicación y crear una regla de replicación son casos especiales. Dado que invocan procesos en segundo plano en los dominios líder y seguidor, se debe pasar un elemento `leader_cluster_role` y `follower_cluster_role` en la solicitud. OpenSearch Service utiliza estos roles en todas las tareas de replicación de backend. Para obtener más información sobre la asignación y el uso de estos roles, consulte Asignación de los roles de clúster líder y seguidor en la documentación de OpenSearch.

Configuración de una conexión entre clústeres

Para replicar índices de un dominio a otro, se debe configurar una conexión entre clústeres entre los dominios. La forma más sencilla de conectar dominios es a través de la pestaña Connections (Conexiones) del panel del dominio. También puede usar la API de configuración o la AWS CLI. Dado que la replicación entre clústeres sigue un modelo de "extracción", las conexiones se inician desde el dominio seguidor.

> **Note**
>
> Si se han conectado anteriormente dos dominios para realizar búsquedas entre clústeres, no se puede usar la misma conexión para la replicación. La conexión está marcada como `SEARCH_ONLY` en la consola. Para realizar la replicación entre dos dominios conectados previamente, se debe eliminar la conexión y volver a crearla. Una vez que se haya hecho esto, la conexión queda disponible tanto para la búsqueda entre clústeres como para la replicación entre clústeres.

Para configurar una conexión

1. En la consola de Amazon OpenSearch Service, seleccione el dominio seguidor, vaya a la pestaña Connections (Conexiones) y elija Request (Solicitar).
2. En Alias de conexión, ingrese un nombre para la conexión.
3. Elija entre conectarse a un dominio de su Cuenta de AWS y región, o hacerlo a otra cuenta o región.

   - Para conectarse a un dominio de su Cuenta de AWS y región, seleccione el dominio y elija Solicitar.

- Para conectarse a un dominio de otra Cuenta de AWS o región, especifique el ARN del dominio remoto y elija Solicitar.

OpenSearch Service valida la solicitud de conexión. Si los dominios son incompatibles, se produce un error en la conexión. Si la validación se realiza correctamente, se envía al dominio de destino para su aprobación. Cuando el dominio de destino aprueba la solicitud, puede iniciar la replicación.

La replicación entre clústeres admite replicación bidireccional. Esto significa que puede crear una conexión saliente del dominio A al dominio B y otra conexión saliente del dominio B al dominio A. A continuación, puede configurar la replicación para que el dominio A siga un índice en el dominio B y el dominio B siga un índice en el dominio A.

Inicio de la replicación

Después de establecer una conexión entre clústeres, puede empezar a replicar datos. En primer lugar, cree un índice en el dominio líder que se va a replicar:

```
PUT leader-01
```

Para replicar ese índice, envíe este comando al dominio seguidor:

```
PUT _plugins/_replication/follower-01/_start
{
   "leader_alias": "connection-alias",
   "leader_index": "leader-01",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Puede encontrar el alias de conexión en la pestaña Conexiones del panel de control del dominio.

Para simplificar, en este ejemplo se supone que un administrador emite la solicitud y utiliza `all_access` para los elementos `leader_cluster_role` y `follower_cluster_role`. No obstante, en entornos de producción, se recomienda crear usuarios de replicación en los índices líder y seguidor, y asignarlos como corresponda. Los nombres de usuario deben ser idénticos. Para obtener información sobre estos roles y cómo asignarlos, consulte Asignación de los roles de clúster líder y seguidor en la documentación de OpenSearch.

Confirmación de replicación

Para confirmar que se está produciendo la replicación, obtenga su estado:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "SYNCING",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01",
  "syncing_details" : {
    "leader_checkpoint" : -5,
    "follower_checkpoint" : -5,
    "seq_no" : 0
  }
}
```

Los valores de los puntos de control líder y seguidor comienzan como enteros negativos y reflejan el número de particiones que se tienen (-1 para una partición, -5 para cinco particiones, etc.). Los valores se incrementan en enteros positivos con cada cambio que se realiza. Si los valores son los mismos, eso significa que los índices están totalmente sincronizados. Puede utilizar estos valores de punto de control para medir la latencia de replicación en todos los dominios.

Para validar aún más la replicación, agregue un documento al índice líder:

```
PUT leader-01/_doc/1
{
   "Doctor Sleep":"Stephen King"
}
```

Y confirme que aparece en el índice seguidor:

```
GET follower-01/_search

{
    ...
    "max_score" : 1.0,
    "hits" : [
      {
```

```
        "_index" : "follower-01",
        "_type" : "_doc",
        "_id" : "1",
        "_score" : 1.0,
        "_source" : {
          "Doctor Sleep" : "Stephen King"
        }
      }
    ]
  }
}
```

Pausa y reanudación de la replicación

Puede pausar temporalmente la replicación si necesita corregir problemas o reducir la carga en el dominio líder. Envíe esta solicitud al dominio seguidor. Asegúrese de incluir un cuerpo de la solicitud vacío:

```
POST _plugins/_replication/follower-01/_pause
{}
```

Después, obtenga el estado para asegurarse de que la replicación esté en pausa:

```
GET _plugins/_replication/follower-01/_status

{
  "status" : "PAUSED",
  "reason" : "User initiated",
  "leader_alias" : "connection-alias",
  "leader_index" : "leader-01",
  "follower_index" : "follower-01"
}
```

Cuando termine de realizar los cambios, reanude la replicación. Envíe esta solicitud al dominio seguidor. Asegúrese de incluir un cuerpo de la solicitud vacío:

```
POST _plugins/_replication/follower-01/_resume
{}
```

No puede reanudar la replicación después de haber estado en pausa durante más de 12 horas. Debe detener la replicación, eliminar el índice de seguidores y reiniciar la replicación del líder.

Detención de la replicación

Cuando se detiene la replicación por completo, el índice seguidor deja de seguir al líder y se convierte en un índice estándar. No se puede reiniciar la replicación después de detenerla.

Detenga la replicación desde el dominio seguidor. Asegúrese de incluir un cuerpo de la solicitud vacío:

```
POST _plugins/_replication/follower-01/_stop
{}
```

Seguimiento automático

Puede definir un conjunto de reglas de replicación en un único dominio líder que replique automáticamente los índices que coincidan con un patrón especificado. Cuando un índice del dominio líder coincide con uno de los patrones (por ejemplo, `books*`), se crea un índice seguidor coincidente en el dominio seguidor. OpenSearch Service replica todos los índices existentes que coincidan con el patrón, así como los nuevos índices que se creen. No replica los índices que ya existan en el dominio seguidor.

Para replicar todos los índices (a excepción de los índices creados por el sistema y los que ya existan en el dominio seguidor), utilice un patrón comodín (`*`).

Creación de una regla de replicación

Cree una regla de replicación en el dominio seguidor y especifique el nombre de la conexión entre clústeres:

```
POST _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name",
   "pattern": "books*",
   "use_roles":{
      "leader_cluster_role": "all_access",
      "follower_cluster_role": "all_access"
   }
}
```

Puede encontrar el alias de conexión en la pestaña Conexiones del panel de control del dominio.

Para simplificar, en este ejemplo se supone que un administrador emite la solicitud, que utiliza `all_access` como reglas de los dominios líder y seguidor. No obstante, en entornos de producción se recomienda crear usuarios de replicación en los índices líder y seguidor, y asignarlos como corresponda. Los nombres de usuario deben ser idénticos. Para obtener información sobre estos roles y cómo asignarlos, consulte Asignación de los roles de clúster líder y seguidor en la documentación de OpenSearch.

Para recuperar una lista de reglas de replicación existentes en un dominio, utilice la operación de la API de estadísticas de seguimiento automático.

Para probar la regla, cree un índice que coincida con el patrón del dominio líder:

```
PUT books-are-fun
```

Y verifique que su réplica aparece en el dominio seguidor:

```
GET _cat/indices

health status index          uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   books-are-fun  ldfHO78xYYdxRMULuiTvSQ     1   1          0            0
     208b           208b
```

Eliminación de una regla de replicación

Cuando se elimina una regla de replicación, OpenSearch Service deja de replicar nuevos índices que coincidan con el patrón, pero prosigue con la actividad de replicación existente hasta que se detenga la replicación de esos índices.

Detenga las reglas de replicación desde el dominio seguidor.

```
DELETE _plugins/_replication/_autofollow
{
   "leader_alias" : "connection-alias",
   "name": "rule-name"
}
```

Actualización de los dominios conectados

Para actualizar la versión del motor de dos dominios que tienen una conexión entre clústeres, actualice primero el dominio seguidor y, después, el dominio principal. No elimine la conexión entre ellos; de lo contrario, la replicación se detendrá y no podrá reanudarla.

Migración de índices de Amazon OpenSearch Service mediante la reindexación remota

La reindexación remota te permite copiar índices de un dominio de Amazon OpenSearch Service a otro. Puede migrar índices desde cualquier dominio de OpenSearch servicio o desde clústeres autogestionados OpenSearch y de Elasticsearch.

Un dominio y un índice remotos hacen referencia al origen de los datos o al dominio y el índice desde los que desea copiar los datos. Un dominio y un índice locales hacen referencia al destino de los datos o al dominio y el índice en donde desea copiar los datos.

La reindexación remota requiere la OpenSearch versión 1.0 o una versión posterior, o Elasticsearch 6.7 o una versión posterior, en el dominio local. El dominio remoto debe ser inferior o la misma versión principal que el dominio local. Las versiones de Elasticsearch se consideran inferiores a las versiones, lo que significa que OpenSearch puedes reindexar datos de dominios de Elasticsearch a dominios. OpenSearch Dentro de la misma versión principal, el dominio remoto puede ser cualquier versión secundaria. Por ejemplo, se admite la reindexación remota de Elasticsearch 7.10.x a 7.9, pero no se admite la versión 1.0 a Elasticsearch 7.10.x. OpenSearch

La documentación completa de la `reindex` operación, incluidos los pasos detallados y las opciones compatibles, está disponible en la documentación. OpenSearch

Temas

Requisitos previos

La reindexación remota requiere lo siguiente:

- El dominio remoto debe ser accesible desde el dominio local. Para un dominio remoto que reside en una VPC, el dominio local debe tener acceso a la VPC. Este proceso depende de la configuración de la red, pero probablemente implica conectarse a una VPN o a una red administrada, o utilizar la conexión de punto de conexión de VPC nativa. Para obtener más información, consulte the section called “Compatibilidad con VPC”.
- La solicitud debe autorizarse por el dominio remoto como cualquier otra solicitud REST. Si el dominio remoto tiene habilitado el control de acceso detallado, debe tener permiso para realizar la reindexación en el dominio remoto y leer el índice en el dominio local. Para obtener más consideraciones de seguridad, consulte the section called “Control de acceso detallado”.
- Recomendamos que cree un índice con la configuración deseada en el dominio local antes de comenzar con el proceso de reindexación.
- Si un dominio utiliza un tipo de instancia T2 o T3 para los nodos de datos, no se puede utilizar la reindexación en remoto.

Reindexe los datos entre los dominios OpenSearch de Internet del Servicio

El escenario más básico es que el índice remoto esté en el mismo Región de AWS lugar que su dominio local con un punto final de acceso público y que tenga las credenciales de IAM firmadas.

Desde el dominio remoto, especifique el índice remoto desde el que se va a reindexar y el índice local para reindexar:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

Debe agregar 443 al final del punto de conexión del dominio remoto para una comprobación de validación.

Para comprobar que el índice se ha copiado en el dominio local, envíe esta solicitud al dominio local:

```
GET local_index/_search
```

Si el índice remoto se encuentra en una región diferente del dominio local, pase su nombre de región, como en esta solicitud de ejemplo:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "region": "eu-west-1"
    },
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

En el caso de regiones aisladas, como las regiones de China AWS GovCloud (US) o China, es posible que no se pueda acceder al punto final porque su usuario de IAM no está reconocido en esas regiones.

Si el dominio remoto está protegido con una autenticación básica, especifique el nombre de usuario y la contraseña:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password"
    },
    "index": "remote_index"
  },
```

```
  "dest": {
    "index": "local_index"
  }
}
```

Vuelva a indexar los datos entre los dominios de OpenSearch servicio cuando el control remoto esté en una VPC

Cada dominio de OpenSearch servicio está compuesto por su propia infraestructura interna de nube privada virtual (VPC). Al crear un dominio nuevo en una VPC de OpenSearch servicio existente, se crea una interface de red elástica para cada nodo de datos de la VPC.

Como la operación de reindexación remota se realiza desde el dominio de OpenSearch servicio remoto y, por lo tanto, dentro de su propia VPC privada, necesita una forma de acceder a la VPC del dominio local. Puede hacerlo mediante la función de conexión de punto final de la VPC integrada para establecer una conexión a través AWS PrivateLinkde ella o configurando un proxy.

Si tu dominio local usa la OpenSearch versión 1.0 o posterior, puedes usar la consola o la AWS CLI para crear una AWS PrivateLink conexión. Una AWS PrivateLink conexión permite que los recursos de la VPC local se conecten de forma privada a los recursos de la VPC remota dentro de la misma. Región de AWS

Vuelva a indexar los datos con la AWS Management Console

Puede usar la reindexación remota con la consola para copiar índices entre dos dominios que comparten una conexión de punto de conexión de VPC.

1. Dirígete a la consola OpenSearch de Amazon Service enhttps://console.aws.amazon.com/aos/.
2. En el panel de navegación izquierdo, seleccione Dominios.
3. Seleccione el dominio local, que es el dominio en el que desea copiar los datos. Se abrirá la página de detalles del dominio. Seleccione la pestaña Conexiones situada debajo de la información general, y luego Solicitar.
4. En la página Solicitar conexión, seleccione Conexión de punto de conexión de VPC como modo de conexión e ingrese otros detalles relevantes. Estos detalles incluyen el dominio remoto, que es el dominio desde el que desea copiar los datos. A continuación, seleccione Solicitar.
5. Vaya a la página de detalles del dominio remoto, seleccione la pestaña Conexiones y busque la tabla Conexiones entrantes. Seleccione la casilla de verificación situada junto al nombre del dominio desde el que acaba de crear la conexión (el dominio local). Seleccione Aprobar.

6. Vuelva al dominio local, seleccione la pestaña Conexiones y busque la tabla Conexiones salientes. Una vez que la conexión entre los dos dominios esté activa, aparecerá un punto de conexión disponible en la columna Punto de conexión de la tabla. Copie el punto de conexión.
7. Abra el panel de control del dominio local y seleccione Herramientas de desarrollo en el panel de navegación de la izquierda. Para confirmar que el índice del dominio remoto aún no existe en el dominio local, ejecute la siguiente solicitud GET. *remote-domain-index-name*Sustitúyalo por tu propio nombre de índice.

```
GET remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

   En el resultado, debería aparecer un error que indica que no se ha encontrado el índice.
8. Debajo de la solicitud GET, cree una solicitud POST y utilice el punto de conexión como host remoto, tal y como sigue.

```
POST _reindex
{
   "source":{
      "remote":{
         "host":"endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
}
```

   Ejecute esta solicitud.
9. Vuelva a ejecutar la solicitud GET. Ahora el resultado debería indicar que el índice local existe. Puede consultar este índice para comprobar que OpenSearch copió todos los datos del índice remoto.

Vuelva a indexar los datos con las operaciones OpenSearch de la API de servicio

Puede usar la reindexación remota con la API para copiar índices entre dos dominios que comparten una conexión de punto de conexión de VPC.

1. Usa la operación de la CreateOutboundConnectionAPI para solicitar una nueva conexión desde tu dominio local a tu dominio remoto.

```
POST https://es.region.amazonaws.com/2021-01-01/opensearch/cc/outboundConnection

{
   "ConnectionAlias": "remote-reindex-example",
   "ConnectionMode": "VPC_ENDPOINT",
   "LocalDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "local-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   },
   "RemoteDomainInfo": {
      "AWSDomainInformation": {
         "DomainName": "remote-domain-name",
         "OwnerId": "aws-account-id",
         "Region": "region"
      }
   }
}
```

   Recibirá un `ConnectionId` en la respuesta. Guarde este ID para utilizarlo en el siguiente paso.

2. Usa la operación de AcceptInboundConnectionAPI con tu ID de conexión para aprobar la solicitud del dominio local.

```
PUT https://es.region.amazonaws.com/2021-01-01/opensearch/cc/
inboundConnection/ConnectionId/accept
```

3. Usa la operación de DescribeOutboundConnectionsAPI para recuperar el punto final de tu dominio remoto.

```
{
    "Connections": [
```

```
        {
            "ConnectionAlias": "remote-reindex-example",
            "ConnectionId": "connection-id",
            "ConnectionMode": "VPC_ENDPOINT",
            "ConnectionProperties": {
                "Endpoint": "connection-endpoint"
            },
            ...
        }
    ]
}
```

Guarde el *connection-endpoint* para usarlo en el paso 5.

4. Para confirmar que el índice del dominio remoto aún no existe en el dominio local, ejecute la siguiente solicitud GET. *remote-domain-index-name*Sustitúyalo por tu propio nombre de índice.

```
GET local-domain-endpoint/remote-domain-index-name/_search
{
   "query":{
      "match_all":{}
   }
}
```

En el resultado, debería aparecer un error que indica que no se ha encontrado el índice.

5. Cree una solicitud POST y utilice el punto de conexión como host remoto, tal y como se muestra a continuación.

```
POST local-domain-endpoint/_reindex
{
   "source":{
      "remote":{
         "host":"connection-endpoint",
         "username":"username",
         "password":"password"
      },
      "index":"remote-domain-index-name"
   },
   "dest":{
      "index":"local-domain-index-name"
   }
```

```
}
```

Ejecute esta solicitud.

6. Vuelva a ejecutar la solicitud GET. Ahora el resultado debería indicar que el índice local existe. Puede consultar este índice para comprobar que OpenSearch copió todos los datos del índice remoto.

Si el dominio remoto está alojado dentro de una VPC y no desea utilizar la característica de conexión de punto de conexión de VPC, debe configurar un proxy con un punto de conexión accesible públicamente. En este caso, el OpenSearch servicio requiere un punto final público porque no tiene la capacidad de enviar tráfico a su VPC.

Cuando ejecuta un dominio en modo VPC, se colocan uno o más puntos de conexión en su VPC. Sin embargo, estos puntos de conexión son únicamente para el tráfico que entra en el dominio de la VPC y no permiten que el tráfico entre en la VPC misma.

El comando reindexación remota se ejecuta desde el dominio local, por lo que el tráfico de origen no puede usar esos puntos de conexión para acceder al dominio remoto. Por eso se requiere un proxy en este caso de uso. El dominio proxy debe tener un certificado firmado por una entidad de certificación (CA) pública. No se admiten los certificados autofirmados o firmados por una entidad de certificación privada.

Vuelva a indexar los datos entre dominios que no son de servicio OpenSearch

Si el índice remoto está alojado fuera del OpenSearch servicio, como en una instancia EC2 autogestionada, defina el `external` parámetro en: `true`

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "username": "username",
      "password": "password",
      "external": true
    },
    "index": "remote_index"
  },
```

```
  "dest": {
    "index": "local_index"
  }
}
```

En este caso, solo se admite la autenticación básica con un nombre de usuario y una contraseña. El dominio remoto debe tener un punto final de acceso público (incluso si está en la misma VPC que el dominio de OpenSearch servicio local) y un certificado firmado por una CA pública. No se admiten los certificados autofirmados o firmados por una CA privada.

Reindexar conjuntos de datos grandes

La reindexación remota envía una solicitud de desplazamiento al dominio remoto con los siguientes valores predeterminados:

- Contexto de búsqueda de 5 minutos
- Tiempo de espera del socket de 30 segundos
- Tamaño del lote de 1000

Recomendamos ajustar estos parámetros para adaptarlos a sus datos. Para documentos grandes, considere un tamaño de lote más pequeño o un tiempo de espera más largo. Para obtener más información, consulte Búsqueda por desplazamiento.

```
POST _reindex?pretty=true&scroll=10h&wait_for_completion=false
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443",
      "socket_timeout": "60m"
    },
    "size": 100,
    "index": "remote_index"
  },
  "dest": {
    "index": "local_index"
  }
}
```

También recomendamos agregar la siguiente configuración al índice local para un mejor rendimiento:

```
PUT local_index
{
  "settings": {
    "refresh_interval": -1,
    "number_of_replicas": 0
  }
}
```

Una vez finalizado el proceso de reindexación, puede establecer el recuento de réplicas deseado y eliminar la configuración del intervalo de actualización.

Para reindexar únicamente un subconjunto de documentos que seleccione a través de una consulta, envíe esta solicitud al dominio local:

```
POST _reindex
{
  "source": {
    "remote": {
      "host": "https://remote-domain-endpoint:443"
    },
    "index": "remote_index",
    "query": {
      "match": {
        "field_name": "text"
      }
    }
  },
  "dest": {
    "index": "local_index"
  }
}
```

La reindexación remota no admite la división, por lo que no puede realizar varias operaciones de desplazamiento para la misma solicitud en paralelo.

Configuración remota de reindexación

Además de las opciones de reindexación estándar, OpenSearch Service admite las siguientes opciones:

Opciones	Valores válidos	Descripción	Obligatorio
externo	Booleano	Si el dominio remoto no es un dominio de OpenSearch servicio o si vas a volver a indexar entre dos dominios de VPC, especifica como. `true`	No
región	Cadena	Si el dominio remoto se encuentra en otra región, especifique el nombre de la región.	No

Administración de datos de series temporales en Amazon OpenSearch Service con Data Streams

Un flujo de trabajo típico para administrar datos de serie temporal consta de varios pasos, como la creación de un alias de índice de reversión, la definición de un índice de escritura y la definición de mapeos y configuraciones comunes para los índices de respaldo.

Data Streams de Amazon OpenSearch Service ayuda a simplificar este proceso de configuración inicial. Data Streams funciona de inmediato para los datos basados en el tiempo, como los registros de aplicaciones, que normalmente son anexos.

Data Streams requiere OpenSearch 1.0 o posterior. Encontrará la documentación completa sobre esta característica en la documentación de OpenSearch.

Introducción a Data Streams

Un flujo de datos se compone internamente de múltiples índices de respaldo. Las peticiones de búsqueda se dirigen a todos los índices de respaldo, mientras que las solicitudes de indexación se dirigen al índice de escritura más reciente.

Paso 1: crear una plantilla de índices

Para crear un flujo de datos, primero debe crear una plantilla de índice que configure un conjunto de índices como un flujo de datos. El objeto `data_stream` indica que se trata de un flujo de datos y no de una plantilla de índice normal. El patrón de índice coincide con el nombre del flujo de datos:

```
PUT _index_template/logs-template
{
  "index_patterns": [
    "my-data-stream",
    "logs-*"
  ],
  "data_stream": {},
  "priority": 100
}
```

En este caso, cada documento capturado debe tener un campo `@timestamp`. También puede definir su propio campo de marca temporal personalizado como una propiedad en el objeto `data_stream`.

```
PUT _index_template/logs-template
{
  "index_patterns": "my-data-stream",
  "data_stream": {
    "timestamp_field": {
      "name": "request_time"
    }
  }
}
```

Paso 2: crear un flujo de datos

Después de crear una plantilla de índice, puede comenzar directamente a incorporar datos sin crear un flujo de datos.

Debido a que tenemos una plantilla de índice coincidente con un objeto `data_stream`, OpenSearch crea automáticamente el flujo de datos:

```
POST logs-staging/_doc
{
  "message": "login attempt failed",
```

```
  "@timestamp": "2013-03-01T00:00:00"
}
```

Paso 3: incorporar datos en el flujo de datos

Para incorporar datos en un flujo de datos, puede utilizar las API de indexación regulares. Asegúrese de que cada documento que indexe tenga un campo temporal. Si intenta incorporar un documento que no tiene un campo temporal, aparecerá un error.

```
POST logs-redis/_doc
{
  "message": "login attempt",
  "@timestamp": "2013-03-01T00:00:00"
}
```

Paso 4: búsqueda de un flujo de datos

Puede buscar en un flujo de datos igual que en un índice normal o en un alias de índice. La operación de búsqueda se aplica a todos los índices de respaldo (todos los datos presentes en el flujo).

```
GET logs-redis/_search
{
  "query": {
    "match": {
      "message": "login"
    }
  }
}
```

Paso 5: revertir un flujo de datos

Puede configurar una política de Administración de estados de índice (ISM) para automatizar el proceso de reversión del flujo de datos. La política de ISM se aplica a los índices de respaldo en el momento de su creación. Cuando se asocia una política a un flujo de datos, solo afecta a los índices de respaldo futuros de ese flujo de datos. Tampoco es necesario proporcionar la configuración `rollover_alias`, ya que la política de ISM deduce esta información del índice de respaldo.

> **Note**
>
> Si migra un índice de respaldo al almacenamiento en frío, OpenSearch elimina este índice del flujo de datos. Incluso si vuelve a mover el índice a UltraWarm, el índice sigue siendo independiente y no parte del flujo de datos. Una vez que se haya eliminado un índice del flujo de datos, al buscar en el flujo no se devolverá ningún dato del índice.

> **Warning**
>
> El índice de escritura de un flujo de datos no se puede migrar a un almacenamiento en frío. Si desea migrar los datos de su flujo de datos a un almacenamiento en frío, debe transferir el flujo de datos antes de la migración.

Paso 6: administrar Data Streams en OpenSearch Dashboards

Para administrar Data Streams desde OpenSearch Dashboards, abra OpenSearch Dashboards, elija Gestión de índices y, a continuación, seleccione Índices o Índices administrados por políticas.

Paso 7: eliminar un flujo de datos

La operación de eliminación elimina primero los índices de respaldo de un flujo de datos y, a continuación, elimina el propio flujo de datos.

Para eliminar un flujo de datos y todos sus índices de respaldo ocultos:

```
DELETE _data_stream/name_of_data_stream
```

Monitoreo de datos en Amazon OpenSearch Service

Monitoree de forma proactiva sus datos en Amazon OpenSearch Service con alertas y detección de anomalías. Configure alertas para recibir notificaciones cuando los datos superan umbrales determinados. La detección de anomalías utiliza el aprendizaje automático para detectar automáticamente cualquier valor atípico en los datos de streaming. Puede emparejar la detección de anomalías con las alertas para asegurarse de que se le notifique tan pronto como se detecte una anomalía.

Temas

Configuración de alertas en Amazon OpenSearch Service

Configura alertas en Amazon OpenSearch Service para recibir notificaciones cuando los datos de uno o más índices cumplan determinadas condiciones. Por ejemplo, es posible que desee recibir un email si la aplicación registra más de cinco errores HTTP 503 en una hora o tal vez desee avisar a un desarrollador si no se indexaron nuevos documentos en los últimos 20 minutos.

Las alertas requieren Elasticsearch 6.2 OpenSearch o una versión posterior. Para obtener la documentación completa, incluidas las descripciones de las API, consulte Alertas en la documentación. OpenSearch En este tema se destacan las diferencias entre las alertas de OpenSearch Service y las de la versión de código abierto.

Temas

Permisos de alertas

Las alertas admiten el control de acceso detallado. Para obtener más información sobre cómo combinar y combinar permisos para adaptarlos a su caso de uso, consulte la sección Seguridad de las alertas en la OpenSearch documentación.

Para acceder a la página de alertas en los OpenSearch paneles de control, debe estar asignado como mínimo a la función `alerting_read_access` predefinida o tener permisos equivalentes. Esta función otorga permisos para ver las alertas, los destinos y los monitores, pero no para reconocer las alertas ni modificar los destinos o los monitores.

Introducción a las alertas

Para crear una alerta, debe configurar un monitor, que es un trabajo que se ejecuta según un cronograma definido y consulta OpenSearch los índices. También puede configurar disparadores, que definen las condiciones que generan los eventos. Por último, se configuran las acciones, lo que ocurre después de que se activa una alerta.

Para comenzar a trabajar con alertas

1. Elija Alertas en el menú principal del OpenSearch panel de mandos y elija Crear monitor.
2. Cree un monitor por consulta, por bucket, por métricas de clúster o por documento. Para obtener instrucciones, consulte Create a monitor (Crear un monitor).
3. En Triggers (Disparadores), cree uno o más disparadores. Para obtener instrucciones, consulte Create triggers (Creación de disparadores).
4. En Actions (Acciones), configure un notification channel (canal de notificación) para la alerta. Seleccione entre Slack, Amazon Chime, un webhook personalizado o Amazon SNS. Como puede imaginar, las notificaciones requieren conectividad con el canal. Por ejemplo, tu dominio de OpenSearch servicio debe poder conectarse a Internet para notificar a un canal de Slack o enviar un webhook personalizado a un servidor de terceros. El webhook personalizado debe tener una dirección IP pública para que un dominio de OpenSearch servicio pueda enviarle alertas.

> **Tip**
>
> Después de que una acción envíe correctamente un mensaje, tiene la responsabilidad de asegurar el acceso a ese mensaje (por ejemplo, el acceso a un canal de Slack). Si

el dominio contiene información confidencial, considere utilizar desencadenadores sin acciones y verificar periódicamente si hay alertas en Dashboards.

Notificaciones

Las alertas se integran con las notificaciones, que es un sistema unificado de OpenSearch notificaciones. Las notificaciones le permiten configurar el servicio de comunicación que desea utilizar y ver las estadísticas pertinentes y la información para la solución de problemas. Para obtener una documentación completa, consulte Notificaciones en la OpenSearch documentación.

Tu dominio debe tener la OpenSearch versión 2.3 o posterior para poder usar las notificaciones.

> **Note**
>
> OpenSearch las notificaciones son independientes de las notificaciones de OpenSearch servicio, que proporcionan detalles sobre las actualizaciones del software del servicio, las mejoras de Auto-Tune y otra información importante a nivel de dominio. OpenSearch las notificaciones son específicas del complemento.

Los canales de notificación sustituyeron a los destinos de alerta a partir de la versión 2.0. OpenSearch Los destinos quedaron obsoletos de forma definitiva y, a partir de ahora, todas las notificaciones de alertas se gestionarán a través de los canales.

Cuando actualizas tus dominios a la versión 2.3 o posterior (dado que el soporte de OpenSearch servicio para la versión 2.x comienza con la 2.3), tus destinos actuales se migran automáticamente a los canales de notificación. Si un destino no se migra, el monitor seguirá usándolo hasta que el monitor se migre a un canal de notificación. Para obtener más información, consulta la sección Preguntas sobre los destinos en la OpenSearch documentación.

Para empezar con las notificaciones, inicia sesión en los OpenSearch paneles de control y selecciona Notificaciones, Canales y Crear canal.

Amazon Simple Notification Service (Amazon SNS) es un tipo de canal compatible para las notificaciones. Para autenticar a los usuarios, debe proporcionar al usuario acceso completo a Amazon SNS o dejar que asuma un rol de IAM con permisos para acceder a Amazon SNS. Para obtener instrucciones, consulte Amazon SNS as a channel type (Amazon SNS como un tipo de canal).

Diferencias

En comparación con la versión de código abierto de OpenSearch, las alertas en Amazon OpenSearch Service presentan algunas diferencias notables.

Configuración de alertas

OpenSearch El servicio te permite modificar la siguiente configuración de alertas:

- `plugins.scheduled_jobs.enabled`
- `plugins.alerting.alert_history_enabled`
- `plugins.alerting.alert_history_max_age`
- `plugins.alerting.alert_history_max_docs`
- `plugins.alerting.alert_history_retention_period`
- `plugins.alerting.alert_history_rollover_period`
- `plugins.alerting.filter_by_backend_roles`

Todas las demás configuraciones utilizan los valores predeterminados que no se pueden cambiar.

Para deshabilitar las alertas, envíe la siguiente solicitud:

```
PUT _cluster/settings
{
  "persistent" : {
    "plugins.scheduled_jobs.enabled" : false
  }
}
```

La siguiente solicitud configura las alertas para eliminar automáticamente los índices del historial después de siete días, en lugar de los 30 días predeterminados:

```
PUT _cluster/settings
{
  "persistent": {
    "plugins.alerting.alert_history_retention_period": "7d"
  }
}
```

Si previamente creó monitores y desea detener la creación de índices de alerta diaria, elimine todos los índices del historial de alertas:

```
DELETE .plugins-alerting-alert-history-*
```

Para reducir el recuento de particiones de los índices del historial, cree una plantilla de índice. La siguiente solicitud establece índices de historial para las alertas y administración de estados de índice para una partición y una réplica:

```
PUT _index_template/template-name
{
  "index_patterns": [".opendistro-alerting-alert-history-*"],
  "template": {
    "settings": {
      "number_of_shards": 1,
      "number_of_replicas": 1
    }
  }
}
```

En función de la tolerancia a la pérdida de datos, incluso podría considerar no utilizar ninguna réplica. Para obtener más información sobre la creación y administración de plantillas de índice, consulte las plantillas de índice en la OpenSearch documentación.

Detección de anomalías en Amazon OpenSearch Service

La detección de anomalías de Amazon OpenSearch Service detecta automáticamente anomalías en los datos de OpenSearch casi en tiempo real mediante el algoritmo de bosque de corte aleatorio (Random Cut Forest, RCF). RCF es un algoritmo de machine learning no supervisado que modela un esquema del flujo de datos entrante. El algoritmo calcula un `anomaly grade` y valor `confidence score` para cada punto de datos entrante. La detección de anomalías utiliza estos valores para diferenciar una anomalía de las variaciones habituales de los datos.

Puede emparejar el complemento de detección de anomalías con el complemento the section called “Alertas” para recibir una notificación en cuanto se detecte una anomalía.

La detección de anomalías está disponible en dominios que ejecutan cualquier versión de OpenSearch o Elasticsearch 7.4 o posterior. Todos los tipos de instancias admiten la detección

de anomalías, excepto `t2.micro` y `t2.small`. La documentación completa sobre la detección de anomalías, incluidos los pasos detallados y las descripciones de la API, está disponible en la documentación de OpenSearch.

Requisitos previos

La detección de anomalías posee los siguientes requisitos previos:

- La detección de anomalías requiere OpenSearch o Elasticsearch 7.4 o posterior.
- La detección de anomalías solo admite el control de acceso detallado en las versiones 7.9 y posteriores de Elasticsearch y en todas las versiones de OpenSearch. En las versiones anteriores a Elasticsearch 7.9, solo los usuarios administradores pueden crear, ver y administrar detectores.
- Si el dominio utiliza un control de acceso detallado, los usuarios que no son administradores deben estar mapeados al rol `anomaly_read_access` en OpenSearch Dashboards para ver detectores o al rol `anomaly_full_access` para crear y administrar detectores.

Introducción a la detección de anomalías

Para empezar, elija Anomaly Detection (Detección de anomalías) en OpenSearch Dashboards.

Paso 1: crear un detector

Un detector es una tarea individual de detección de anomalías. Puede crear varios detectores y todos los detectores se pueden ejecutar simultáneamente; cada uno podrá analizar datos de distintos orígenes.

Paso 2: agregar características a su detector

Una característica es el campo del índice que se verifica para ver si hay anomalías. Un detector puede detectar anomalías en una o varias características. Debe elegir una de las siguientes agrupaciones para cada característica: `average()`, `sum()`, `count()`, `min()` o `max()`.

> **Note**
>
> El método de suma `count()` solo está disponible en OpenSearch y Elasticsearch 7.7 o posterior. Para Elasticsearch 7.4, utilice una expresión personalizada como la siguiente:
>
> ```
> {
> ```

```
  "aggregation_name": {
     "value_count": {
        "field": "field_name"
     }
  }
}
```

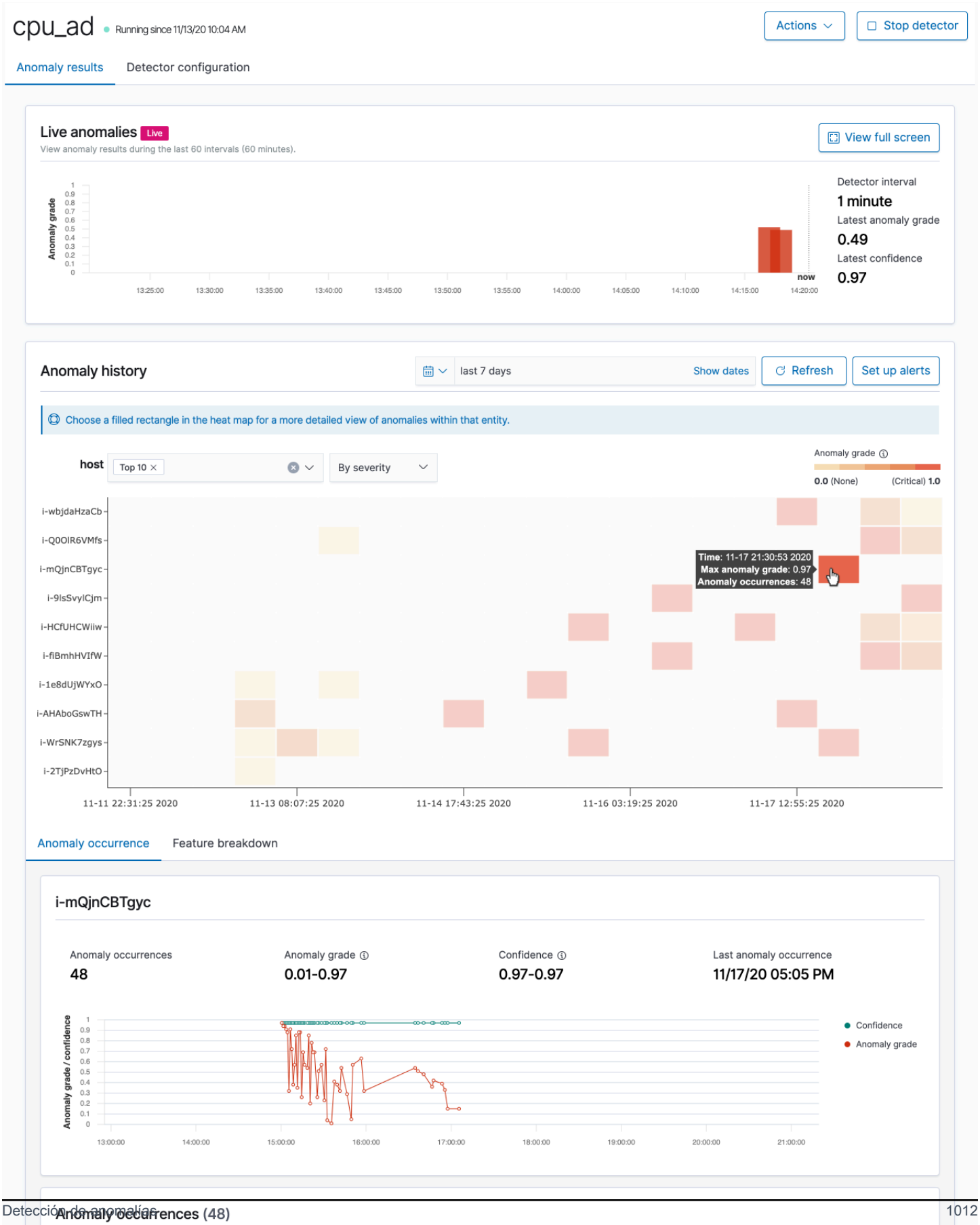
El método de agrupación determina qué constituye una anomalía. Por ejemplo, si elige `min()`, el detector se centra en buscar anomalías basadas en los valores mínimos de la característica. Si elige `average()`, el detector busca anomalías basadas en los valores medios de la característica. Puede agregar un máximo de cinco características por detector.

Puede configurar los siguientes parámetros opcionales (disponibles en Elasticsearch 7.7 y posterior):

- Category field (Categoría): clasifique o corte los datos con una dimensión como dirección IP, ID del producto, código de país, etc.
- Window size (Tamaño de ventana): establezca el número de intervalos de suma del flujo de datos que se tendrán en cuenta en una ventana de detección.

Después de configurar las características, obtenga una previsualización de las muestras de anomalías y ajuste la configuración de las características, si es necesario.

Paso 3: observar los resultados



- Live anomalies (Anomalías activas): muestra los resultados de anomalías activas de los últimos 60 intervalos. Por ejemplo, si el intervalo se establece en 10, muestra los resultados de los últimos 600 minutos. Este gráfico se actualiza cada 30 segundos.
- Anomaly history (Historial de anomalías): traza el grado de anomalía con la medida de confianza correspondiente.
- Feature breakdown (Desglose de características): traza las características según el método de agrupación. Puede variar el rango de fecha y hora del detector.
- Anomaly occurrence (Ocurrencia de anomalías): muestra los valores `Start time`, `End time`, `Data confidence` y `Anomaly grade` de cada anomalía detectada.

  Si establece el campo de categoría, verá un grafico Heat map (Mapa térmico) que correlaciona los resultados de entidades anómalas. Elija un rectángulo relleno para ver una vista más detallada de la anomalía.

Paso 4: configurar alertas

Para crear un monitor que envíe notificaciones cuando se detectan anomalías, elija Set up alerts (Configurar alertas). El complemento lo redirige a la página Add monitor (Agregar monitor) donde puede configurar una alerta.

Tutorial: Detectar un uso elevado de la CPU con la detección de anomalías

Este tutorial muestra cómo crear un detector de anomalías en Amazon OpenSearch Service para detectar un uso elevado de la CPU. Utilizará los paneles de OpenSearch para configurar un detector que supervise el uso de la CPU y genere una alerta cuando su uso supere un umbral especificado.

> **Note**
>
> Estos pasos se aplican a la versión más reciente de OpenSearch y pueden diferir ligeramente para las versiones anteriores.

Requisitos previos

- Debe tener un dominio de OpenSearch Service que ejecute Elasticsearch 7.4 o versiones posteriores, o cualquier versión de OpenSearch.

- Debe ingerir archivos de registro de aplicaciones en el clúster que contengan datos de uso de la CPU.

Paso 1: crear un detector

Primero, cree un detector que identifique las anomalías en los datos de uso de la CPU.

1. Abra el menú del panel izquierdo en los paneles de OpenSearch y elija Anomaly Detection (Detección de anomalías) y, después, elija Create detector (Crear detector).
2. Asigne el nombre **`high-cpu-usage`** al detector.
3. Para el origen de datos, elija el índice que contenga los archivos de registro de uso de la CPU en los que desee identificar anomalías.
4. Elija el icono Timestamp field (Campo de marca temporal) de los datos. Opcionalmente, puede agregar un filtro de datos. Este filtro de datos analiza únicamente un subconjunto del origen de datos y reduce el ruido de los datos que no son relevantes.
5. Establezca Detector interval (Intervalo de detector) en 2 minutos. Este intervalo define el tiempo (por intervalo de minutos) que tendrá el detector para recopilar los datos.
6. En Window delay (Demora del plazo), agregue una demora de 1 minute (1 minuto). Esta demora agrega tiempo de procesamiento adicional para garantizar que todos los datos dentro del plazo estén presentes.
7. Elija Next (Siguiente). En el panel de detección de anomalías, en el nombre del detector, seleccione Configure model (Configurar modelo).
8. En Feature name (Nombre de la característica), ingrese **`max_cpu_usage`**. En Feature state (Estado de la característica), seleccione Enable feature (Habilitar característica).
9. En Find anomalies based on (Encontrar anomalías en función de), elija Field value (Valor de campo).
10. En Aggregation method (Método de agregación), elija **`max()`**.
11. En Field (Campo), seleccione el campo de los datos para ver si hay anomalías. Por ejemplo, podría llamarse `cpu_usage_percentage`.
12. Mantenga todas las demás configuraciones en sus valores predeterminados y elija Next (Siguiente).
13. Ignore la configuración de trabajos del detector y elija Next (Siguiente).
14. En la ventana emergente, elija cuándo desea iniciar el detector (automática o manualmente) y, a continuación, elija Confirm (Confirmar).

Ya que se configuró el detector, después de inicializarse, podrá ver los resultados en tiempo real del uso de la CPU en la sección Real-time results (Resultados en tiempo real) del panel del detector. La sección Live anomalies (Anomalías en vivo) muestra cualquier anomalía que se produce cuando los datos se ingieren en tiempo real.

Paso 2: configurar una alerta

Ya que se creó un detector, cree un monitor que invoque una alerta para enviar un mensaje a Slack cuando se detecte un uso de la CPU que cumpla con las condiciones especificadas en la configuración del detector. Recibirá notificaciones de Slack cuando los datos de uno o más índices cumplan con las condiciones que invocan la alerta.

1. Abra el menú del panel izquierdo en los paneles de OpenSearch y elija Alerting (Alertas) y, a continuación, elija Create monitor (Crear monitor).
2. Proporcione un nombre para el monitor.
3. En Monitor type (Tipo de monitor), elija Per-query monitor (Monitor por consulta). Un monitor por consulta ejecuta una consulta específica y define los activadores.
4. En Monitor defining method (Método de definición de monitor), elija Anomaly detector (Detector de anomalías) y, a continuación, seleccione el detector que ha creado en la sección anterior en el menú desplegable Detector.
5. En Schedule (Programación), elija la frecuencia con la que el monitor recopilará datos y recibirá alertas. Para los fines de este tutorial, establezca la programación para que se ejecute cada 7 minutos.
6. En la sección Triggers (Desencadenadores), elija Add trigger (Agregar desencadenador). En Trigger name (Nombre del desencadenador), ingrese **`High CPU usage`**. En este tutorial, en Severity level (Nivel de gravedad), elija 1, que es el nivel de gravedad más alto.
7. En Anomaly grade threshold (Umbral de clasificación de anomalías), elija IS ABOVE (ES SUPERIOR). En el menú que hay debajo, elija el umbral de clasificación que desea aplicar. En este tutorial, establezca Clasificación de anomalías en 0,7.
8. En Anomaly confidence threshold (Umbral de confianza de anomalías), elija IS ABOVE (ES SUPERIOR). En el menú que hay debajo, ingrese el mismo número que su clasificación de anomalías. En este tutorial, establezca Anomaly confidence threshold (Umbral de confianza de anomalías) en 0,7.
9. En la sección Actions (Acciones), elija Destination (Destino). En el campo Name (Nombre), elija el nombre del destino. En el menú Type (Tipo), elija Slack. En el campo Webhook URL (URL del webhook), ingrese una URL de webhook donde quiera recibir alertas. Para obtener más

información, consulte Sending messages using incoming webhooks (Envío de mensajes mediante webhooks entrantes).

10. Seleccione Create (Crear).

Recursos relacionados

- the section called “Alertas”

- the section called “Detección de anomalías”
- API de detección de anomalías

Aprendizaje automático para Amazon OpenSearch Service

ML Commons es un OpenSearch complemento que proporciona un conjunto de algoritmos comunes de aprendizaje automático (ML) mediante llamadas a la API de transporte y REST. Esas llamadas eligen los nodos y los recursos correctos para cada solicitud de ML y supervisan las tareas de ML para garantizar el tiempo de actividad. Esto le permite aprovechar los algoritmos de ML de código abierto existentes y reducir el esfuerzo necesario para desarrollar nuevas características de ML. Para obtener más información sobre el complemento, consulte Aprendizaje automático en la OpenSearch documentación. En este capítulo se explica cómo utilizar el complemento con Amazon OpenSearch Service.

Temas

Conectores Amazon OpenSearch Service ML para Servicios de AWS

Cuando utilizas conectores de aprendizaje automático (ML) de Amazon OpenSearch Service con otro Servicio de AWS, debes configurar un rol de IAM para conectar el OpenSearch Servicio a ese servicio de forma segura. Servicios de AWS que puedes configurar un conector para incluir Amazon SageMaker y Amazon Bedrock. En este tutorial, explicamos cómo crear un conector desde OpenSearch Service hasta SageMaker Runtime. Para obtener más información sobre los conectores, consulte Conectores compatibles.

Temas

Requisitos previos

Para crear un conector, debe tener un punto de enlace de Amazon SageMaker Domain y un rol de IAM que otorgue acceso al OpenSearch servicio.

Configurar un SageMaker dominio de Amazon

Consulte Implementación de un modelo en Amazon SageMaker en la Guía para SageMaker desarrolladores de Amazon para implementar su modelo de aprendizaje automático. Anote la URL del punto de conexión de su modelo, que necesitará para crear un conector de IA.

Creación de un rol de IAM

Configure una función de IAM para delegar los permisos SageMaker de tiempo de ejecución al OpenSearch servicio. Para crear un rol nuevo, consulte Creación de roles de IAM (consola) en la Guía del usuario de IAM. Si lo desea, puede utilizar un rol existente siempre que tenga el mismo conjunto de privilegios. Si crea un rol nuevo en lugar de usar un rol AWS administrado, `opensearch-sagemaker-role` sustitúyalo en este tutorial por el nombre de su propio rol.

1. Adjunte la siguiente política de IAM gestionada a su nueva función para permitir que el OpenSearch Servicio acceda a su SageMaker punto final. Para asociar una política a un rol, consulte Añadir permisos de identidad de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:InvokeEndpointAsync",
                "sagemaker:InvokeEndpoint"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Siga las instrucciones de Modificación de una política de confianza de rol para editar la relación de confianza del rol. Debe especificar el OpenSearch servicio en la `Principal` declaración:

```
{
```

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

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para limitar el acceso a un dominio específico. `SourceAccount`Es el Cuenta de AWS ID que pertenece al propietario del dominio y `SourceArn` es el ARN del dominio. Por ejemplo, puede agregar el siguiente bloque de condición a la política de confianza:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configuración de permisos de

Para crear el conector, necesita permiso para transferir la función de IAM a OpenSearch Service. También necesita tener acceso a la acción `es:ESHttpPost`. Para conceder estos dos permisos, asocie la siguiente política al rol de IAM cuyas credenciales se utilicen para firmar la solicitud:

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

```
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Si su usuario o rol no tiene permisos de `iam:PassRole` para transferir su rol, puede que se produzca un error de autorización cuando intente registrar un repositorio en el siguiente paso.

Asigne la función de aprendizaje automático en los OpenSearch paneles de control (si utiliza un control de acceso detallado)

El control de acceso detallado presenta un paso adicional al configurar un conector. Incluso si utiliza autenticación HTTP básica para todos los demás fines, debe asignar el rol `ml_full_access` al rol de IAM que tenga permisos `iam:PassRole` para transferir `opensearch-sagemaker-role`.

1. Navegue hasta el complemento OpenSearch Dashboards de su dominio de servicio. OpenSearch Puedes encontrar el punto de conexión de Dashboards en el panel de control de tu dominio, en la consola de OpenSearch servicio.
2. En el menú principal, seleccione Seguridad, Roles y seleccione el rol ml_full_access.
3. Seleccione Usuarios asignados, Administrar mapeo.
4. En Roles de backend, agregue el ARN del rol que tenga permisos para transferir `opensearch-sagemaker-role`.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Seleccione Asignar y confirme que el usuario o el rol aparecen en Usuarios asignados.

Crea un conector de OpenSearch servicio

Para crear un conector, envíe una `POST` solicitud al punto final del dominio de OpenSearch servicio. Puede usar curl, el cliente Python de muestra, Postman u otro método para enviar una solicitud firmada. Tenga en cuenta que no puede usar una solicitud `POST` en la consola de Kibana. La solicitud tiene el siguiente formato:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
```

Si el dominio reside en una nube privada virtual (VPC), la computadora debe estar conectada a la VPC para que la solicitud cree correctamente el conector de IA. El acceso a una VPC depende de la configuración de red, pero generalmente implica conectarse a una VPN o una red corporativa. Para comprobar si puedes acceder a tu dominio de OpenSearch servicio, navega `https://your-vpc-domain.region.es.amazonaws.com` en un navegador web y comprueba que recibes la respuesta JSON predeterminada.

Cliente Python de muestra

El cliente de Python es más simple de automatizar que una solicitud HTTP y tiene una mejor reutilización. Para crear el conector de IA con el cliente Python, guarde el siguiente código de ejemplo en un archivo Python. El cliente necesita los paquetes AWS SDK for Python (Boto3), `requests` y `requests-aws4auth`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

# Register repository
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
   "name": "sagemaker: embedding",
   "description": "Test connector for Sagemaker embedding model",
   "version": 1,
   "protocol": "aws_sigv4",
   "credential": {
      "roleArn": "arn:aws:iam::account-id:role/opensearch-sagemaker-role"
   },
   "parameters": {
      "region": "region",
      "service_name": "sagemaker"
   },
   "actions": [
      {
         "action_type": "predict",
         "method": "POST",
         "headers": {
            "content-type": "application/json"
         },
         "url": "https://runtime.sagemaker.region.amazonaws.com/endpoints/endpoint-id/
invocations",
         "request_body": "{ \"inputs\": { \"question\": \"${parameters.question}\",
 \"context\": \"${parameters.context}\" } }"
      }
   ]
}
headers = {"Content-Type": "application/json"}
```

```
r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Conectores Amazon OpenSearch Service ML para plataformas de terceros

En este tutorial, explicamos cómo crear un conector de OpenSearch Service a Cohere. Para obtener más información sobre los conectores, consulte Conectores compatibles.

Cuando utilizas un conector de aprendizaje automático (ML) de Amazon OpenSearch Service con un modelo remoto externo, debes almacenar tus credenciales de autorización específicas en él AWS Secrets Manager. Puede ser una clave de API o una combinación de nombre de usuario y contraseña. Esto significa que también debe crear un rol de IAM que permita al OpenSearch Servicio acceder a Secrets Manager para leer.

Temas

- Requisitos previos
- Crea un conector de OpenSearch servicio

Requisitos previos

Para crear un conector para Cohere o cualquier proveedor externo con el OpenSearch Servicio, debe tener un rol de IAM que le dé acceso al OpenSearch Servicio AWS Secrets Manager, donde almacene sus credenciales. También debe almacenar sus credenciales en Secrets Manager.

Creación de un rol de IAM

Configure un rol de IAM para delegar los permisos de Secrets Manager a OpenSearch Service. También puede usar el rol de `SecretManagerReadWrite` existente. Para crear un rol nuevo, consulte Creación de roles de IAM (consola) en la Guía del usuario de IAM. Si crea un nuevo rol en lugar de usar un rol AWS administrado, `opensearch-secretmanager-role` sustitúyalo en este tutorial por el nombre de su propio rol.

1. Adjunta la siguiente política de IAM gestionada a tu nueva función para permitir que OpenSearch Service acceda a tus valores de Secrets Manager. Para adjuntar una política a un rol, consulte Adición de permisos de identidad de IAM.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

2. Siga las instrucciones de Modificación de una política de confianza de rol para editar la relación de confianza del rol. Debe especificar el OpenSearch servicio en la `Principal` declaración:

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

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para limitar el acceso a un dominio específico. `SourceAccount`Es el Cuenta de AWS ID que pertenece al propietario del dominio y `SourceArn` es el ARN del dominio. Por ejemplo, puede agregar el siguiente bloque de condición a la política de confianza:

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account-id"
```

```
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:es:region:account-id:domain/domain-name"
    }
}
```

Configuración de permisos de

Para crear el conector, necesita permiso para transferir la función de IAM a OpenSearch Service. También necesita tener acceso a la acción `es:ESHttpPost`. Para conceder estos dos permisos, asocie la siguiente política al rol de IAM cuyas credenciales se utilicen para firmar la solicitud:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    {
      "Effect": "Allow",
      "Action": "es:ESHttpPost",
      "Resource": "arn:aws:es:region:account-id:domain/domain-name/*"
    }
  ]
}
```

Si su usuario o rol no tiene permisos de `iam:PassRole` para transferir su rol, puede que se produzca un error de autorización cuando intente registrar un repositorio en el siguiente paso.

Configurar AWS Secrets Manager

Para almacenar sus credenciales de autorización en Secrets Manager, consulte Create an AWS Secrets Manager secret en la Guía del usuario de AWS Secrets Manager .

Después de que Secrets Manager acepta su par clave-valor como secreto, recibirá un ARN con el formato: `arn:aws:secretsmanager:us-west-2:123456789012:secret:MySecret-a1b2c3`. Mantenga un registro de este ARN, a medida que lo usa y su clave cuando cree un conector en el siguiente paso.

Asigne la función del aprendizaje automático en los OpenSearch paneles de control (si utiliza un control de acceso detallado)

El control de acceso detallado presenta un paso adicional al configurar un conector. Incluso si utiliza autenticación HTTP básica para todos los demás fines, debe asignar el rol `ml_full_access` al rol de IAM que tenga permisos `iam:PassRole` para transferir `opensearch-sagemaker-role`.

1. Navegue hasta el complemento OpenSearch Dashboards de su dominio de servicio. OpenSearch Puedes encontrar el punto de conexión de Dashboards en el panel de control de tu dominio, en la consola de OpenSearch servicio.
2. En el menú principal, seleccione Seguridad, Roles y seleccione el rol ml_full_access.
3. Seleccione Usuarios asignados, Administrar mapeo.
4. En Roles de backend, agregue el ARN del rol que tenga permisos para transferir `opensearch-sagemaker-role`.

   ```
   arn:aws:iam::account-id:role/role-name
   ```

5. Seleccione Asignar y confirme que el usuario o el rol aparecen en Usuarios asignados.

Crea un conector de OpenSearch servicio

Para crear un conector, envíe una `POST` solicitud al punto final del dominio de OpenSearch servicio. Puede usar curl, el cliente Python de muestra, Postman u otro método para enviar una solicitud firmada. Tenga en cuenta que no puede usar una solicitud `POST` en la consola de Kibana. La solicitud tiene el siguiente formato:

```
POST domain-endpoint/_plugins/_ml/connectors/_create
{
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
```

```
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}
```

El cuerpo de esta solicitud es diferente de una solicitud de conector de código abierto en dos aspectos. Dentro del `credential` campo, se pasa el ARN del rol de IAM que permite al OpenSearch Servicio leer Secrets Manager, junto con el ARN del secreto qué. En el campo `headers`, se hace referencia al secreto mediante la clave secreta y al hecho de que proviene de un ARN.

Si el dominio reside en una nube privada virtual (VPC), la computadora debe estar conectada a la VPC para que la solicitud cree correctamente el conector de IA. El acceso a una VPC depende de la configuración de red, pero generalmente implica conectarse a una VPN o una red corporativa. Para comprobar que puedes acceder a tu dominio de OpenSearch servicio, navega `https://your-vpc-domain.region.es.amazonaws.com` en un navegador web y comprueba que recibes la respuesta JSON predeterminada.

Cliente Python de muestra

El cliente de Python es más simple de automatizar que una solicitud HTTP y tiene una mejor reutilización. Para crear el conector de IA con el cliente Python, guarde el siguiente código de ejemplo en un archivo Python. El cliente necesita los paquetes AWS SDK for Python (Boto3), `requests` y `requests-aws4auth`.

```
import boto3
import requests
from requests_aws4auth import AWS4Auth

host = 'domain-endpoint/'
region = 'region'
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)
```

```
path = '_plugins/_ml/connectors/_create'
url = host + path

payload = {
    "name": "Cohere Connector: embedding",
    "description": "The connector to cohere embedding model",
    "version": 1,
    "protocol": "http",
    "credential": {
        "secretArn": "arn:aws:secretsmanager:region:account-id:secret:cohere-key-id",
        "roleArn": "arn:aws:iam::account-id:role/opensearch-secretmanager-role"
    },
    "actions": [
        {
            "action_type": "predict",
            "method": "POST",
            "url": "https://api.cohere.ai/v1/embed",
            "headers": {
                "Authorization": "Bearer ${credential.secretArn.cohere-key-used-in-
secrets-manager}"
            },
            "request_body": "{ \"texts\": ${parameters.texts}, \"truncate\": \"END\" }"
        }
    ]
}

headers = {"Content-Type": "application/json"}

r = requests.post(url, auth=awsauth, json=payload, headers=headers)
print(r.status_code)
print(r.text)
```

Se utiliza AWS CloudFormation para configurar la inferencia remota para la búsqueda semántica

A partir de OpenSearch la versión 2.9, puede utilizar la inferencia remota con la búsqueda semántica para alojar sus propios modelos de aprendizaje automático (ML). La inferencia remota utiliza el complemento ML Commons para permitirle alojar sus inferencias de modelos de forma remota en servicios de aprendizaje automático, como Amazon SageMaker Amazon BedRock, y conectarlas a Amazon OpenSearch Service con conectores de aprendizaje automático.

Para facilitar la configuración de la inferencia remota, Amazon OpenSearch Service proporciona una AWS CloudFormationplantilla en la consola. CloudFormation es una Servicio de AWS que permite modelar, aprovisionar AWS y gestionar recursos de terceros al tratar la infraestructura como código.

La OpenSearch CloudFormation plantilla automatiza el proceso de aprovisionamiento de modelos, de modo que puede crear fácilmente un modelo en su dominio de OpenSearch servicio y, a continuación, utilizar el ID del modelo para ingerir datos y ejecutar consultas de búsqueda neuronal.

Temas

- Requisitos previos
- Amazon SageMaker plantillas
- Plantillas Amazon Bedrock

Requisitos previos

Para usar una CloudFormation plantilla con OpenSearch Service, complete los siguientes requisitos previos.

Configure un dominio de OpenSearch servicio

Antes de poder usar una CloudFormation plantilla, debes configurar un dominio de Amazon OpenSearch Service con la versión 2.9 o posterior y un control de acceso detallado activado. Crea un rol OpenSearch de backend del servicio para dar permiso al plugin ML Commons para que cree tu conector por ti.

La CloudFormation plantilla crea una función de IAM de Lambda para usted con el nombre predeterminado`LambdaInvokeOpenSearchMLCommonsRole`, que puede anular si desea elegir un nombre diferente. Una vez que la plantilla cree este rol de IAM, debe conceder permiso a la función Lambda para llamar a OpenSearch su dominio de servicio. Para ello, asigne la función nombrada `ml_full_access` a su función de backend del OpenSearch servicio siguiendo los siguientes pasos:

1. Navega hasta el complemento OpenSearch Dashboards de tu dominio de OpenSearch servicio. Puedes encontrar el punto de conexión de Dashboards en el panel de control de tu dominio, en la consola de OpenSearch servicio.
2. En el menú principal, seleccione Seguridad, Roles y seleccione el rol ml_full_access.
3. Seleccione Usuarios asignados, Administrar mapeo.

4. En Roles de backend, agregue el ARN del rol de Lambda que necesita permiso para llamar a su dominio.

```
arn:aws:iam::account-id:role/role-name
```

5. Seleccione Asignar y confirme que el usuario o el rol aparecen en Usuarios asignados.

Una vez que haya asignado la función, vaya a la configuración de seguridad de su dominio y añada la función Lambda IAM a OpenSearch su política de acceso al servicio.

Habilite los permisos en su Cuenta de AWS

Cuenta de AWS Debe tener permiso para acceder CloudFormation a Lambda, junto con lo que Servicio de AWS elija para su plantilla, ya sea SageMaker Runtime o Amazon. BedRock

Si utiliza Amazon Bedrock, también debe registrar su modelo. Consulte Acceso al modelo en la Guía del usuario de Amazon Bedrock para registrar su modelo.

Si utiliza su propio bucket de Amazon S3 para proporcionar artefactos modelo, debe añadir la función de CloudFormation IAM a su política de acceso a S3. Para más información, consulte Adición y eliminación de permisos de identidad de IAM en la Guía del usuario de IAM de .

Amazon SageMaker plantillas

SageMaker CloudFormation Las plantillas de Amazon definen varios AWS recursos para configurar el complemento neuronal y la búsqueda semántica por usted.

En primer lugar, usa la SageMaker plantilla Integración con modelos de incrustación de texto a través de Amazon para implementar un modelo de incrustación de texto en SageMaker Runtime como servidor. Si no proporciona un punto de enlace de modelo, CloudFormation crea un rol de IAM que permite a SageMaker Runtime descargar artefactos de modelos de Amazon S3 e implementarlos en el servidor. Si proporciona un punto final, CloudFormation crea un rol de IAM que permite a la función Lambda acceder al dominio OpenSearch del servicio o, si el rol ya existe, actualiza y reutiliza el rol. El punto final sirve al modelo remoto que se utiliza para el conector ML con el complemento ML Commons.

A continuación, utilice la plantilla Integración con codificadores dispersos a través de Amazon Sagemaker para crear una función Lambda que haga que su dominio configure conectores de inferencia remota. Una vez creado el conector en OpenSearch Service, la inferencia remota puede

ejecutar una búsqueda semántica utilizando el modelo remoto en tiempo de ejecución. SageMaker La plantilla te devuelve el ID del modelo de tu dominio para que puedas empezar a buscar.

Para usar las SageMaker CloudFormation plantillas de Amazon

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación izquierdo, seleccione Integraciones.
3. En cada una de las SageMaker plantillas de Amazon, selecciona Configurar dominio y Configurar dominio público.
4. Siga las instrucciones de la CloudFormation consola para aprovisionar su pila y configurar un modelo.

> **Note**
>
> OpenSearch El servicio también proporciona una plantilla independiente para configurar el dominio de VPC. Si usa esta plantilla, debe proporcionar el ID de VPC para la función de Lambda.

Plantillas Amazon Bedrock

Al igual que las SageMaker CloudFormation plantillas de Amazon, la CloudFormation plantilla Amazon Bedrock proporciona los AWS recursos necesarios para crear conectores entre OpenSearch Service y Amazon Bedrock.

En primer lugar, la plantilla crea una función de IAM que permite a la futura función de Lambda acceder a OpenSearch su dominio de servicio. A continuación, la plantilla crea la función Lambda, que hace que el dominio cree un conector mediante el complemento ML Commons. Una vez que OpenSearch Service crea el conector, finaliza la configuración de la inferencia remota y puede ejecutar búsquedas semánticas mediante las operaciones de la API de Amazon Bedrock.

Tenga en cuenta que, dado que Amazon Bedrock aloja sus propios modelos de aprendizaje automático, no necesita implementar un modelo en SageMaker Runtime. En su lugar, la plantilla utiliza un punto de enlace predeterminado para Amazon Bedrock y omite los pasos de aprovisionamiento del punto de conexión.

Para usar la plantilla Amazon Bedrock CloudFormation

1. Abre la consola OpenSearch de Amazon Service en https://console.aws.amazon.com/aos/home.
2. En el panel de navegación izquierdo, seleccione Integraciones.
3. En Integrar con el modelo Amazon Titan Text Embeddings mediante Amazon Bedrock, elija Configurar dominio y Configurar dominio público.
4. Siga las instrucciones para configurar el modelo.

> **Note**
>
> OpenSearch El servicio también proporciona una plantilla independiente para configurar el dominio de VPC. Si usa esta plantilla, debe proporcionar el ID de VPC para la función de Lambda.

Además, OpenSearch Service proporciona las siguientes plantillas de Amazon Bedrock para conectarse al modelo Cohere y al modelo de incrustaciones multimodales Amazon Titan:

- `Integration with Cohere Embed through Amazon Bedrock`
- `Integrate with Amazon Bedrock Titan Multi-modal`

Configuración de ML Commons no compatible

Amazon OpenSearch Service no admite el uso de las siguientes configuraciones de ML Commons:

- `plugins.ml_commons.allow_registering_model_via_url`
- `plugins.ml_commons.allow_registering_model_via_local_file`

Para obtener más información sobre la configuración de ML Commons, consulta la configuración del clúster de ML Commons.

Análisis de seguridad para Amazon OpenSearch Service

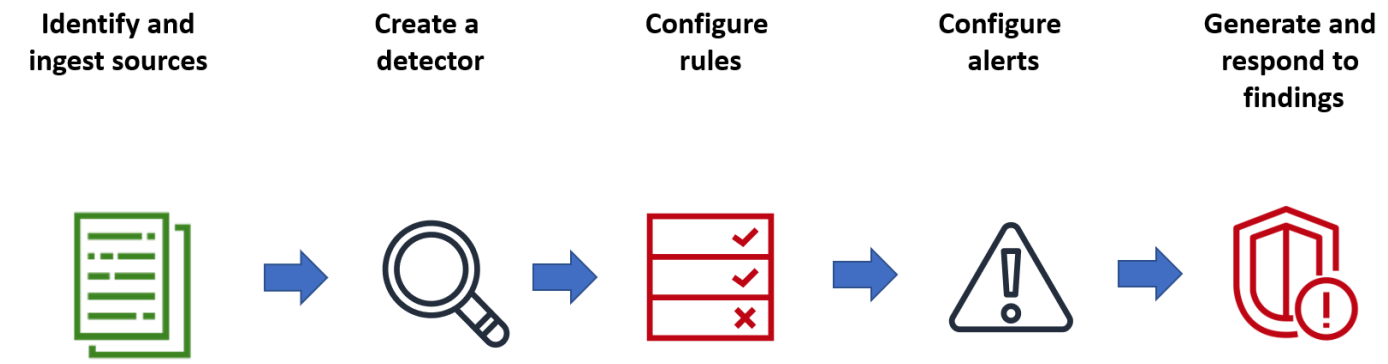
Security Analytics es una OpenSearch solución que proporciona visibilidad de la infraestructura de su organización, monitorea la actividad anómala, detecta posibles amenazas de seguridad en tiempo real y activa alertas a destinos preconfigurados. Puede monitorear la actividad maliciosa de sus registros de eventos de seguridad evaluando continuamente las reglas de seguridad y revisando los resultados de seguridad generados automáticamente. Además, Security Analytics puede generar alertas automatizadas y enviarlas a un canal de notificación específico, como Slack o el correo electrónico.

Puede usar el complemento Security Analytics para detectar amenazas comunes out-of-the-box y generar información de seguridad crítica a partir de los registros de eventos de seguridad existentes, como los registros de firewall, los registros de Windows y los registros de auditoría de autenticación. Para usar Security Analytics, su dominio debe ejecutar la OpenSearch versión 2.5 o posterior.

Para obtener más información sobre la configuración del complemento Security Analytics, consulte Security Analytics en la OpenSearch documentación.

Componentes y conceptos de Security Analytics

Una serie de herramientas y características constituyen la base del funcionamiento de Security Analytics. Los principales componentes que componen el complemento incluyen los detectores, los tipos de registro, las reglas, los resultados y las alertas.



Tipos de registro

OpenSearch admite varios tipos de registros y proporciona out-of-the-box mapeos para cada tipo. Al crear un detector, debe especificar el tipo de registro y configurar un intervalo de tiempo y, a partir de

ahí, Security Analytics activa automáticamente un conjunto de reglas relevante que se ejecutan en ese intervalo.

Detectores

Los detectores identifican una variedad de amenazas de ciberseguridad para un tipo de registro en todos sus índices de datos. El detector se configura para que utilice tanto reglas personalizadas como reglas Sigma preconfiguradas que evalúan los eventos que ocurren en el sistema. A continuación, el detector genera los resultados de seguridad a partir de estos eventos. Para obtener más información sobre los detectores, consulte Creación de detectores en la OpenSearch documentación.

Reglas

Las reglas de detección de amenazas definen las condiciones que los detectores aplican a los datos de registro incorporados para identificar un evento de seguridad. Security Analytics permite importar, crear y personalizar reglas para cumplir con sus requisitos, y también proporciona reglas Sigma empaquetadas previamente y de código abierto para detectar las amenazas más comunes en sus registros. Security Analytics asigna muchas reglas a una base de conocimientos cada vez mayor sobre tácticas y técnicas de los adversarios, mantenida por la organización MITRE ATT&CK. Puede usar los OpenSearch paneles de control o las API para crear y usar reglas. Para obtener más información sobre las reglas, consulte Trabajar con reglas en la OpenSearch documentación.

Resultados

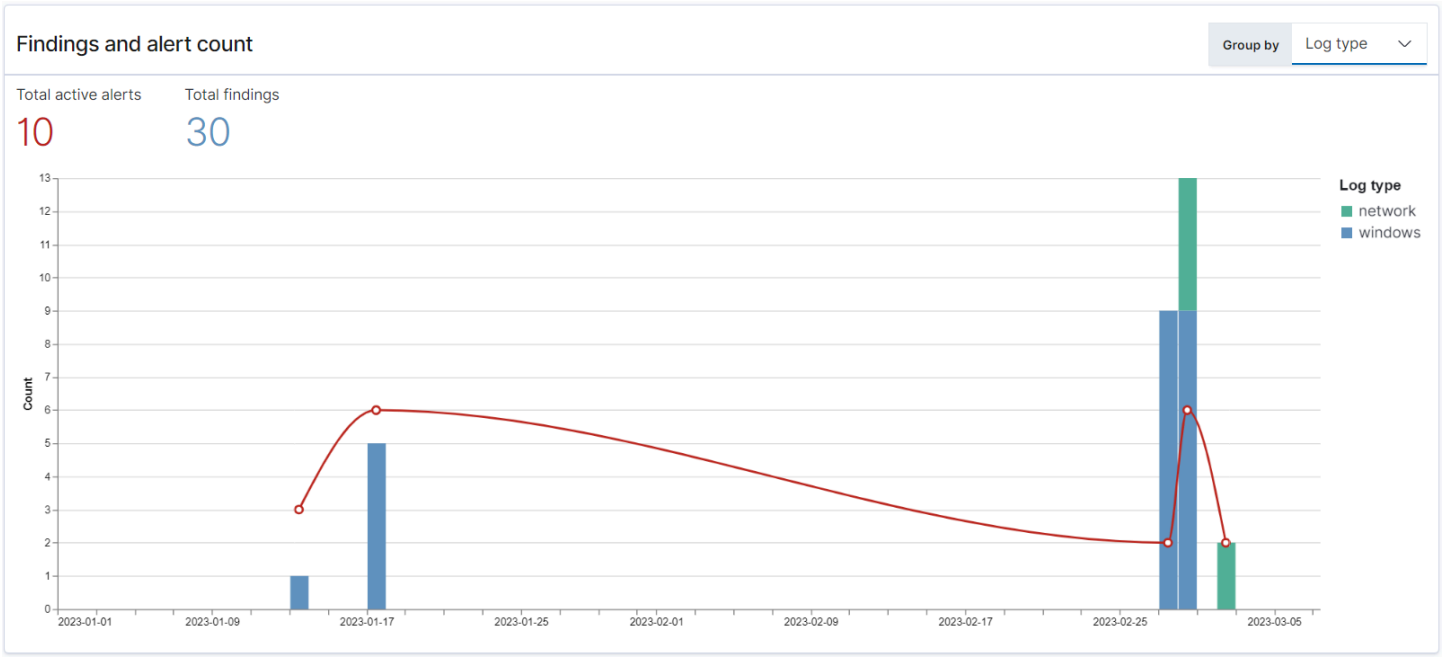
Cuando un detector hace coincidir una regla con un evento de registro, genera un resultado. Cada resultado incluye una combinación única de reglas seleccionadas, un tipo de registro y la gravedad de la regla. Los resultados no necesariamente apuntan a amenazas inminentes dentro del sistema, pero siempre aíslan un evento de interés. Para obtener más información sobre las conclusiones, consulte Trabajar con las conclusiones en la OpenSearch documentación.

Alertas

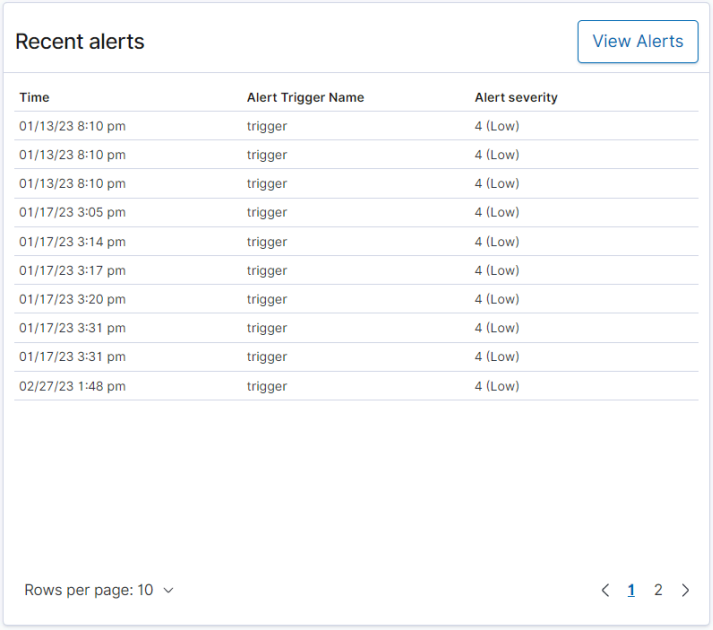
Al crear un detector, puede especificar una o varias condiciones que activan una alerta. Una alerta es una notificación que se envía a un canal preferido, como Slack o el correo electrónico. Puede configurar la alerta para que se active cuando el detector coincida con una o varias reglas y puede personalizar el mensaje de notificación. Para obtener más información sobre las alertas, consulte Trabajar con alertas en la OpenSearch documentación.

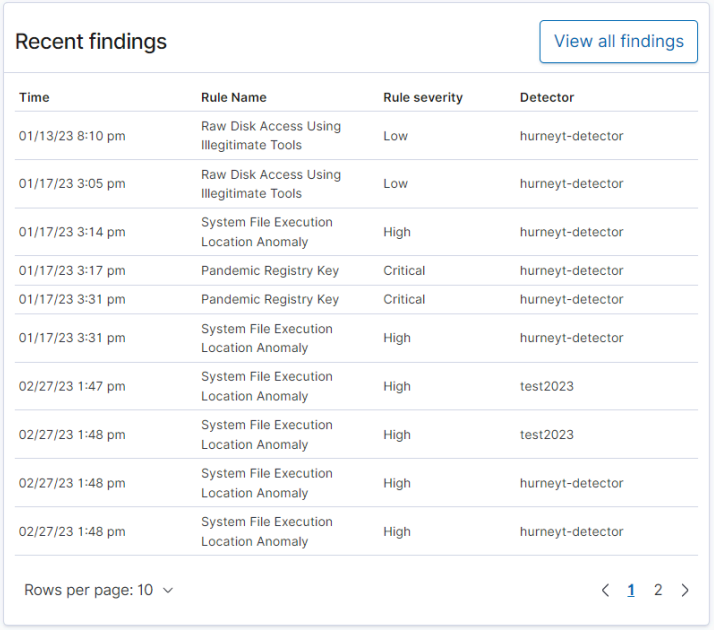
Exploración de Security Analytics

Puede usar los OpenSearch paneles de control para visualizar y obtener información sobre su complemento de análisis de seguridad. La vista general proporciona información como los hallazgos y el recuento de alertas, los hallazgos y alertas recientes, las reglas de detección frecuentes y una lista de sus detectores. Puede ver una vista resumida compuesta por varias visualizaciones. El siguiente gráfico, por ejemplo, muestra la tendencia de los resultados y las alertas de varios tipos de registros durante un período de tiempo determinado.



Más abajo en la página, puede revisar los resultados y alertas más recientes.





Además, puede ver una distribución de las reglas que se activan con más frecuencia en todos los detectores activos. Esto puede ayudarle a detectar e investigar diferentes tipos de actividades maliciosas en todos los tipos de registros.

Por último, puede ver el estado de los detectores configurados. Desde este panel, también puede acceder al flujo de trabajo de creación de detectores.

Para configurar Security Analytics, cree reglas en la página de Reglas y utilícelas para escribir los detectores en la página de Detectores. Para tener una visión más precisa de los resultados de Security Analytics, puede utilizar las páginas de Resultados y Alertas.

Configuración de permisos de

Si habilita Security Analytics en un dominio de OpenSearch servicio preexistente, es posible que la `security_analytics_manager` función no esté definida en el dominio. Los usuarios que no sean administradores deben estar asignados a este rol para poder administrar índices templados en los dominios mediante un control de acceso detallado. Para crear el rol `security_analytics_manager` de forma manual, siga estos pasos:

1. En los OpenSearch paneles, vaya a Seguridad y elija Permisos.
2. Elija Crear grupo de acciones y configure los siguientes grupos:

Nombre del grupo	Permisos
`security_analytics_full_access`	• `cluster:admin/opensearch/securityanalytics/alerts/*` • `cluster:admin/opensearch/securityanalytics/detector/*` • `cluster:admin/opensearch/securityanalytics/findings/*` • `cluster:admin/opensearch/securityanalytics/mapping/*` • `cluster:admin/opensearch/securityanalytics/rule/*`

Nombre del grupo	Permisos
`security_analytics_read_access`	• `cluster:admin/opensearch/securityanalytics/alerts/get` • `cluster:admin/opensearch/securityanalytics/detector/get` • `cluster:admin/opensearch/securityanalytics/detector/search` • `cluster:admin/opensearch/securityanalytics/findings/get` • `cluster:admin/opensearch/securityanalytics/mapping/get` • `cluster:admin/opensearch/securityanalytics/mapping/view/get` • `cluster:admin/opensearch/securityanalytics/rule/get` • `cluster:admin/opensearch/securityanalytics/rule/search`

3. Elija Roles y, a continuación, elija Crear rol.
4. Asigne el nombre security_analytics_manager al rol.
5. Para Permisos de clúster, seleccione `security_analytics_full_access` y `security_analytics_read_access`.
6. Para Índice, escriba `*`.
7. Para Permisos de índice, seleccione `indices:admin/mapping/put` y `indices:admin/mappings/get`.
8. Seleccione Crear.
9. Después de crear el rol, debe mapearlo a cualquier rol de usuario o back-end que administre los índices de Security Analytics.

Solución de problemas

No existe tal error de índice

Si no tiene detectores y abre el panel de Security Analytics, es posible que vea una notificación en la parte inferior derecha que diga `[index_not_found_exception] no such index [.opensearch-sap-detectors-config]`. Puede ignorar esta notificación, que desaparece en unos segundos y no volverá a aparecer una vez que crea un detector.

Observabilidad en Amazon OpenSearch Service

La instalación predeterminada de OpenSearch Dashboards para Amazon OpenSearch Service incluye el complemento Observability, que se puede utilizar para visualizar eventos controlados por datos mediante el lenguaje de procesamiento con plecas (PPL) para explorar, descubrir y consultar los datos almacenados en OpenSearch. Este complemento requiere OpenSearch 1.2 o posterior.

El complemento Observability proporciona una experiencia unificada para recopilar y supervisar métricas, registros y seguimientos de orígenes de datos habituales. La recopilación y supervisión de datos en un solo lugar permite una observabilidad integral de extremo a extremo de toda la infraestructura. La documentación completa sobre el complemento Observability está disponible en la documentación de OpenSearch.

Cada cual tiene un proceso de exploración de datos diferente. Si no tiene experiencia explorando datos y creando visualizaciones, le recomendamos que pruebe un flujo de trabajo como el siguiente:

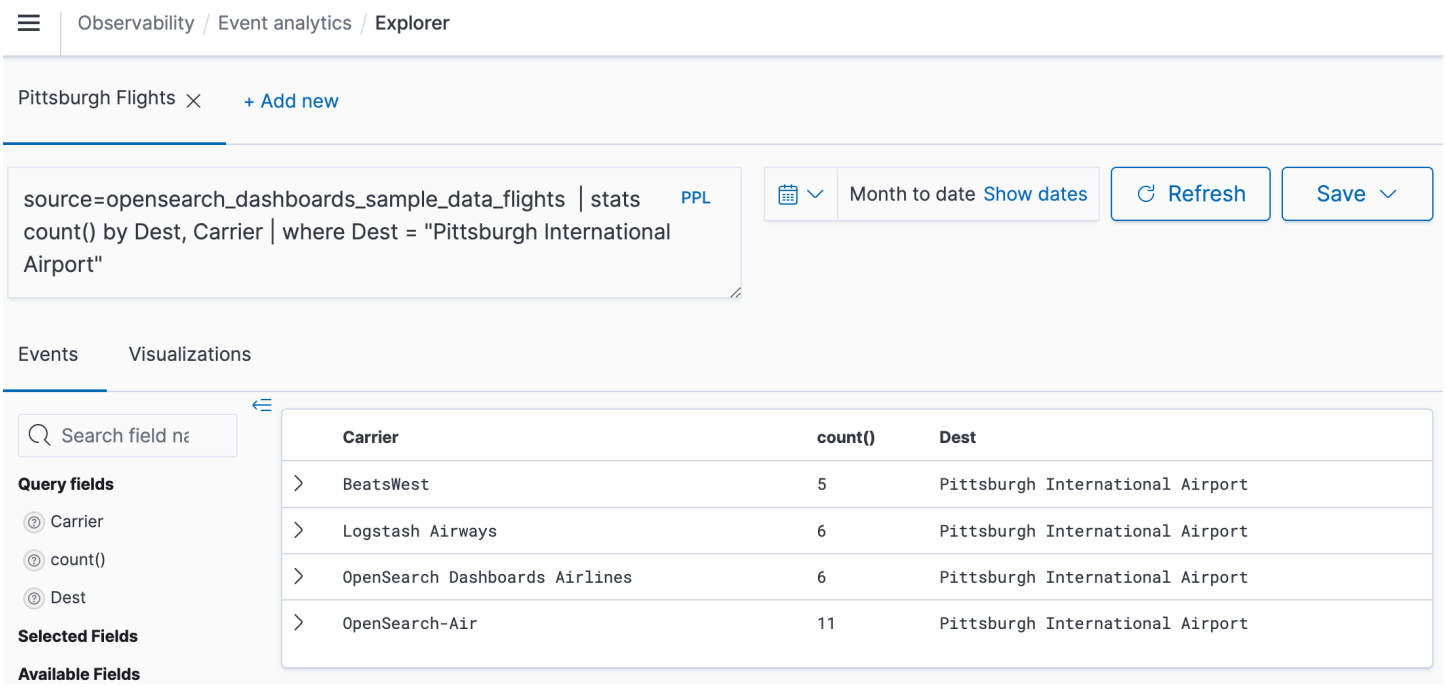
Explore los datos con análisis de eventos

Para empezar, supongamos que está recopilando datos de vuelos en un dominio de OpenSearch Service y desea averiguar qué aerolínea tuvo más llegadas de vuelos desde el Aeropuerto Internacional de Pittsburgh el mes pasado. Escribe la siguiente consulta PPL:

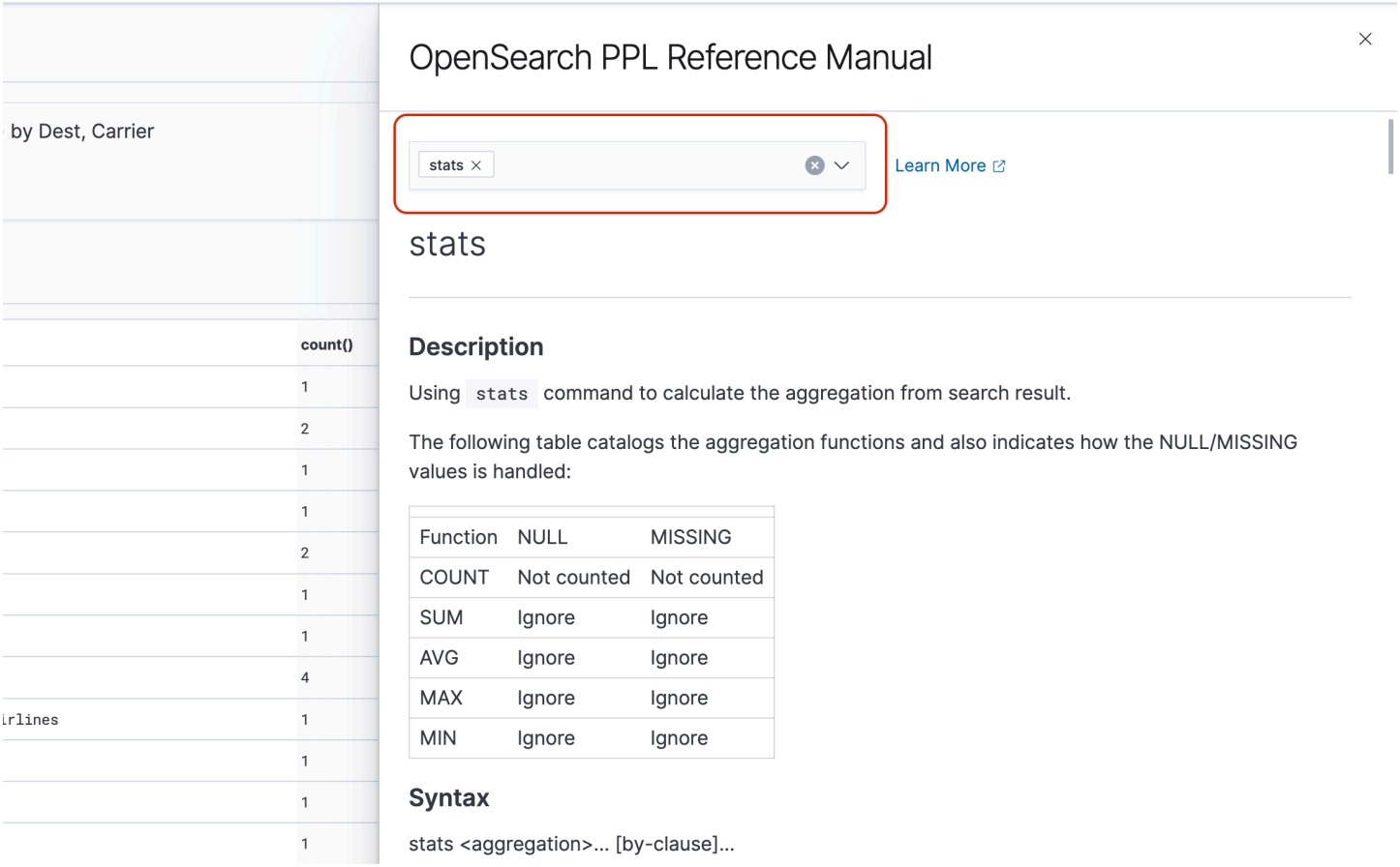
```
source=opensearch_dashboards_sample_data_flights |
    stats count() by Dest, Carrier |
    where Dest = "Pittsburgh International Airport"
```

Esta consulta extrae datos del índice denominado `opensearch_dashboards_sample_data_flights`. A continuación, utiliza el comando `stats` para obtener un recuento total de vuelos y agrupar por aeropuerto de destino y aerolínea. Por último, utiliza la cláusula `where` para filtrar los resultados y mostrar los vuelos con llegada al Aeropuerto Internacional de Pittsburgh.

Este es el aspecto de los datos que se muestran para el último mes:



Puede elegir el botón PPL del editor de consultas para obtener información y ejemplos de uso de cada comando PPL:



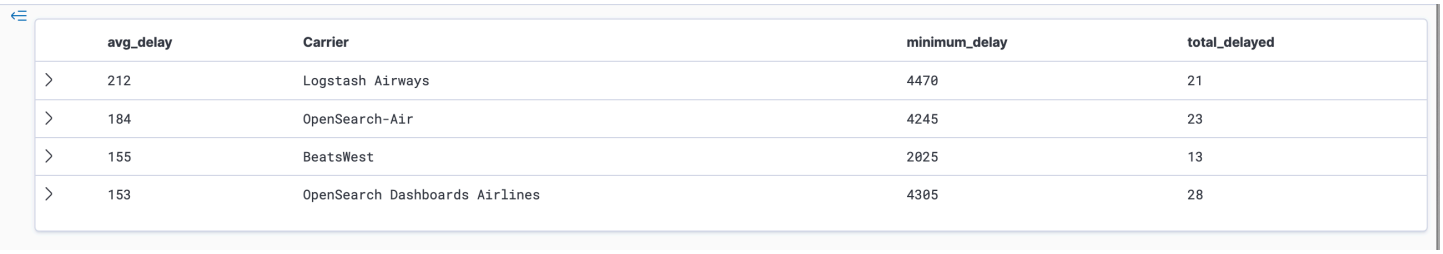
Veamos un ejemplo más complejo, en el que se realizan consultas de información sobre retrasos de vuelos:

```
source=opensearch_dashboards_sample_data_flights |
    where FlightDelayMin > 0 |
    stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier,
 Dest |
    eval avg_delay=minimum_delay / total_delayed |
    sort - avg_delay
```

Cada comando de la consulta afecta al resultado final:

- `source=opensearch_dashboards_sample_data_flights`: extrae datos del mismo índice que el ejemplo anterior
- `where FlightDelayMin > 0`: filtra los datos para mostrar los vuelos retrasados
- `stats sum(FlightDelayMin) as minimum_delay, count() as total_delayed by Carrier`: para cada aerolínea, obtiene el tiempo de retraso mínimo total y el recuento total de vuelos retrasados
- `eval avg_delay=minimum_delay / total_delayed`: calcula el tiempo de retraso medio de cada aerolínea dividiendo el tiempo de retraso mínimo entre el número total de vuelos retrasados
- `sort - avg_delay`: ordena los resultados por retraso medio en orden descendente

Con esta consulta, se puede determinar que OpenSearch Dashboards Airlines tiene menos retrasos de media.



	avg_delay	Carrier	minimum_delay	total_delayed
>	212	Logstash Airways	4470	21
>	184	OpenSearch-Air	4245	23
>	155	BeatsWest	2025	13
>	153	OpenSearch Dashboards Airlines	4305	28

Dispone de más ejemplos de consultas PPL en Queries and Visualizations (Consultas y visualizaciones) en la página Event analytics (Análisis de eventos).

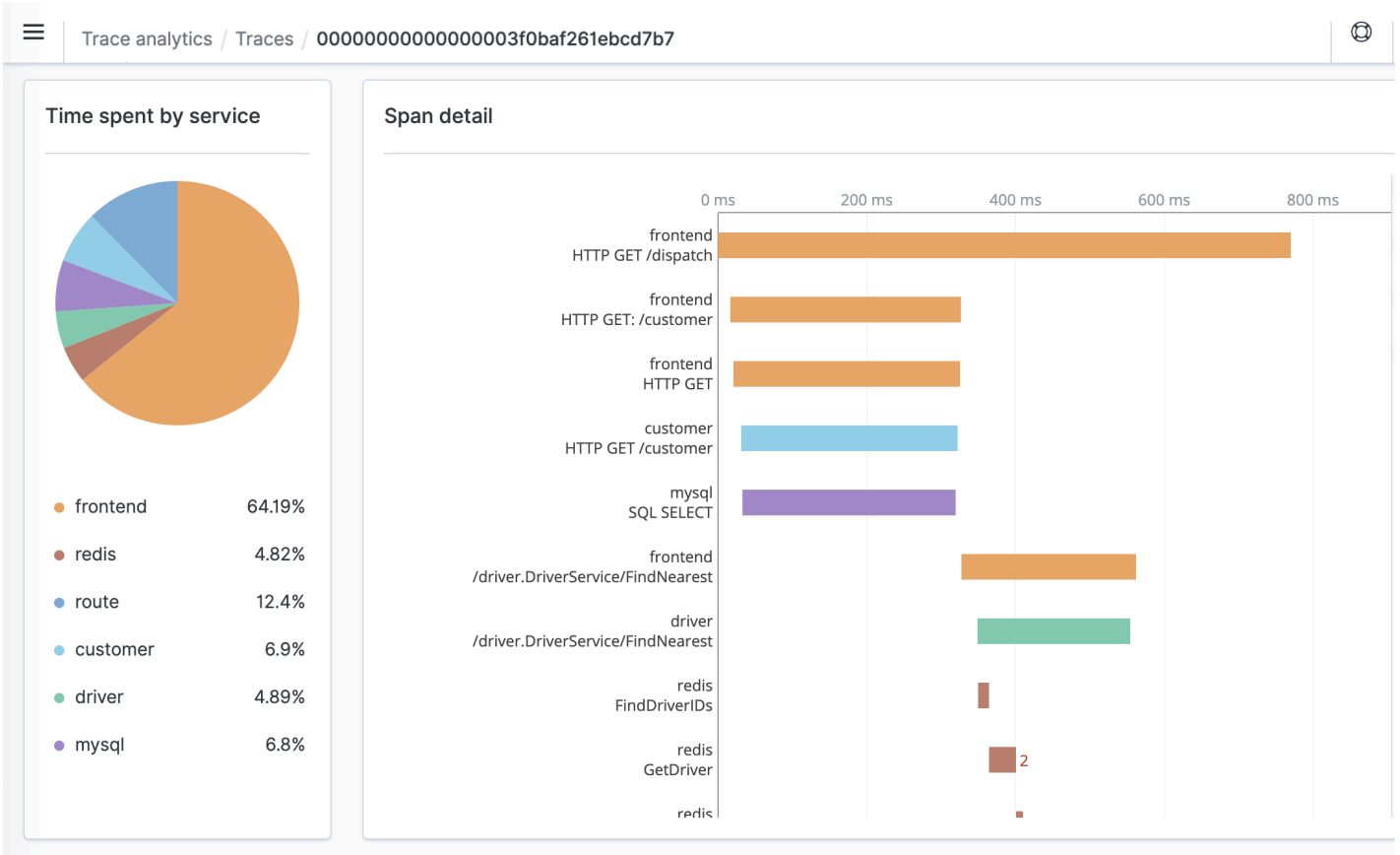
Crear visualizaciones

Una vez que haya consultado correctamente los datos que le interesan, puede guardar esas consultas como visualizaciones:

A continuación, agregue esas visualizaciones a paneles operacionales para comparar diferentes datos. Aproveche los cuadernos para combinar diferentes visualizaciones y bloques de código y compartirlos con miembros de su equipo.

Profundizar más con Trace Analytics

Trace Analytics proporciona una forma de visualizar el flujo de eventos de los datos de OpenSearch para identificar y solucionar problemas de rendimiento en aplicaciones distribuidas.

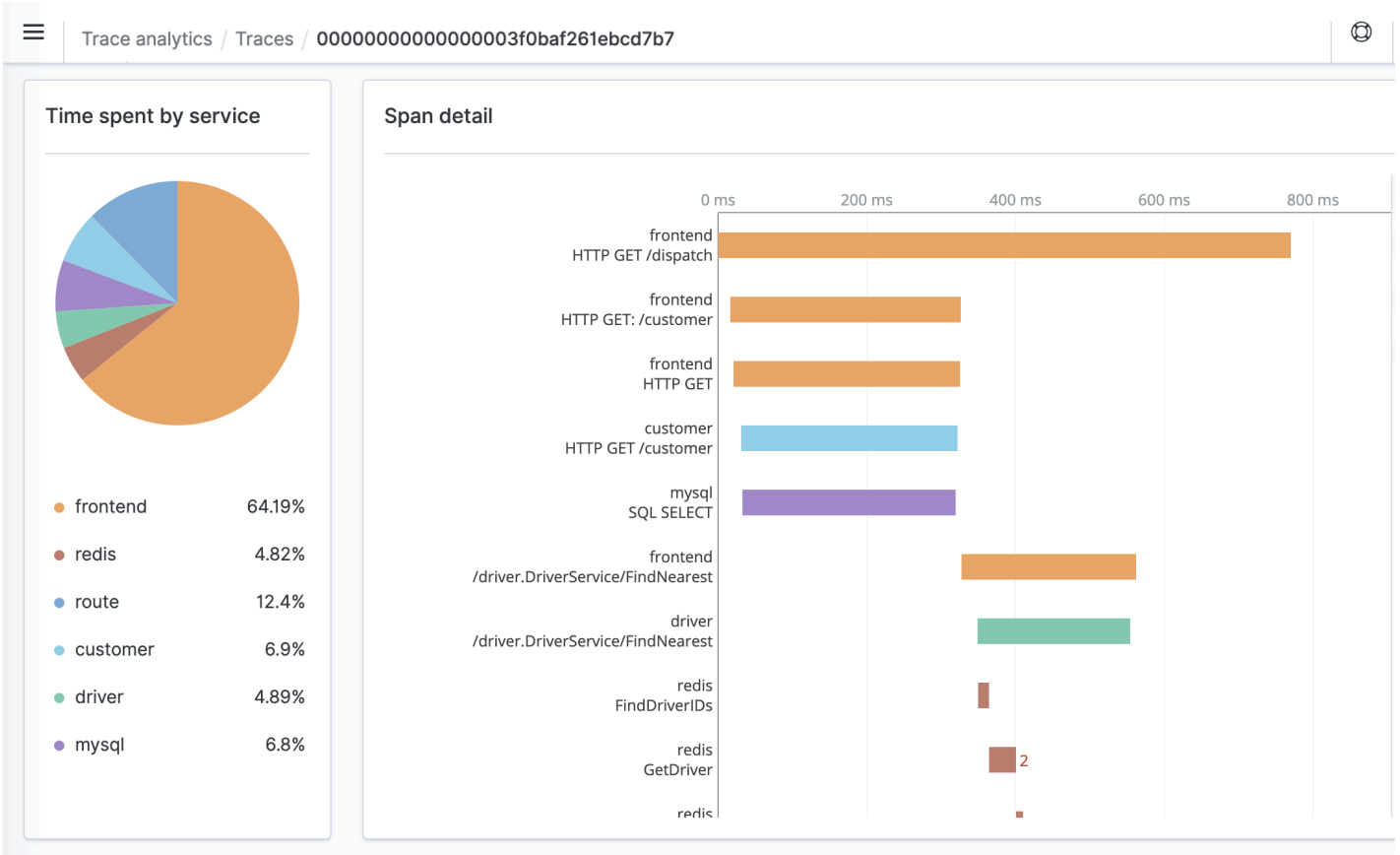


Análisis de seguimiento para Amazon OpenSearch Service

Puede utilizar Trace Analytics, que forma parte del complemento Observability de OpenSearch, para analizar datos de seguimiento de aplicaciones distribuidas. Trace Analytics requiere OpenSearch o Elasticsearch 7.9 o posterior.

En una aplicación distribuida, una sola operación, como un usuario que hace clic en un botón, puede desencadenar una serie extendida de eventos. Por ejemplo, el front-end de la aplicación puede llamar a un servicio backend, que llama a otro servicio, que consulta una base de datos, que procesa la consulta y devuelve un resultado. Luego, el primer servicio backend envía una confirmación al front-end, que actualiza la interfaz de usuario.

Puede utilizar Trace Analytics para ayudarle a visualizar este flujo de eventos e identificar problemas de rendimiento.



Requisitos previos

Trace Analytics requiere que agregue instrumentación a su aplicación y genere datos de rastreo usando una biblioteca compatible con OpenTelemetry como Jaeger or Zipkin. Este paso se produce completamente fuera de OpenSearch Service. La AWSDocumentación de la Distro para OpenTelemetry contiene aplicaciones de ejemplo para muchos lenguajes de programación que pueden ayudarle a comenzar, que incluyen Java, Python, Go y JavaScript.

Después de agregar la instrumentación a la aplicación, el Recopilador de OpenTelemetry recibe datos de la aplicación y los formatea en datos de OpenTelemetry. Vea la lista de receptores en GitHub.AWS La distribución para OpenTelemetry incluye un Receptor para AWS X-Ray.

Por último, Data Prepper, un componente independiente de OpenSearch, da formato a los datos de OpenTelemetry para su uso con OpenSearch. Data Prepper se ejecuta en un equipo fuera del clúster de OpenSearch Service, similar a Logstash.

Para obtener un archivo Docker Compose que demuestre el flujo de datos de extremo a extremo, consulte la Documentación de OpenSearch.

Configuración de ejemplo de OpenTelemetry Collector

Para utilizar OpenTeletry Collector con Amazon OpenSearch Ingestion, pruebe la siguiente configuración de ejemplo:

```
extensions:
  sigv4auth:
    region: "us-east-1"
    service: "osis"

receivers:
  jaeger:
    protocols:
      grpc:

exporters:
  otlphttp:
    traces_endpoint: "https://pipeline-endpoint.us-east-1.osis.amazonaws.com/
opentelemetry.proto.collector.trace.v1.TraceService/Export"
    auth:
      authenticator: sigv4auth
    compression: none

service:
  extensions: [sigv4auth]
  pipelines:
    traces:
      receivers: [jaeger]
      exporters: [otlphttp]
```

Configuración de muestra de OpenSearch Ingestion

Para enviar datos de seguimiento a un dominio de servicio OpenSearch, pruebe la siguiente configuración de canalización de ingestión OpenSearch de ejemplo. Para obtener instrucciones sobre cómo crear una canalización, consulte Creación de canalizaciones de Amazon OpenSearch Ingestion.

```
version: "2"
otel-trace-pipeline:
  source:
    otel_trace_source:
```

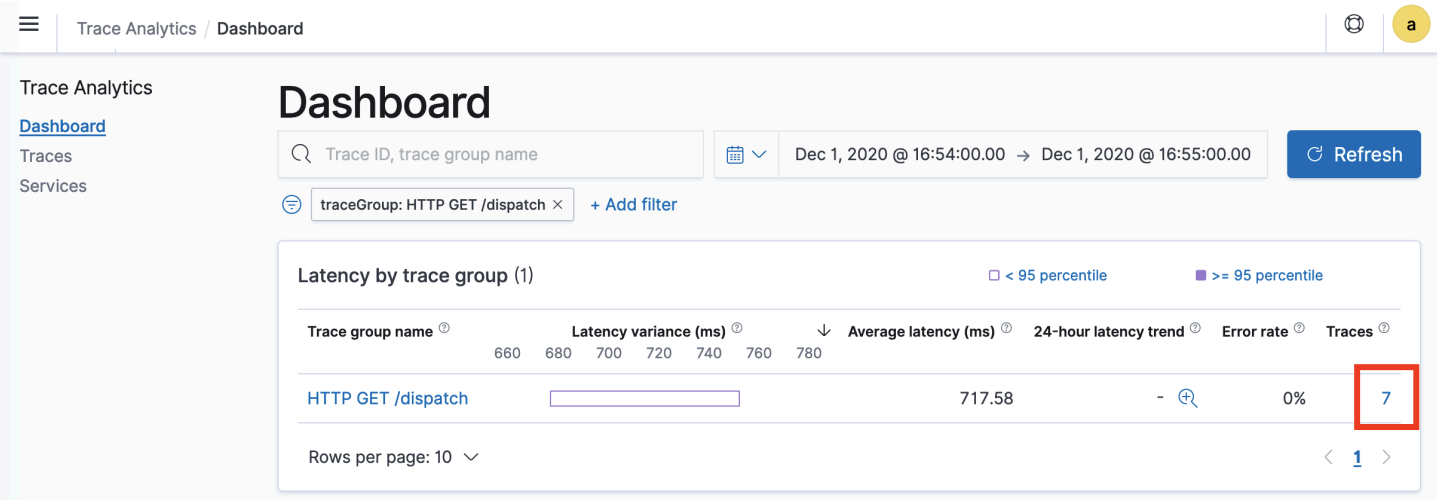
```
      "/${pipelineName}/ingest"
  processor:
    - trace_peer_forwarder:
  sink:
    - pipeline:
        name: "trace_pipeline"
    - pipeline:
        name: "service_map_pipeline"
trace-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - otel_traces:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-raw
        aws:
          # IAM role that OpenSearch Ingestion assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"

service-map-pipeline:
  source:
    pipeline:
      name: "otel-trace-pipeline"
  processor:
    - service_map:
  sink:
    - opensearch:
        hosts: ["https://domain-endpoint"]
        index_type: trace-analytics-service-map
        aws:
          # IAM role that the pipeline assumes to access the domain sink
          sts_role_arn: "arn:aws:iam::{account-id}:role/pipeline-role"
          region: "us-east-1"
```

El rol de canalización que especifique en la opción `sts_role_arn` debe disponer de permisos de escritura en el receptor del dominio. Para obtener instrucciones sobre cómo configurar los permisos para el rol de canalización, consulte Permitir que las canalizaciones de Amazon OpenSearch Ingestion escriban en los dominios.

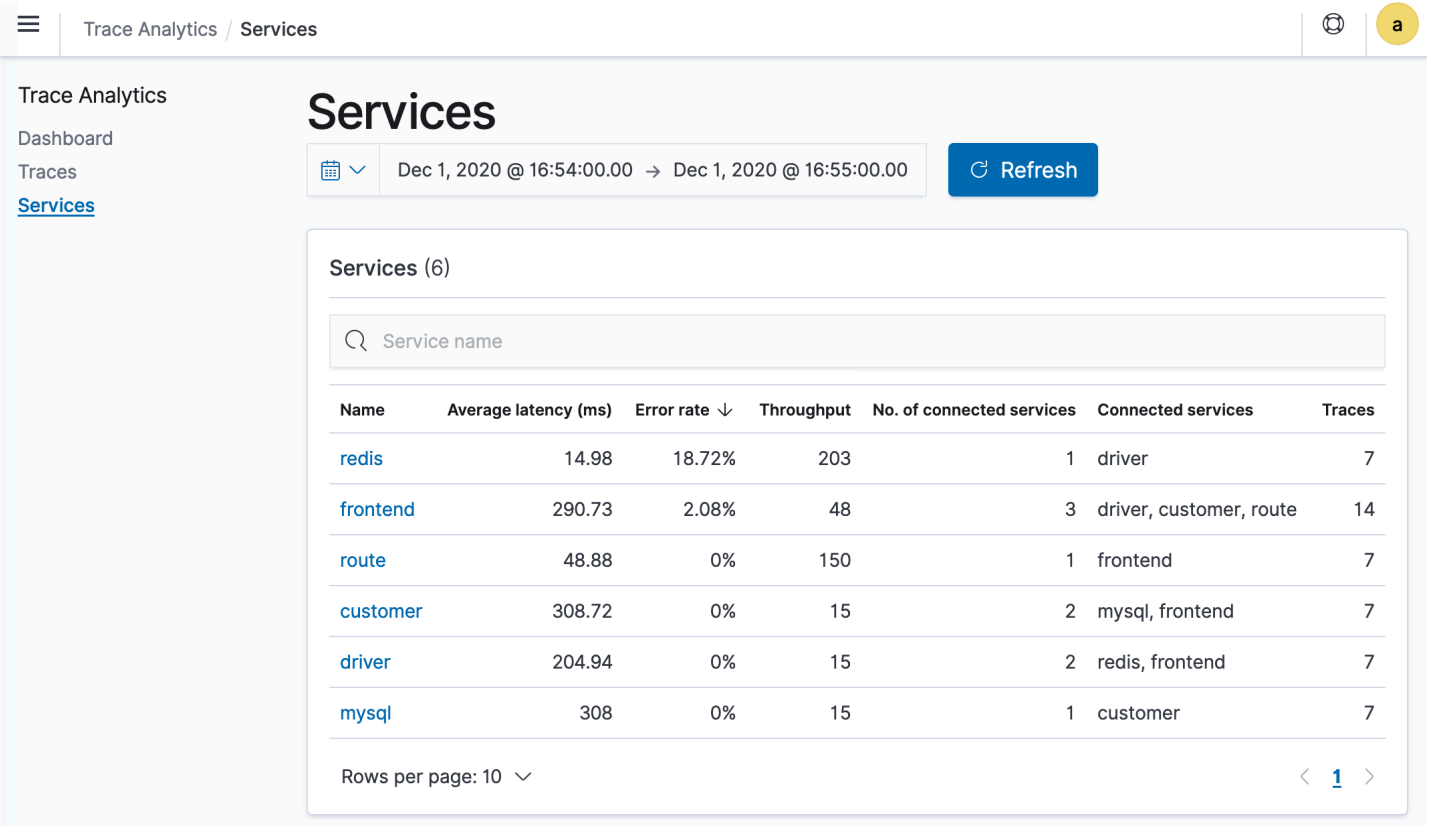
Exploración de datos de rastreo

La vista de Panel agrupa los rastreos por método HTTP y ruta de acceso para que pueda ver la latencia media, la tasa de error y las tendencias asociadas a una operación concreta. Para obtener una vista más enfocada, intente filtrar por nombre de grupo de rastreo.



Para detallar los rastreos que componen un grupo de rastreo, elija el número de rastreos en la columna de la derecha. A continuación, elija un rastreo individual para obtener un resumen detallado.

La vista de Servicios contiene todos los servicios de la aplicación, además de un mapa interactivo que muestra cómo los distintos servicios se conectan entre sí. A diferencia del panel (que ayuda a identificar problemas por operación), el mapa de servicio le ayuda a identificar problemas por servicio. Intente ordenar por tasa de error o latencia para obtener una idea de las áreas problemáticas potenciales de su aplicación.



Consulta de datos de Amazon OpenSearch Service mediante el lenguaje de procesamiento de canalizaciones

El lenguaje de procesamiento de canalizaciones (PPL) es un lenguaje de consulta que permite utilizar la sintaxis de canalizaciones (|) para consultar los datos almacenados en Amazon OpenSearch Service.

La sintaxis PPL consta de comandos delimitados por un carácter de canalización (|) donde los datos fluyen de izquierda a derecha a través de cada canalización. Por ejemplo, la sintaxis PPL para buscar el número de anfitriones con errores HTTP 403 o 503, agregarlos por anfitrión y ordenarlos en el orden de impacto es la siguiente:

```
source = dashboards_sample_data_logs | where response='403' or response='503' | stats
 count(request) as request_count by host, response | sort -request_count
```

La PPL requiere OpenSearch o Elasticsearch 7.9 o posterior. Los pasos detallados y las descripciones de los comandos están disponibles en el OpenSearch PPL reference manual (Manual de referencia de PPL de OpenSearch).

Para comenzar, elija Query Workbench (Consulta del entorno de trabajo) en OpenSearch Dashboards y seleccione PPL. Utilice la operación `bulk` para indexar algunos datos de muestra:

```
PUT accounts/_bulk?refresh
{"index":{"_id":"1"}}
{"account_number":1,"balance":39225,"firstname":"Amber","lastname":"Duke","age":32,"gender":"M"
 Holmes
 Lane","employer":"Pyrami","email":"amberduke@pyrami.com","city":"Brogan","state":"IL"}
{"index":{"_id":"6"}}
{"account_number":6,"balance":5686,"firstname":"Hattie","lastname":"Bond","age":36,"gender":"M"
 Bristol
 Street","employer":"Netagy","email":"hattiebond@netagy.com","city":"Dante","state":"TN"}
{"index":{"_id":"13"}}
{"account_number":13,"balance":32838,"firstname":"Nanette","lastname":"Bates","age":28,"gender"
 Mady Street","employer":"Quility","city":"Nogal","state":"VA"}
{"index":{"_id":"18"}}
{"account_number":18,"balance":4180,"firstname":"Dale","lastname":"Adams","age":33,"gender":"M"
 Hutchinson Court","email":"daleadams@boink.com","city":"Orick","state":"MD"}
```

En el siguiente ejemplo, se devuelven los campos `firstname` y `lastname` para documentos en un índice de cuentas con `age`: mayor que 18:

```
search source=accounts | where age > 18 | fields firstname, lastname
```

Respuesta de ejemplo

id	firstname	lastname
0	Amber	Duke
1	Hattie	Bond
2	Nanette	Bates
3	Dale	Adams

Puede utilizar un conjunto completo de comandos de solo lectura como `search`, `where`, `fields`, `rename`, `dedup`, `stats`, `sort`, `eval`, `head`, `top` `rare`. Para obtener descripciones y ejemplos de cada comando, consulte el OpenSearch PPL reference manual (Manual de referencia de PPL de OpenSearch).

El complemento PPL admite todas las funciones SQL, incluidas las matemáticas, las trigonométricas, las de fecha y hora, las de cadena, las agregadas, las de operadores y expresiones avanzadas. Para obtener más información, consulte el OpenSearch PPL reference manual (Manual de referencia de PPL de OpenSearch).

Mejores prácticas operativas para Amazon OpenSearch Service

Este capítulo proporciona las mejores prácticas para operar los dominios de Amazon OpenSearch Service e incluye pautas generales que se aplican a muchos casos de uso. Cada carga de trabajo es única, con características únicas, por lo que ninguna recomendación genérica es exactamente adecuada para cada caso de uso. La práctica general más importante consiste en implementar, probar y ajustar sus dominios en un ciclo continuo para encontrar la configuración, la estabilidad y el costo óptimos para su carga de trabajo.

Temas

Monitorización y alertas

Las siguientes prácticas recomendadas se aplican a la supervisión de sus dominios OpenSearch de servicio.

Configure CloudWatch las alarmas

OpenSearch El servicio emite métricas de rendimiento a Amazon CloudWatch. Revisa periódicamente las métricas de tu clúster e instancia y configura las CloudWatch alarmas recomendadas en función del rendimiento de tu carga de trabajo.

Habilitación de la publicación de registros

OpenSearch El servicio expone los registros de OpenSearch errores, los registros lentos de búsqueda, los registros lentos de indexación y los registros de auditoría en Amazon CloudWatch Logs. Los registros lentos de búsqueda, los registros lentos de índice y los registros de errores son útiles para la resolución de problemas de rendimiento y estabilidad. Los registros de auditoría, que solo están disponibles si habilita control de acceso preciso, realizan un seguimiento de la actividad del usuario. Para obtener más información, consulte los registros en la OpenSearch documentación.

Los registros lentos de búsqueda e indexación de registros lentos son una herramienta importante para comprender y solucionar problemas del rendimiento de sus operaciones de búsqueda e indexación. Habilite la entrega lenta de registros de búsqueda e índice para todos los dominios de producción. También debe configurar los umbrales de registro; de lo contrario, CloudWatch no capturará los registros.

Estrategia de particiones

Los fragmentos distribuyen la carga de trabajo entre los nodos de datos de su OpenSearch dominio de servicio. Los índices configurados correctamente pueden ayudar a mejorar el rendimiento general del dominio.

Cuando envías datos al OpenSearch Servicio, los envías a un índice. Un índice es análogo a una tabla de base de datos, con documentos como las filas y campos como las columnas. Al crear el índice, indica OpenSearch cuántos fragmentos principales desea crear. Los fragmentos principales son particiones independientes del conjunto de datos completo. OpenSearch El servicio distribuye automáticamente los datos entre los fragmentos principales de un índice. También puede configurar réplicas del índice. Cada partición de réplica incluye un conjunto completo de copias de las particiones principales de ese índice.

OpenSearch El servicio mapea los fragmentos de cada índice en los nodos de datos del clúster. Garantiza que las particiones principales y de réplica del índice residan en nodos de datos diferentes. La primera réplica garantiza que tenga dos copias de los datos en el índice. Siempre debe usar al menos una réplica. Las réplicas adicionales proporcionan redundancia y capacidad de lectura adicionales.

OpenSearch envía solicitudes de indexación a todos los nodos de datos que contienen fragmentos que pertenecen al índice. Envía solicitudes de indexación primero a los nodos de datos que contienen particiones principales y, después, a los nodos de datos que contienen particiones de

réplica. El nodo coordinador dirige las solicitudes de búsqueda, ya sea a una partición principal o a una réplica, para todas las particiones que pertenecen al índice.

Por ejemplo, para un índice con cinco particiones principales y una réplica, cada solicitud de indexación toca 10 particiones. En contraste, las solicitudes de búsqueda se envían a las particiones n, donde n es el número de particiones principales. Para un índice con cinco particiones principales y una réplica, cada consulta de búsqueda toca cinco particiones (principales o réplicas) de ese índice.

Determinar los recuentos de particiones y nodos de datos

Utilice las siguientes prácticas recomendadas para determinar los recuentos de nodos de datos y particiones para su dominio.

Tamaño de las particiones: el tamaño de los datos en el disco es un resultado directo del tamaño de los datos de origen y cambia a medida que se indexan más datos. La source-to-index proporción puede variar considerablemente, de 1:10 a 10:1 o más, pero por lo general es de alrededor de 1:1,10. Puede usar esa relación para predecir el tamaño del índice en el disco. Puede también indexar algunos datos y recuperar los tamaños reales del índice para determinar la relación de la carga de trabajo. Después de tener un tamaño de índice previsto, establezca un recuento de particiones para que cada partición tenga entre 10 y 30 GiB (para cargas de trabajo de búsqueda) o entre 30 y 50 GiB (para cargas de trabajo de registros). 50 GiB debería ser el máximo; asegúrese de planificar el crecimiento.

Recuento de particiones: la distribución de particiones a los nodos de datos tiene un gran impacto en el rendimiento de un dominio. Cuando tenga índices con múltiples particiones, intente hacer que el recuento de particiones sea un múltiplo par del recuento de nodos de datos. Esto ayuda a garantizar que las particiones se distribuyan de manera uniforme entre los nodos de datos y evita los nodos activos. Por ejemplo, si tiene 12 particiones principales, el recuento de nodos de datos debe ser 2, 3, 4, 6 o 12. Sin embargo, el recuento de particiones es secundario al tamaño de la partición; si tiene 5 GiB de datos, debe seguir utilizando una sola partición.

Particiones por nodo de datos: el número total de particiones que puede contener un nodo es proporcional a la memoria en montón de máquina virtual Java (JVM) del nodo. Trate de obtener 25 particiones o menos por GiB de memoria en montón. Por ejemplo, un nodo con 32 GiB de memoria en montón no debe contener más de 800 particiones. Aunque la distribución de particiones puede variar según los patrones de carga de trabajo, hay un límite de 1000 particiones por nodo. La API cat/allocation proporciona una vista rápida de la cantidad de particiones y el almacenamiento total de particiones en los nodos de datos.

Proporción de partición a CPU: cuando una partición participa en una solicitud de indexación o búsqueda, utiliza una vCPU para procesar la solicitud. Como práctica recomendada, utilice un punto de escala inicial de 1,5 vCPU por partición. Si su tipo de instancia tiene 8 vCPU, configure el recuento de nodos de datos para que cada nodo no tenga más de seis particiones. Tenga en cuenta que se trata de una aproximación. Asegúrese de probar la carga de trabajo y escalar el clúster en consecuencia.

Para obtener recomendaciones sobre el volumen de almacenamiento, el tamaño de las particiones y el tipo de instancia, consulte los recursos siguientes:

- the section called “Determinación del tamaño de dominios”
- the section called “Escala de petabytes”

Evite el sesgo de almacenamiento

El sesgo de almacenamiento ocurre cuando uno o más nodos de un clúster contienen una mayor proporción de almacenamiento para uno o más índices que los demás. Los indicios de que hay sesgo de almacenamiento incluyen utilización desigual de la CPU, latencia intermitente y desigual, y colocación en cola desigual en los nodos de datos. Para determinar si tiene problemas de sesgo, consulte las siguientes secciones de solución de problemas:

- the section called “Partición de nodos y sesgo de almacenamiento”
- the section called “Partición del índice y el sesgo de almacenamiento”

Stability

Las siguientes prácticas recomendadas se aplican para mantener un dominio de servicio estable y en buen estado. OpenSearch

Manténgase al día con OpenSearch

Actualizaciones del software del servicio

OpenSearch El servicio publica periódicamente actualizaciones de software que añaden funciones o mejoran sus dominios. Las actualizaciones no cambian la versión del motor de búsqueda OpenSearch ni la de Elasticsearch. Te recomendamos programar una hora periódica para ejecutar la operación de la DescribeDomainAPI e iniciar una actualización del software del

`UpdateStatus` servicio, si es así. `ELIGIBLE` Si no actualizas tu dominio dentro de un período de tiempo determinado (normalmente dos semanas), el OpenSearch Servicio realizará la actualización automáticamente.

OpenSearch actualizaciones de versión

OpenSearch El servicio añade periódicamente soporte para las versiones mantenidas por la comunidad de OpenSearch. Actualice siempre a las OpenSearch versiones más recientes cuando estén disponibles.

OpenSearch El servicio actualiza simultáneamente OpenSearch tanto los OpenSearch paneles como los de Elasticsearch (o Elasticsearch y Kibana si tu dominio ejecuta un motor antiguo). Si el clúster tiene nodos maestros dedicados, las actualizaciones se completan sin tiempo de inactividad. De lo contrario, es posible que el clúster deje de responder durante varios segundos después de la actualización mientras elige un nodo principal. OpenSearch Es posible que los paneles no estén disponibles durante parte de la actualización o durante toda la actualización.

Hay dos formas de actualizar un dominio:

- Actualización local: esta opción es más fácil porque mantiene el mismo clúster.
- Actualización de instantáneas y restauración: esta opción es buena para probar nuevas versiones en un clúster nuevo o migrar entre clústeres.

Independientemente del proceso de actualización que utilice, recomendamos mantener un dominio que sea únicamente para desarrollo y pruebas y actualizarlo a la nueva versión antes de actualizar el dominio de producción. Para el tipo de implementación, seleccione Desarrollo y pruebas cuando cree el dominio de prueba. Asegúrese de actualizar todos los clientes a versiones compatibles inmediatamente después de la actualización del dominio.

Cómo mejorar el rendimiento de las instantáneas

Para evitar que la instantánea se bloquee durante el procesamiento, el tipo de instancia del nodo maestro dedicado debe coincidir con el número de particiones. Para más información, consulte the section called “Elección de tipos de instancias para nodos principales dedicados”. Además, cada nodo no debe tener más de las 25 particiones recomendadas por cada GiB de memoria dinámica de Java. Para más información, consulte the section called “Selección del número de particiones”.

Habilite los nodos maestros dedicados

Nodos maestros dedicados para mejorar la estabilidad de los clústeres. Un nodo maestro dedicado realiza tareas de administración de clústeres, pero no contiene datos de índice ni responde a las solicitudes de los clientes. Al asumir de este modo las tareas de administración de clústeres, aumenta la estabilidad de su dominio y hace posible que se lleven a cabo algunos cambios de configuración sin tiempo de inactividad.

Habilite y utilice tres nodos maestros dedicados para lograr una estabilidad óptima del dominio en tres zonas de disponibilidad. La implementación con Multi-AZ con modo de espera le permite configurar tres nodos maestros dedicados. Para obtener recomendaciones de tipos de instancias, consulte the section called “Elección de tipos de instancias para nodos principales dedicados”.

Implemente en varias zonas de disponibilidad

Para evitar que se pierdan datos y minimizar el tiempo de inactividad del clúster en caso de que se produzca una interrupción del servicio, puede distribuir los nodos en dos o tres zonas de disponibilidad de la misma Región de AWS. La práctica recomendada es realizar la implementación mediante Multi-AZ con modo de espera, que configura tres zonas de disponibilidad: dos zonas activas y una en espera, y con dos particiones de réplicas por índice. Esta configuración permite a OpenSearch Service distribuir los fragmentos de réplica en zonas de disponibilidad distintas a las de sus correspondientes fragmentos principales. No hay cargos por transferencia de datos entre zonas de disponibilidad para las comunicaciones de clústeres entre zonas de disponibilidad.

Las zonas de disponibilidad son ubicaciones aisladas dentro de cada región. Con una configuración de dos zonas de disponibilidad, perder una zona de disponibilidad significa que se pierde la mitad de toda la capacidad del dominio. El cambio a tres zonas de disponibilidad reduce aún más el impacto de perder una sola zona de disponibilidad.

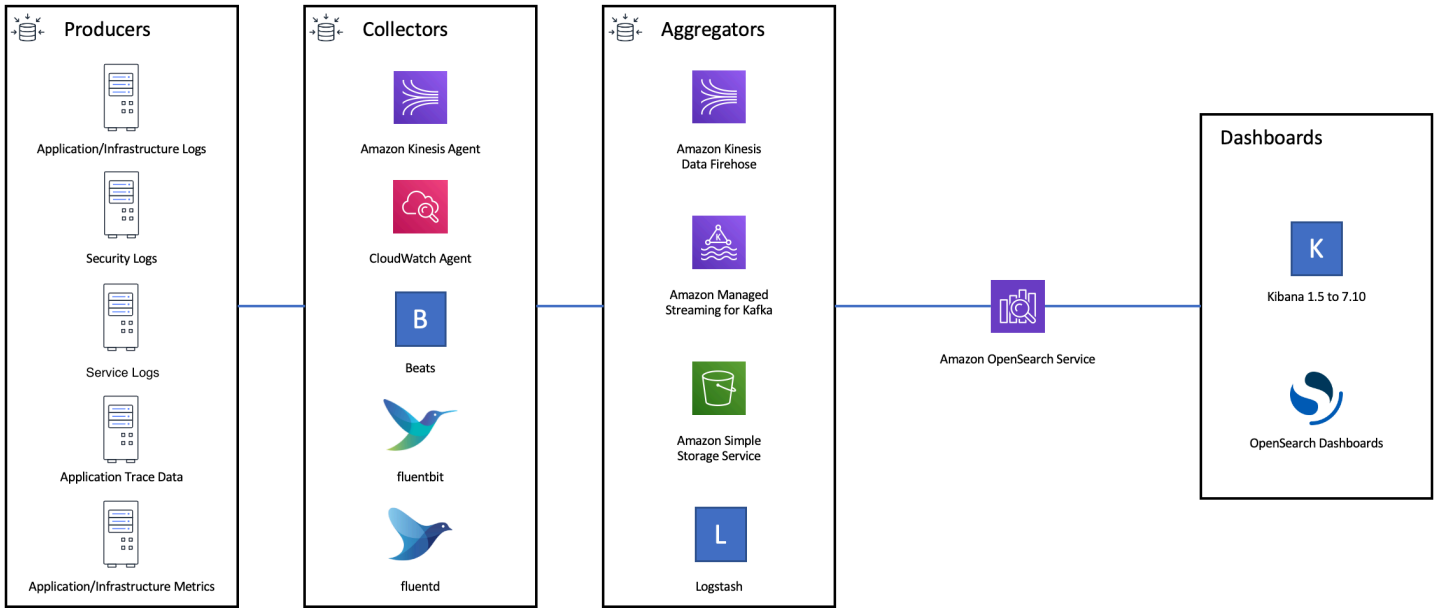
Controle el flujo de incorporación y el almacenamiento en búfer

Recomendamos que se limite el recuento total de solicitudes mediante la operación de la API _bulk. Es más eficiente enviar una solicitud `_bulk` que contiene 5000 documentos que enviar 5000 solicitudes que contienen un solo documento.

Para lograr una estabilidad operativa óptima, a veces es necesario limitar o incluso detener el flujo ascendente de las solicitudes de indexación. Limitar la tasa de solicitudes de índices es un mecanismo importante para hacer frente a picos inesperados u ocasionales en las solicitudes que,

de otro modo, podrían abrumar al clúster. Considere la posibilidad de crear un mecanismo de control de flujo en su arquitectura ascendente.

El siguiente diagrama muestra varias opciones de componentes para una arquitectura de incorporación de registros. Configure la capa de agregación para dejar espacio suficiente para almacenar en búfer los datos entrantes para picos de tráfico repentinos y un breve mantenimiento del dominio.



Cree asignaciones para cargas de trabajo de búsqueda

Para las cargas de trabajo de búsqueda, cree mapeos que definan cómo se OpenSearch almacenan e indexan los documentos y sus campos. Establezca `dynamic` en `strict` para evitar la adición accidental de nuevos campos.

```
PUT my-index
{
  "mappings": {
    "dynamic": "strict",
    "properties": {
      "title": { "type" : "text" },
      "author": { "type" : "integer" },
      "year": { "type" : "text" }
    }
  }
}
```

Utilice plantillas de índice

Puedes usar una plantilla de índice como una forma de indicar OpenSearch cómo configurar un índice cuando se crea. Configure las plantillas de índices antes de crear índices. Luego, cuando crea un índice, hereda la configuración y las asignaciones de la plantilla. Puede aplicar más de una plantilla a un único índice, de manera que pueda especificar la configuración en una plantilla y las asignaciones en otra. Esta estrategia permite una plantilla para configuraciones comunes en varios índices y plantillas separadas para configuraciones y asignaciones más específicas.

Los siguientes parámetros son útiles para configurar en plantillas:

- Número total de particiones primarias y de réplicas
- Intervalo de actualización (frecuencia con la que se actualizan y se realizan cambios recientes en el índice disponibles para la búsqueda)
- Control de mapeo dinámico
- Asignaciones de campo explícito

La siguiente plantilla de ejemplo contiene cada una de estas configuraciones:

```
{
   "index_patterns":[
      "index-*"
   ],
   "order": 0,
   "settings": {
      "index": {
         "number_of_shards": 3,
         "number_of_replicas": 1,
         "refresh_interval": "60s"
      }
   },
   "mappings": {
      "dynamic": false,
      "properties": {
         "field_name1": {
            "type": "keyword"
         }
      }
   }
}
```

Aunque cambien con poca frecuencia, tener la configuración y los mapeos definidos de forma centralizada OpenSearch es más fácil de administrar que actualizar varios clientes anteriores.

Administre los índices con la administración de estado de índice

Si administra registros o datos de serie temporal, le recomendamos que utilice Administración de estados de índice (ISM). ISM le permite automatizar las tareas regulares de administración del ciclo de vida. Con ISM, puede crear políticas que invoquen la renovación de alias de índice, tomen instantáneas de índices, muevan índices entre niveles de almacenamiento y eliminen índices antiguos. Incluso puede usar la operación sustitución de ISM como estrategia alternativa de administración del ciclo de vida de los datos para evitar el sesgo de las particiones.

En primer lugar, establezca una política de ISM. Por ejemplo, consulte the section called “Ejemplos de política”. A continuación, puede adjuntar la política a uno o más índices. Si incluye un campo de plantilla de ISM en la política, OpenSearch Service aplicará automáticamente la política a cualquier índice que coincida con el patrón especificado.

Eliminar los índices que no se utilizan

Revise periódicamente los índices de su clúster e identifique los que no estén en uso. Tome una instantánea de esos índices para que se almacenen en S3 y, a continuación, elimínelos. Cuando se eliminan los índices no utilizados, se reduce el recuento de particiones y se permite una distribución del almacenamiento de información y una utilización de recursos más equilibradas entre los nodos. Incluso cuando están inactivos, los índices consumen algunos recursos durante las actividades de mantenimiento de índices internos.

En lugar de eliminar manualmente los índices no utilizados, puede usar ISM para tomar automáticamente una instantánea y eliminar los índices después de un período de tiempo determinado.

Utilice varios dominios para disfrutar de una alta disponibilidad

Para lograr una alta disponibilidad más allá del 99,9 % de tiempo de actividad en varias regiones, considere la posibilidad de usar dos dominios. Para conjuntos de datos pequeños o que cambian lentamente, puede configurar la replicación entre clústerespara mantener un modelo activo-pasivo. En este modelo, solo se escribe el dominio principal, pero se puede leer cualquiera de los dos dominios. Para conjuntos de datos más grandes y datos que cambian rápidamente, configure la entrega dual en la canalización de incorporación para que todos los datos se escriban de forma independiente en ambos dominios en un modelo activo-activo.

Diseñe sus aplicaciones ascendentes y descendentes teniendo en cuenta la conmutación por error. Asegúrese de probar el proceso de conmutación por error junto con otros procesos de recuperación de desastres.

Rendimiento

Las siguientes prácticas recomendadas se aplican para ajustar sus dominios para lograr un rendimiento óptimo.

Optimice el tamaño y la compresión de solicitudes

El tamaño masivo depende de los datos, el análisis y la configuración del clúster, pero un buen punto de partida es de 3 a 5 MiB por solicitud masiva.

Envíe solicitudes y reciba respuestas de sus OpenSearch dominios mediante la compresión gzip para reducir el tamaño de la carga útil de las solicitudes y respuestas. Puedes usar la compresión gzip con el cliente OpenSearch Python o incluir los siguientes encabezados desde el lado del cliente:

- `'Accept-Encoding': 'gzip'`
- `'Content-Encoding': 'gzip'`

Para optimizar el tamaño de las solicitudes, comience con un tamaño de solicitud de 3 MiB. Luego, aumente lentamente el tamaño de la solicitud hasta que el desempeño de la indexación deje de mejorar.

> **Note**
>
> Para habilitar la compresión gzip en dominios que ejecutan Elasticsearch versión 6.x, debe establecer `http_compression.enabled` a nivel de clúster. Esta configuración se cumple de forma predeterminada en las versiones 7.x de Elasticsearch y en todas las versiones de. OpenSearch

Reduzca el tamaño de las respuestas de solicitudes masivas

Para reducir el tamaño de OpenSearch las respuestas, excluya los campos innecesarios con el parámetro. `filter_path` Asegúrese de no filtrar ningún campo que sea necesario para identificar

o reintentar las solicitudes fallidas. Para obtener más información y ejemplos, consulte the section called “Reducción del tamaño de la respuesta”.

Ajuste intervalos de actualización

OpenSearch los índices tienen una coherencia de lectura eventual. Una operación de actualización hace que todas las actualizaciones que se realizan en un índice estén disponibles para la búsqueda. El intervalo de actualización predeterminado es de un segundo, lo que OpenSearch significa que se actualiza cada segundo mientras se escribe en un índice.

Cuando menos frecuente sea la actualización de un índice (mayor intervalo de actualización), mejor será el rendimiento general de la indexación. La desventaja de aumentar el intervalo de actualización es que hay un retraso mayor entre la actualización del índice y el momento en que los nuevos datos están disponibles para la búsqueda. Establezca el intervalo de actualización tan alto como pueda tolerar para mejorar el rendimiento general.

Recomendamos configurar el parámetro `refresh_interval` para todos los índices a 30 segundos o más.

Habilite el ajuste automático

Auto-Tune utiliza las métricas de rendimiento y uso del OpenSearch clúster para sugerir cambios en el tamaño de las colas, el tamaño de la caché y la configuración de la máquina virtual Java (JVM) en los nodos. Estos cambios opcionales mejoran la velocidad y la estabilidad del clúster. Puede volver a la configuración de OpenSearch servicio predeterminada en cualquier momento. La función de ajuste automático está habilitada de forma predeterminada en nuevos dominios, a menos que la desactive explícitamente.

Recomendamos que se habilite el ajuste automático en todos los dominios y se establezca un período de mantenimiento periódico o se revisen periódicamente sus recomendaciones.

Seguridad

Las siguientes prácticas recomendadas se aplican a la protección de sus dominios.

Cómo habilitar el control de acceso detallado

El control de acceso detallado le permite controlar quién puede acceder a determinados datos dentro de un dominio del Servicio. OpenSearch En comparación con el control de acceso generalizado, el control de acceso detallado proporciona a cada clúster, índice, documento y campo su propia política

de acceso especificada. Los criterios de acceso pueden basarse en una serie de factores, incluido el rol de la persona quien solicita el acceso y la acción que pretende realizar con los datos. Por ejemplo, puede dar a un usuario acceso para escribir en un índice, y a otra se le puede dar acceso solo para leer los datos del índice sin realizar cambios.

El control de acceso detallado permite que los datos con diferentes requisitos de acceso existan en el mismo espacio de almacenamiento sin tener problemas de seguridad o cumplimiento.

Se recomienda habilitar un control de acceso detallado para sus dominios.

Implemente dominios dentro de una VPC

Colocar su dominio de OpenSearch servicio en una nube privada virtual (VPC) permite una comunicación segura entre el OpenSearch Servicio y otros servicios dentro de la VPC, sin necesidad de una puerta de enlace a Internet, un dispositivo NAT o una conexión VPN. Todo el tráfico permanece seguro dentro de la nube. AWS Debido a su aislamiento lógico, los dominios que residen dentro de una VPC tienen una capa adicional de seguridad en comparación con los dominios que utilizan puntos de conexión públicos.

Le recomendamos que utilice crear sus dominios dentro de una VPC.

Aplique una política de acceso restrictivo

Incluso si su dominio se implementa dentro de una VPC, es una práctica recomendada la implementación de la seguridad en capas. Asegúrese de comprobar la configuración de sus políticas de acceso actuales.

Aplica a tus dominios una política de acceso restrictiva basada en los recursos y sigue el principio de privilegios mínimos al conceder acceso a la API de configuración y a las operaciones de la OpenSearch API. Como regla general, evite usar la entidad principal de usuario anónimo `"Principal": {"AWS": "*" }` en sus políticas de acceso.

Sin embargo, hay algunas situaciones en las que es aceptable usar una política de acceso abierto, como cuando se habilita un control de acceso detallado. Una política de acceso abierto puede permitirle acceder al dominio en los casos en que la firma de solicitudes sea difícil o imposible, por ejemplo, desde ciertos clientes y herramientas.

Habilite el cifrado en reposo

OpenSearch Los dominios de servicio ofrecen el cifrado de los datos en reposo para evitar el acceso no autorizado a los datos. El cifrado en reposo utiliza AWS Key Management Service (AWS KMS)

para almacenar y administrar las claves de cifrado, y el algoritmo estándar de cifrado avanzado con claves de 256 bits (AES-256) para realizar el cifrado.

Si el dominio almacena información confidencial, habilite el cifrado de datos en reposo.

Habilita el cifrado node-to-node

El ode-to-node cifrado N proporciona un nivel de seguridad adicional además de las funciones de seguridad predeterminadas del OpenSearch Servicio. Implementa la seguridad de la capa de transporte (TLS) para todas las comunicaciones entre los nodos que están aprovisionados. OpenSearch Sin ode-to-node cifrado, todos los datos enviados a su dominio de OpenSearch servicio a través de HTTPS permanecen cifrados en tránsito mientras se distribuyen y replican entre los nodos.

Si tu dominio almacena datos confidenciales, habilita el node-to-node cifrado.

Supervisa con AWS Security Hub

Supervise su uso del OpenSearch Servicio en relación con las mejores prácticas de seguridad mediante el uso de AWS Security Hub. Security Hub utiliza controles de seguridad para evaluar las configuraciones de los recursos y los estándares de seguridad para ayudarle a cumplir varios marcos de conformidad. Para obtener más información sobre el uso de Security Hub para evaluar los recursos del OpenSearch servicio, consulte Amazon OpenSearch Service los controles en la Guía delAWS Security Hub usuario.

Optimización de costos

Las siguientes prácticas recomendadas se aplican a la optimización y el ahorro de los costes OpenSearch del servicio.

Use los tipos de instancia de última generación

OpenSearch El servicio siempre adopta nuevos tipos de instancias de Amazon EC2 que ofrecen un mejor rendimiento a un coste menor. Recomendamos usar siempre las instancias de última generación.

Evite usar instancias T2 o `t3.small` para dominios de producción, ya que pueden volverse inestables bajo una carga pesada sostenida. Las instancias `t3.medium` son una opción para cargas de trabajo de producción pequeñas (tanto como nodos de datos, como nodos maestros dedicados).

Use los volúmenes gp3 de Amazon EBS más recientes

OpenSearch los nodos de datos requieren un almacenamiento de baja latencia y alto rendimiento para proporcionar una indexación y consultas rápidas. Utilizando volúmenes gp3 de Amazon EBS, se obtiene un mayor rendimiento de referencia (IOPS y rendimiento) a un costo un 9,6 % inferior que con el tipo de volumen gp2 de Amazon EBS que se ofrecía anteriormente. Puede aprovisionar IOPS y rendimiento adicionales independientemente del tamaño de los volúmenes mediante gp3. Además, estos volúmenes son más estables que los de la generación anterior, ya que no utilizan créditos de ráfaga. El tipo de volumen gp3 también duplica los límites de tamaño de per-data-node volumen del tipo de volumen gp2. Con estos volúmenes de mayor tamaño, puede reducir el costo de los datos pasivos mediante el incremento de la cantidad de almacenamiento por nodo de datos.

Utilice UltraWarm y almacene en frío los datos de registro de series temporales

Si lo utiliza OpenSearch para el análisis de registros, traslade sus datos a un UltraWarm almacenamiento en frío para reducir los costes. Utilice la Administración de estado de índices (ISM) para migrar datos entre niveles de almacenamiento y administrar la retención de datos.

UltraWarmproporciona una forma rentable de almacenar grandes cantidades de datos de solo lectura en OpenSearch Service. UltraWarm utiliza Amazon S3 para el almacenamiento, lo que significa que los datos son inmutables y solo se necesita una copia. Solo paga por un almacenamiento que es equivalente al tamaño de las particiones principales de sus índices. Las latencias de las UltraWarm consultas aumentan con la cantidad de datos de S3 que se necesitan para atender la consulta. Una vez que los datos se han almacenado en caché en los nodos, las consultas a los UltraWarm índices tienen un rendimiento similar al de las consultas a los índices activos.

El almacenamiento en frío también cuenta con el respaldo de S3. Cuando necesite consultar datos inactivos, puede adjuntarlos de forma selectiva a los nodos existentes. UltraWarm Los datos inactivos incurren en el mismo coste de almacenamiento gestionado que los objetos almacenados en frío UltraWarm, pero los objetos almacenados en frío no consumen recursos de los UltraWarm nodos. Por lo tanto, el almacenamiento en frío proporciona una cantidad significativa de capacidad de almacenamiento sin afectar al tamaño o al recuento de los UltraWarm nodos.

UltraWarm se vuelve rentable cuando tiene que migrar aproximadamente 2,5 TiB de datos desde un almacenamiento activo. Supervise su tasa de llenado y planifique trasladar los índices a ellos UltraWarm antes de alcanzar ese volumen de datos.

Revise las recomendaciones para instancias reservadas

Considere comprar instancias reservadas (RI) después de contar con una buena referencia sobre el rendimiento y el consumo de cómputos. Los descuentos comienzan en torno al 30 % para reservas sin pago anticipado de 1 año y pueden aumentar hasta un 50 % para todos los compromisos de pagos iniciales de 3 años.

Después de que observe un funcionamiento estable durante al menos 14 días, revise las Recomendaciones de instancias reservadas en el Explorador de costos. El encabezado Amazon OpenSearch Service muestra recomendaciones de compra específicas de RI y ahorros proyectados.

Dimensionamiento de los dominios de Amazon OpenSearch Service

No existe un método perfecto para dimensionar los dominios de Amazon OpenSearch Service. Sin embargo, si comienza por comprender sus necesidades de almacenamiento, el servicio y OpenSearch en sí mismo, puede realizar una estimación inicial fundamentada de sus necesidades de hardware. Este cálculo puede servir como un buen punto de partida para la mayoría de los aspectos esenciales de la determinación del tamaño de los dominios: probarlos con cargas de trabajo representativas y monitorear su rendimiento.

Temas

Cálculo de requisitos de almacenamiento

La mayoría OpenSearch de las cargas de trabajo se clasifican en una de estas dos amplias categorías:

- Índice de larga duración: se escribe código que procesa los datos en uno o más OpenSearch índices y, a continuación, se actualizan esos índices periódicamente a medida que cambian los datos de origen. Algunos ejemplos comunes son las búsquedas en sitios Web, documentos y comercio electrónico.

- Índices continuos: los datos fluyen de manera continua en un conjunto de índices temporales, con un periodo de indexación y de retención (como un conjunto de índices diarios que se conservan durante dos semanas). Algunos ejemplos comunes son el análisis de registros, el procesamiento de series temporales y el análisis de secuencias de clics.

Para las cargas de trabajo de índices de larga duración, puede examinar el origen de datos en disco y determinar fácilmente la cantidad de espacio de almacenamiento que consumen. Si los datos provienen de varias fuentes, solo tiene que agregar esas fuentes juntas.

Para los índices continuos, puede multiplicar la cantidad de datos generados durante un periodo de tiempo representativo por el periodo de retención. Por ejemplo, si genera 200 MiB de datos de registro por hora, o sea 4,7 GiB por día, eso significa que contará con un total de 66 GiB de datos en un momento dado si hubo un periodo de retención de dos semanas.

Sin embargo, el tamaño de los datos de origen es solo uno de los aspectos de las necesidades de almacenamiento. También debe considerar lo siguiente:

- Número de réplicas: cada réplica es una copia completa de un índice y necesita la misma cantidad de espacio en disco. De forma predeterminada, cada OpenSearch índice tiene una réplica. Recomendamos tener al menos una para evitar la pérdida de datos. Las réplicas también mejoran el rendimiento, por lo que tal vez convenga tener más si tiene una carga de trabajo que realiza muchas operaciones de lectura. Utilice `PUT /my-index/_settings` para actualizar la configuración `number_of_replicas` para su índice.
- OpenSearch sobrecarga de indexación: el tamaño en disco de un índice varía. El tamaño total de los datos de origen más el índice suele ser del 110 % del origen, y el índice de hasta el 10 % de los datos de origen. Después de indexar los datos, puede utilizar la API `_cat/indices?v` y el valor de `pri.store.size` para calcular la sobrecarga exacta. `_cat/allocation?v` también proporciona un resumen útil.
- Espacio reservado por el sistema operativo: de forma predeterminada, Linux reserva el 5 % del sistema de archivos para el usuario `root` para procesos críticos, recuperación del sistema y como medida de seguridad frente a problemas de fragmentación del disco.
- OpenSearch Sobrecarga del OpenSearch servicio: el servicio reserva el 20% del espacio de almacenamiento de cada instancia (hasta 20 GiB) para fusiones de segmentos, registros y otras operaciones internas.

  Debido a este máximo de 20 GiB, la cantidad total de espacio reservado puede variar drásticamente en función del número de instancias del dominio. Por ejemplo, un dominio

podría tener tres instancias `m6g.xlarge.search`, cada una con 500 GiB de espacio de almacenamiento, lo que equivaldría a un total de 1,46 TiB. En este caso, el espacio reservado total solo es de 60 GiB. Otro dominio podría tener 10 instancias `m3.medium.search`, cada una con 100 GiB de espacio de almacenamiento, lo que equivaldría a un total de 0,98 TiB. Aquí, el espacio reservado total es de 200 GiB, aunque el primer dominio sea un 50 % mayor.

En la siguiente fórmula, aplicamos una estimación “en el peor de los casos” de los gastos generales. Este cálculo incluye espacio libre adicional para ayudar a minimizar el impacto de los errores de nodo y las interrupciones en la zona de disponibilidad.

En resumen, si tiene 66 GiB de datos en un momento dado y quiere una réplica, el requisito de almacenamiento mínimo será aproximadamente 66 * 2 * 1,1 / 0,95 / 0,8 = 191 GiB. Se podría generalizar este cálculo de la manera siguiente:

Datos de origen * (1 más cantidad de réplicas) * (1 más sobrecarga de indexación)/(1: espacio reservado de Linux)/(1: sobrecarga de OpenSearch servicio) = requisito mínimo de almacenamiento

O puede utilizar esta versión simplificada:

Datos de origen * (1 + número de réplicas) * 1,45 = requisito mínimo de almacenamiento

La falta de espacio de almacenamiento suficiente es una de las causas más comunes de la inestabilidad del clúster. Por lo tanto, debe verificar los números cuando elige tipos de instancia, recuentos de instancias y volúmenes de almacenamiento.

Existen otras consideraciones respecto al almacenamiento:

- Si el requisito mínimo de almacenamiento es superior a 1 PB, consulte the section called “Escala de petabytes”.
- Si tiene índices continuos y desea usar una arquitectura caliente/templada, consulte the section called “UltraWarm almacenamiento”.

Selección del número de particiones

Una vez que conozca los requisitos de almacenamiento, puede investigar la estrategia de indexación. De forma predeterminada, en OpenSearch Service, cada índice se divide en cinco fragmentos principales y una réplica (10 fragmentos en total). Este comportamiento es diferente al del código abierto OpenSearch, que de forma predeterminada es un fragmento principal y uno de

réplica. Como no se puede cambiar fácilmente el número de particiones principales de un índice existente, debe decidir el número de particiones antes de indexar el primer documento.

El objetivo general de la selección de un número de particiones es distribuir un índice de manera uniforme entre todos los nodos de datos del clúster. Sin embargo, estas particiones no deberían ser demasiado grandes ni demasiado numerosas. Una pauta general es tratar de mantener el tamaño de la partición entre 10 y 30 GiB para las cargas de trabajo en las que la latencia de búsqueda es un objetivo de rendimiento clave y entre 30 y 50 GiB para las cargas de trabajo con mucha escritura, como el análisis de registros.

Los fragmentos grandes pueden dificultar la recuperación en caso de un error, pero dado que cada fragmento utiliza cierta cantidad de CPU y memoria, tener demasiados fragmentos pequeños puede provocar problemas de rendimiento y errores de memoria insuficiente. OpenSearch En otras palabras, los fragmentos deben ser lo suficientemente pequeños como para que la instancia de OpenSearch servicio subyacente pueda gestionarlos, pero no tan pequeños como para que supongan una carga innecesaria para el hardware.

Por ejemplo, supongamos que tiene 66 GiB de datos. No espera que el número aumente a lo largo del tiempo y desea mantener las particiones en torno a los 30 GiB cada una. El número de particiones debería ser, por tanto, aproximadamente 66 * 1,1/30 = 3. Se podría generalizar este cálculo de la manera siguiente:

(Datos de origen + espacio para crecer) * (1 + sobrecarga de indexación) / tamaño de partición deseado = número aproximado de particiones principales

Esta ecuación ayuda a compensar el aumento de los datos a lo largo del tiempo. Si prevé que estos mismos 66 GiB de datos se cuadrupliquen a lo largo del próximo año, el número aproximado de particiones es (66 + 198) * 1,1/30 = 10. Recuerde, sin embargo, que aún no tiene esos 198 GiB de datos adicionales. Asegúrese de que estos preparativos para el futuro no creen particiones innecesariamente diminutas que consuman grandes cantidades de CPU y memoria en la actualidad. En este caso, tendrá 66 * 1,1/10 particiones = 7,26 GiB por partición, lo que consumirá recursos adicionales y queda debajo del intervalo de tamaño recomendado. Podrías considerar el middle-of-the-road enfoque más amplio de seis fragmentos, lo que te deja con fragmentos de 12 GiB en la actualidad y fragmentos de 48 GiB en el futuro. De nuevo, es posible que prefiera empezar con tres particiones y reindexar sus datos cuando las particiones superen los 50 GiB.

Un problema mucho menos común implica limitar el número de particiones por nodo. Si el tamaño de las particiones es adecuado, normalmente se queda sin espacio en disco mucho antes de alcanzar este límite. Por ejemplo, una instancia de `m6g.large.search` tiene un tamaño

máximo de disco de 512 GiB. Si permanece por debajo del 80 % de uso del disco y el tamaño de sus particiones en 20 GiB, puede acomodar aproximadamente 20 particiones. Elasticsearch 7. x y versiones posteriores, y todas las versiones de OpenSearch, tienen un límite de 1000 fragmentos por nodo. Para ajustar el máximo de particiones por nodo, establezca la configuración `cluster.max_shards_per_node`. Para ver un ejemplo, consulte Configuración del clúster.

El dimensionamiento apropiado de las particiones casi siempre lo mantiene por debajo de este límite, pero también puede considerar el número de particiones por cada GiB del montón de Java. En un nodo dado, no tenga más de 25 particiones por cada GiB del montón de Java. Por ejemplo, una instancia de `m5.large.search` tiene un montón de 4 GiB, por lo que cada nodo no debe tener más de 100 particiones. En ese recuento de particiones, cada uno tiene aproximadamente 5 GiB de tamaño, lo que está muy por debajo de nuestra recomendación.

Selección de tipos de instancias y pruebas

Después de calcular sus requisitos de almacenamiento y elegir el número de particiones que necesita, puede comenzar a tomar decisiones sobre el equipo. Los requisitos del equipo varían enormemente en función de la carga de trabajo, pero aquí también ofrecemos algunas recomendaciones básicas.

En general, los límites de almacenamiento para cada tipo de instancia se corresponden con la cantidad de CPU y memoria que podría necesitar para las cargas de trabajo. Por ejemplo, una instancia `m6g.large.search` tiene un tamaño de volumen de EBS máximo de 512 GiB, 2 núcleos de vCPU y 8 GiB de memoria. Si el clúster tiene muchas particiones, realiza un gran número de altas, actualiza documentos frecuentemente o procesa un gran número de consultas, esos recursos podrían ser insuficientes para sus necesidades. Si su clúster entra dentro de una de estas categorías, empiece con una configuración más cercana a 2 núcleos de vCPU y 8 GiB de memoria para cada 100 GiB de su requisito de almacenamiento.

> **Tip**
>
> Para ver un resumen de los recursos de hardware que se asignan a cada tipo de instancia, consulta los precios OpenSearch de Amazon Service.

Aun así, estos recursos podrían ser insuficientes. Algunos OpenSearch usuarios afirman que necesitan muchas veces esos recursos para cumplir sus requisitos. Para encontrar el equipo correcto para la carga de trabajo, debe realizar una estimación inicial fundamentada, probarla con cargas de trabajo representativas, ajustarla y probarla de nuevo.

Paso 1: realizar una estimación inicial

Para empezar, recomendamos un mínimo de tres nodos para evitar posibles OpenSearch problemas, como un estado cerebral dividido (cuando un fallo en la comunicación provoca que un clúster tenga dos nodos maestros). Aunque tenga tres nodos maestros dedicados, seguiremos recomendando que tenga un mínimo de dos nodos de datos para la reproducción.

Paso 2: calcular los requisitos de almacenamiento por nodo

Si tuviera un requisito de almacenamiento de 184 GiB y el número mínimo recomendado de tres nodos, usaría la ecuación 184 / 3 = 61 GiB para encontrar la cantidad de almacenamiento que necesita cada nodo. En este ejemplo, podría elegir tres instancias `m6g.large.search`, donde cada una con un volumen de almacenamiento de EBS de 90 GiB para no quedarse corto y tener un margen de crecimiento para el futuro. Esta configuración proporciona 6 núcleos de vCPU y 24 GiB de memoria, por lo que resulta adecuada para las cargas de trabajo más ligeras.

Para ver un ejemplo más sustancial, considere un requisito de almacenamiento de 14 TiB (14 336 GiB) y una carga de trabajo pesada. En este caso, podría decidir empezar con 2 * 144 = 288 núcleos de vCPU y 8 * 144 = 1 152 GiB de memoria. Estos números se corresponden con aproximadamente 18 instancias `i3.4xlarge.search`. Si no necesita el almacenamiento local rápido, también puede probar con 18 instancias `r6g.4xlarge.search`, cada una con un volumen de almacenamiento de EBS de 1 TiB.

Si el clúster incluye cientos de terabytes de datos, consulte the section called “Escala de petabytes”.

Paso 3: realizar pruebas representativas

Tras configurar el clúster, puede añadir los índices utilizando el número de fragmentos que calculó anteriormente, realizar algunas pruebas representativas con los clientes utilizando un conjunto de datos realista y supervisar CloudWatch las métricas para ver cómo gestiona el clúster la carga de trabajo.

Paso 4: suceder o iterar

Si el rendimiento satisface sus necesidades, las pruebas se realizan correctamente y CloudWatch las métricas son normales, el clúster está listo para usarse. Recuerde configurar CloudWatch alarmas para detectar un uso deficiente de los recursos.

Si el desempeño no es aceptable, no se superan las pruebas o los valores de `CPUUtilization` o `JVMMemoryPressure` son altos, es posible que tenga que elegir un tipo de instancia diferente

(o agregar instancias) y continuar con las pruebas. A medida que agrega instancias, reequilibra OpenSearch automáticamente la distribución de los fragmentos en todo el clúster.

Debido a que es más fácil medir el exceso de capacidad en un clúster sobrealimentado que el déficit en uno infraalimentado, recomendamos comenzar con un clúster más grande de lo que crea necesario. A continuación, debe realizar pruebas y reducir verticalmente el tamaño hasta tener un clúster eficiente con los recursos adicionales precisos para garantizar operaciones estables durante los períodos de mayor actividad.

Los clústeres en producción o los clústeres con estados complejos se benefician de los nodos maestros dedicados, que mejoran el desempeño y la fiabilidad del clúster.

Escala de petabytes en Amazon Service OpenSearch

Los dominios OpenSearch de Amazon Service ofrecen almacenamiento adjunto de hasta 3 PB. Puede configurar un dominio con 200 tipos de instancias `i3.16xlarge.search`, cada una con 15 TB de almacenamiento. Debido a la gran diferencia de escala, las recomendaciones para los dominios de este tamaño difieren de nuestras recomendaciones generales. En esta sección, se explican consideraciones sobre la creación de dominios, los costos, el almacenamiento y el tamaño de las particiones.

Aunque esta sección hace referencia con frecuencia a los tipos de instancias `i3.16xlarge.search`, puede usar otros tipos de instancias para llegar a 1 PB de almacenamiento total del dominio.

Creación de dominios

Los dominios de este tamaño superan el límite predeterminado de 80 instancias por dominio. Para solicitar un aumento del límite del servicio de hasta 200 instancias por dominio, abra un caso en el Centro de asistencia deAWS.

Precios

Antes de crear un dominio de este tamaño, consulta la página de precios de Amazon OpenSearch Service para asegurarte de que los costes asociados se ajustan a tus expectativas. Examine the section called “UltraWarm almacenamiento” para ver si una arquitectura caliente/templada se ajusta a su caso de uso.

Almacenamiento

Los tipos de instancias `i3` se han diseñado para proporcionar almacenamiento rápido, local y de memoria no volátil (NVMe). Dado que este almacenamiento local suele ofrecer ventajas de rendimiento en comparación con Amazon Elastic Block Store, los volúmenes de EBS no son una opción cuando se seleccionan estos tipos de instancias en OpenSearch Service. Si prefiere el almacenamiento de EBS, utilice otro tipo de instancia, como `r6.12xlarge.search`.

Tamaño y número de fragmentos

Una OpenSearch pauta habitual es no superar los 50 GB por partición. Habida cuenta del número de fragmentos necesarios para acomodar dominios grandes y los recursos disponibles para instancias `i3.16xlarge.search`, le recomendamos un tamaño de fragmento de 100 GB.

Por ejemplo, si tiene 450 TB de datos de origen y solo quiere una réplica, su requisito de almacenamiento mínimo será aproximadamente 450 TB * 2 * 1,1/0.95 = 1.04 PB. Para obtener una explicación de este cálculo, consulte the section called “Cálculo de requisitos de almacenamiento”. Aunque 1,04 PB / 15 TB = 70 instancias, podría seleccionar 90 o más instancias `i3.16xlarge.search` para disponer de una red de seguridad de almacenamiento, hacer frente a los errores de los nodos y tener en cuenta cierta variación en la cantidad de datos a lo largo del tiempo. Cada instancia añade otros 20 GiB a su requisito de almacenamiento mínimo, pero para discos de este tamaño, esos 20 GiB son casi insignificantes.

Controlar el número de fragmentos es complicado. OpenSearch los usuarios suelen rotar los índices a diario y conservar los datos durante una o dos semanas. En esta situación, puede que le resulte útil distinguir entre fragmentos "activos" e "inactivos". Los fragmentos activos son fragmentos que se están escribiendo o leyendo activamente. Las particiones inactivas pueden dar servicio a algunas solicitudes de lectura, pero están en gran medida inactivos. En general, debe mantener el número de fragmentos activos por debajo de varios miles. Cuando el número de fragmentos activos se acerca a los 10 000, surgen riesgos importantes de desempeño y estabilidad.

Para calcular el número de fragmentos principales, utilice esta fórmula: 450 000 GB * 1,1 / 100 GB por fragmento = 4 950 fragmentos. Si se duplica ese número para dar cuenta de las réplicas se obtienen 9 900 particiones, lo que supone un grave problema si todas las particiones están activas. Pero si rota los índices y solo una séptima parte o una catorceava parte de las particiones están activas en un día determinado (1,414 o 707 particiones, respectivamente), el clúster puede funcionar correctamente. Como siempre, el paso más importante para determinar el tamaño y la configuración del dominio es realizar pruebas representativas en el cliente utilizando un conjunto de datos realista.

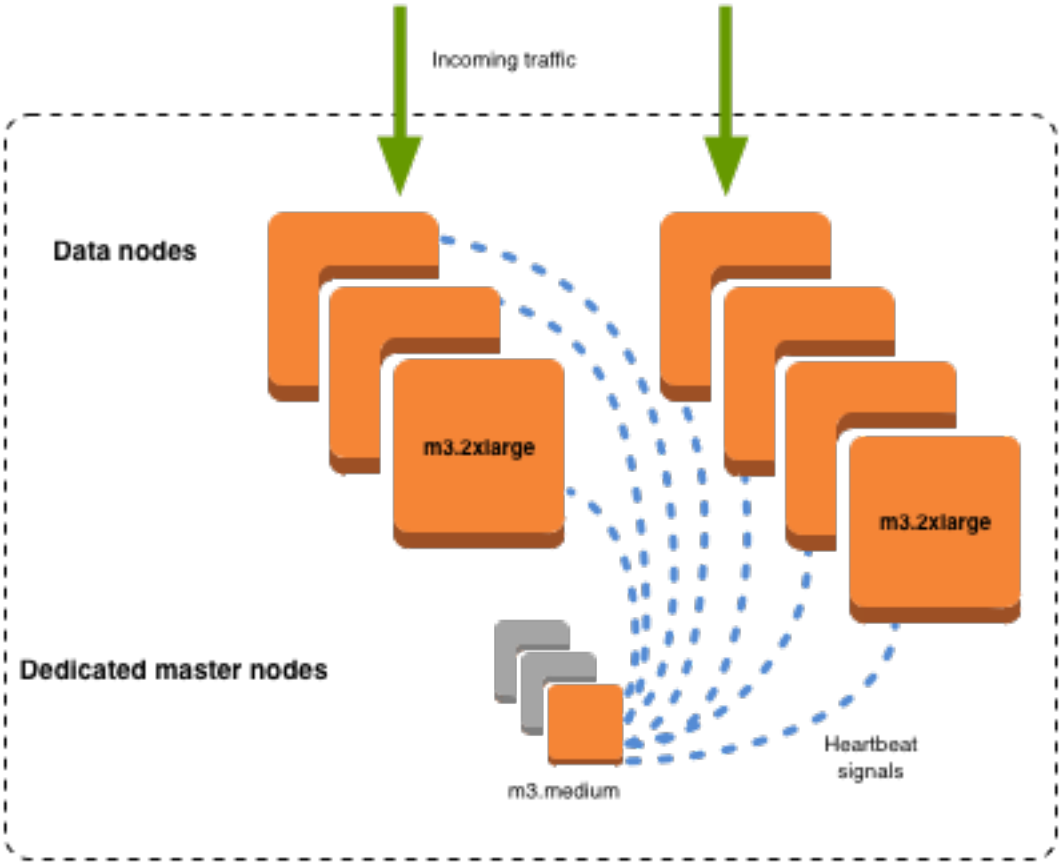
Nodos maestros dedicados en Amazon OpenSearch Service

Amazon OpenSearch Service utiliza nodos maestros dedicados para aumentar la estabilidad del clúster. Un nodo maestro dedicado realiza tareas de administración de clústeres, pero que no contiene datos ni responde a las solicitudes de carga de datos. Al asumir de este modo las tareas de administración del clúster, aumenta la estabilidad del dominio. Al igual que todos los demás tipos de nodos, se paga una tarifa por hora por cada nodo maestro dedicado.

Los nodos maestros dedicados se encargan de realizar las siguientes tareas de administración del clúster:

- Seguimiento de todos los nodos del clúster.
- Seguimiento del número de índices del clúster.
- Seguimiento del número de particiones que pertenecen a cada índice.
- Mantenimiento de la información de enrutamiento para los nodos del clúster.
- Actualización del estado del clúster después de los cambios, como la creación de un índice o la adición o eliminación de nodos en el clúster.
- Reproducción de los cambios de estado del clúster en todos los nodos que lo componen.
- Monitorización del estado de todos los nodos del clúster, mediante el envío de señales de latido, señales periódicas que monitorizan la disponibilidad de los nodos de datos del clúster.

La siguiente ilustración muestra un dominio OpenSearch de servicio con 10 instancias. Siete de ellas son nodos de datos y tres son nodos maestros dedicados. Solo uno de los nodos maestros dedicados está activo. Los dos nodos maestros dedicados grises están en reserva a la espera por si el nodo maestro dedicado activo sufre algún error. Los siete nodos de datos se encargan de atender todas las solicitudes de carga de datos, mientras que el nodo maestro dedicado activo asume las tareas de administración del clúster.



Elección del número de nodos maestros dedicados

Se recomienda utilizar Multi-AZ con modo de espera, que añade tres nodos maestros dedicados a cada dominio de OpenSearch servicio de producción. Si realiza la implementación con Multi-AZ sin modo de espera o con Single-AZ, igual le recomendamos tres nodos maestros dedicados. No elija nunca un número par de nodos maestros dedicados. Tenga en cuenta lo siguiente al elegir el número de nodos maestros dedicados:

- El OpenSearch Servicio prohíbe explícitamente tener un nodo principal dedicado, ya que no se dispone de una copia de seguridad en caso de que se produzca un error. Recibirá una excepción de validación si intenta crear un dominio con un solo nodo maestro dedicado.
- Si tiene dos nodos maestros dedicados, el clúster no tiene el quórum de nodos necesario para elegir un nuevo nodo maestro si se produce algún error.

  El quórum se calcula como el número de nodos maestros dedicados / 2 + 1 (redondeado al número entero más próximo). En este caso, 2 / 2 + 1 = 2. Como un nodo maestro dedicado produjo

un error y solo existe una copia de seguridad, el clúster no tiene quórum y no puede elegir un nuevo nodo principal.

- El uso de tres nodos maestros dedicados, el número recomendado, ofrece dos nodos de backup en caso de que se produzca un error en un nodo maestro y el quórum necesario (2) para elegir un nuevo nodo maestro.
- No es mejor utilizar cuatro nodos maestros dedicados en lugar de tres y se pueden ocasionar problemas si se utilizan múltiples zonas de disponibilidad.
  - Si un nodo maestro produce un error, tiene quórum (3) para elegir un nuevo nodo. Si dos nodos producen un error, pierde ese quórum, de la misma forma que con tres nodos maestros dedicados.
  - En una configuración de tres zonas de disponibilidad, dos AZ tienen un nodo maestro dedicado y una AZ tiene dos. Si esa AZ experimenta alguna interrupción, las dos AZ restantes no tienen quórum necesario (3) para elegir un nuevo maestro.
- Contar con cinco nodos maestros dedicados funciona igual de bien que tres y permite mantener el quórum aunque pierda dos nodos. Sin embargo, dado que solo hay un nodo maestro dedicado activo en cada momento dado, esta configuración supone que usted paga por cuatro nodos inactivos. Muchos clientes consideran excesivo este nivel de protección de conmutación por error.

Si un clúster tiene un número par de nodos aptos para ser maestros OpenSearch y las versiones 7 de Elasticsearch. x y posteriores ignoran un nodo para que la configuración de votación sea siempre un número impar. En este caso, cuatro nodos maestros dedicados equivalen en esencia a tres (y dos, a uno).

> **Note**
>
> Si el clúster no tiene el quórum necesario para elegir un nuevo nodo maestro, se produce un error en las solicitudes de lectura y de escritura en el clúster. Este comportamiento es diferente del OpenSearch predeterminado.

Elección de tipos de instancias para nodos principales dedicados

Si bien los nodos maestros dedicados no procesan solicitudes de búsqueda ni de consulta, su tamaño es proporcional al tamaño y el número de instancias, índices y particiones que son capaces de administrar. En el caso de los clústeres de producción, recomendamos como mínimo asignar los siguientes tipos de instancias para los nodos maestros dedicados.

Estas recomendaciones se basan en las cargas de trabajo habituales, pero pueden variar en función de sus necesidades. En los clústeres con muchas particiones o asignaciones de campo, puede resultar conveniente utilizar tipos de instancias más grandes. Monitoree las métricas de los nodos maestros dedicados para determinar si necesita un tipo de instancia mayor.

Recuento de instancias	Tamaño de RAM de nodo maestro	Número máximo de particiones admitidas	Tipo de instancia maestra dedicada mínima recomendada
De 1 a 10	8 GiB	10 000	`m5.large.search` o `m6g.large.search`
De 11 000 a 30 000	16 GiB	30 000	`c5.2xlarge.search` o `c6g.2xlarge.search`
De 31 000 a 75 000	32 GiB	40 000	`r5.xlarge.search` o `r6g.xlarge.search`
De 76 000 a 125 000	64 GiB	75 000	`r5.2xlarge.search` o `r6g.2xlarge.search`
De 126 000 a 200 000	128 GiB	75 000	`r5.4xlarge.search` o `r6g.4xlarge.search`

- Para obtener información sobre cómo determinados cambios de configuración pueden afectar a los nodos maestros dedicados, consulte the section called “Cambios de configuración”.
- Para obtener más información sobre los límites del número de instancias, consulte Cuotas de instancias y dominios de OpenSearch servicio.

- Para obtener más información sobre tipos de instancias específicos, como la vCPU, la memoria y los precios, consulta los precios de Amazon OpenSearch Service.

CloudWatch Alarmas recomendadas para Amazon OpenSearch Service

CloudWatch las alarmas realizan una acción cuando una CloudWatch métrica supera un valor especificado durante un período de tiempo determinado. Por ejemplo, es posible que AWS desee enviarle un correo electrónico si el estado del clúster es `red` superior a un minuto. En esta sección se incluyen algunas alarmas recomendadas para Amazon OpenSearch Service y cómo responder a ellas.

Puede implementar estas alarmas automáticamente mediante AWS CloudFormation. Para ver una pila de muestras, consulta el GitHubrepositorio relacionado.

> **Note**
>
> Si despliegas la CloudFormation pila, las `KMSKeyInaccessible` alarmas `KMSKeyError` y permanecerán en un `Insufficient Data` estado dado que estas métricas solo aparecen si un dominio encuentra un problema con su clave de cifrado.

Para obtener más información sobre la configuración de alarmas, consulte Creación de CloudWatch alarmas de Amazon en la Guía del CloudWatch usuario de Amazon.

Alarma	Problema
El valor máximo de `ClusterStatus.red` es >= 1 durante 1 minuto, 1 periodo consecutivo	Al menos una partición principal y sus réplicas no están asignados a un nodo. Consulte the section called “Estado rojo del clúster”.
El valor máximo de `ClusterStatus.yellow` es >= 1 durante 1 minuto,	Al menos una partición de réplica no está asignada a un nodo. Consulte the section called “Estado amarillo del clúster”.

Alarma	Problema
5 periodos consecutivos	
El valor mínimo de `FreeStorageSpace` es <= 20 480 durante 1 minuto, 1 periodo consecutivo	El espacio de almacenamiento disponible de un nodo en su clúster se redujo hasta los 20 GiB. Consulte the section called “Falta de espacio de almacenamiento disponible”. Este valor está en MiB, por lo que, en lugar de 20 480, recomendamos que lo configure en un 25 % del espacio de almacenamiento de cada nodo.
El valor de `ClusterIndexWritesBlocked` es >= 1 durante 5 minutos, 1 periodo consecutivo	El clúster bloquea las solicitudes de escritura. Consulte the section called “ClusterBlockException”.
El valor mínimo de `Nodes` es < x 1 día, 1 periodo consecutivo	x es el número de nodos del clúster. Esta alarma indica que al menos un nodo del clúster se mantuvo inaccesible durante un día. Consulte the section called “Nodos de clúster defectuosos”.

El valor máximo de `AutomatedSnapshotFailure` es >= 1 durante 1 minuto, 1 periodo consecutivo	Se produjo un error en una instantánea automatizada. Este error suele ser el resultado de un estado rojo del clúster. Consulte the section called “Estado rojo del clúster”.
	
	Para ver un resumen de todas las instantáneas automatizadas e información sobre los errores, también puede probar las siguientes solicitudes:
	
	`GET domain_endpoint /_snapshot/cs-automated/_all`
	`GET domain_endpoint /_snapshot/cs-automated-enc/_all`

Alarma	Problema
El valor máximo de `CPUUtilization` o `WarmCPUUtilization` es >= 80 % durante 15 minutos, 3 periodos consecutivos	A veces puede producirse un uso de CPU del 100 %, pero el uso sostenido elevado es problemático. Considere la posibilidad de utilizar tipos de instancias más grandes o de agregar instancias.
El valor máximo de `JVMMemoryPressure` es >= 95 % durante 1 minuto, 3 periodos consecutivos	El clúster podría encontrar errores de memoria insuficiente si aumenta el uso. Considere la posibilidad de escalar verticalmente. OpenSearch El servicio utiliza la mitad de la RAM de una instancia para el montón de Java, hasta un tamaño de pila de 32 GiB. Puede escalar las instancias verticalmente hasta 64 GiB de RAM y después escalarlas horizontalmente mediante el agregado de instancias.
El valor máximo de `OldGenJVMMemoryPressure` es >= 80 % durante 1 minuto, 3 periodos consecutivos	
El valor máximo de `MasterCPUUtilization` es >= 50 % durante 15 minutos, 3 periodos consecutivos	Considere la posibilidad de utilizar tipos de instancias más grandes para los nodos maestros dedicados. Debido al rol que desempeñan en la estabilidad del clúster y las implementaciones azul/verde, los nodos maestros dedicados deberían tener un uso de CPU medio menor que los nodos de datos.
El valor máximo de `MasterJVMMemoryPressure` es >= 95 % durante 1 minuto, 3 periodos consecutivos	

Alarma	Problema
El valor máximo de `MasterOldGenJVMMemoryPressure` es >= 80 % durante 1 minuto, 3 periodos consecutivos	
El valor de `KMSKeyError` es >= 1 durante 1 minuto, 1 periodo consecutivo	La clave de AWS KMS cifrado que se usa para cifrar los datos en reposo de tu dominio está deshabilitada. Vuelva a habilitarla para restablecer las operaciones normales. Para más información, consulte the section called “Cifrado en reposo”.
El valor de `KMSKeyInaccessible` es >= 1 durante 1 minuto, 1 periodo consecutivo	La clave de AWS KMS cifrado que se utiliza para cifrar los datos inactivos de tu dominio se ha eliminado o ha revocado su concesión al Servicio. OpenSearch No puede recuperar los dominios que están en este estado. Sin embargo, si tiene una instantánea manual, puede utilizarla para migrar a un nuevo dominio. Para más información, consulte the section called “Cifrado en reposo”.
El valor de `shards.active` es >= 30 000 durante 1 minuto, 1 periodo consecutivo	El número total de particiones primarias y de réplicas activas es superior a 30 000. Es posible que esté rotando los índices con demasiada frecuencia. Considere la posibilidad de utilizar ISM para eliminar los índices una vez que alcancen una antigüedad determinada.
Alarmas `5xx` >= 10 % de `OpenSearchRequests`	Es posible que uno o varios nodos de datos estén sobrecargados, o que las solicitudes no se completen dentro del periodo de tiempo de espera. Considere la posibilidad de cambiar a tipos de instancia más grandes o de agregar más nodos al clúster. Compruebe que está siguiendo las prácticas recomendadas para la arquitectura de particiones y clústeres.

Alarma	Problema
`MasterReachableFromNode` el máximo es < 1 durante 5 minutos, 1 vez consecutiva	Esta alarma indica que el nodo maestro se ha detenido o es inaccesible. Estos errores suelen ser el resultado de un problema de conectividad de red o de AWS dependencia.
El valor medio de `ThreadpoolWriteQueue` es >= 100 durante 1 minuto, 1 periodo consecutivo	El clúster está experimentando una alta simultaneidad de indexación. Revise y controle las solicitudes de indexación, o aumente los recursos del clúster.
El valor medio de `ThreadpoolSearchQueue` es >= 500 durante 1 minuto, 1 periodo consecutivo	El clúster está experimentando una alta simultaneidad de búsqueda. Considere la posibilidad de escalar el clúster. También se puede aumentar el tamaño de la cola de búsqueda, pero si se incrementa excesivamente puede provocar errores de memoria.
El valor máximo de `ThreadpoolSearchQueue` es >= 5000 durante 1 minuto, 1 periodo consecutivo	
El aumento de `ThreadpoolSearchRejected` SUM es >=1{expresión matemática DIFF ( )} durante 1 minuto, 1 periodo consecutivo	Estas alarmas le notifican los problemas del dominio que podrían afectar el rendimiento y la estabilidad.

Alarma	Problema
El aumento de `Threadpool WriteRejected` SUM es >=1{expresión matemática DIFF ( )} durante 1 minuto, 1 periodo consecutivo	

> **Note**
>
> Si solo desea visualizar métricas, consulte the section called “Monitoreo de métricas del clúster”.

Otras alarmas para tener en cuenta

Considere la posibilidad de configurar las siguientes alarmas en función de las funciones del OpenSearch servicio que utilice habitualmente.

Alarma	Problema
El valor mínimo de `WarmFreeStorageSpace` es <= 10 240 durante 1 minuto, 1 periodo consecutivo	Un UltraWarm nodo del clúster tiene menos de 10 GiB de espacio de almacenamiento libre. Consulte the section called “Falta de espacio de almacenamiento disponible”. Este valor está en MiB, por lo que, en lugar de 10240, se recomienda establecerlo en el 10% del espacio de almacenamiento de cada nodo. UltraWarm
El valor de `HotToWarmMigrationQueueSize` es >= 20 durante 1 minuto, 3 periodos consecutivos	Un gran número de índices se mueven simultáneamente del modo activo al almacenamiento. UltraWarm Considere la posibilidad de escalar el clúster.

Alarma	Problema
El valor de `HotToWarm Migration SuccessLatency` es **>=** 1 día, 1 periodo consecutivo	Si está intentando revertir los índices diarios, configure esta alarma para que se le notifique si el `HotToWarmMigrationSuccessCount` x latencia es superior a 24 horas.
El valor máximo de `WarmJVMMe moryPressure` es **>=** 95 % durante 1 minuto, 3 periodos consecutivos	El clúster podría encontrar errores de memoria insuficiente si aumenta el uso. Considere la posibilidad de escalar verticalmente. OpenSearch El servicio utiliza la mitad de la RAM de una instancia para el montón de Java, hasta un tamaño de pila de 32 GiB. Puede escalar las instancia s verticalmente hasta 64 GiB de RAM y después escalarlas horizonta lmente mediante el agregado de instancias.
El valor máximo de `WarmOldGe nJVMMemor yPressure` es **>=** 80 % durante 1 minuto, 3 periodos consecutivos	
El valor de `WarmToCol dMigratio nQueueSize` es **>=** 20 durante 1 minuto, 3 periodos consecutivos	Un gran número de índices se están trasladando simultáneamente al almacenamiento en frío. UltraWarm Considere la posibilidad de escalar el clúster.
El valor de `HotToWarm Migration FailureCount` es **>=** 1 durante 1 minuto, 1 periodo consecutivo	Se pueden producir errores en las migraciones si se realizan durante instantáneas, reubicaciones de particiones o fusiones forzadas. Los errores durante las instantáneas o las reubicaciones de particiones suelen deberse a errores de nodo o problemas de conectividad de S3. La falta de espacio en el disco suele ser la causa subyacente de los errores en las fusiones forzosas.

Alarma	Problema
El valor de `WarmToColdMigrationFailureCount` es >= 1 durante 1 minuto, 1 periodo consecutivo	Las migraciones suelen fallar cuando se produce un error en los intentos de migrar metadatos de índice al almacenamiento en frío. También pueden producirse errores al eliminar el estado de clúster de índice en caliente.
El valor de `WarmToColdMigrationLatency` es >= 1 día, 1 periodo consecutivo	Si está intentando revertir los índices diarios, configure esta alarma para que se le notifique si el `WarmToColdMigrationSuccessCount` x latencia es superior a 24 horas.
El valor de `AlertingDegraded` es >= 1 durante 1 minuto, 1 periodo consecutivo	El índice de alerta está en rojo, o uno o más nodos no ajustan a la programación.
El valor de `ADPluginUnhealthy` es >= 1 durante 1 minuto, 1 periodo consecutivo	El complemento de detección de anomalías no funciona correctamente, ya sea debido a altas tasas de error o porque uno de los índices utilizados está en rojo.
El valor de `AsynchronousSearchFailureRate` es >= 1 durante 1 minuto, 1 periodo consecutivo	Al menos una búsqueda asíncrona ha fallado en el último minuto, lo que probablemente significa que el nodo coordinador ha fallado. El ciclo de vida de una solicitud de búsqueda asíncrona se administra únicamente en el nodo coordinador, por lo que si el coordinador cae, la solicitud falla.

Alarma	Problema
El valor de `AsynchronousSearchStoreHealth` es >= 1 durante 1 minuto, 1 periodo consecutivo	El estado del almacén de respuestas de búsqueda asíncrona en el índice persistente está en rojo. Es posible que esté almacenando respuestas asíncronas de gran tamaño, lo que puede desestabilizar un clúster. Intente limitar las respuestas de búsqueda asíncronas a 10 MB o menos.
El valor de `SQLUnhealthy` es >= 1 durante 1 minuto, 3 periodos consecutivos	El complemento SQL devuelve 5 xx códigos de respuesta o pasa una consulta de DSL no válida a ella. OpenSearch Solucione los problemas de las solicitudes que sus clientes hacen al complemento.
El valor de `LTRStatus.red` es >= 1 durante 1 minuto, 1 periodo consecutivo	Al menos uno de los índices necesarios para ejecutar el complemento Learning to Rank carece de particiones principales y no es funcional.

Referencia general para Amazon OpenSearch Service

Amazon OpenSearch Service admite una variedad de instancias, operaciones, complementos y otros recursos.

Temas

Tipos de instancias compatibles en Amazon OpenSearch Service

Amazon OpenSearch Service admite los siguientes tipos de instancias. No todas las regiones admiten todos los tipos de instancias. Para obtener información sobre la disponibilidad, consulta los precios OpenSearch de Amazon Service.

Para obtener información sobre qué tipo de instancia es adecuada para un caso de uso, consulte the section called “Determinación del tamaño de dominios”, the section called “Cuotas de tamaño del volumen de EBS” y the section called “Cuotas de red”.

Tipos de instancias de generación actual

Para obtener el mejor rendimiento, le recomendamos que utilice los siguientes tipos de instancias al crear nuevos dominios OpenSearch de servicio.

Tipo de instancia	instancias	Restricciones
OR1	`or1.medium.search`	• Los tipos de instancias OR1 requieren la versión OpenSearch 2.11 o una versión posterior.

Tipo de instancia	instancias	Restricciones

	`or1.large.search`
	`or1.xlarge.search`
	`or1.2xlarge.search`
	`or1.4xlarge.search`
	`or1.8xlarge.search`
	`or1.12xlarge.search`
	`or1.16xlarge.search`
		• Las instancias OR1 solo son compatibles con otros tipos de instancias Graviton de nodos maestros (C6g, M6g, R6g).

Tipo de instancia	instancias	Restricciones

Im4gn	`im4gn.large.search`
	`im4gn.xlarge.search`
	`im4gn.2xlarge.search`
	`im4gn.4xlarge.search`
	`im4gn.8xlarge.search`
	`im4gn.16xlarge.search`
		• Los tipos de instancia iM4gn requieren Elasticsearch 7.9 o posterior o cualquier versión de OpenSearch, y no son compatibles con los volúmenes de almacenamiento de EBS.
		• Las instancias Im4gn solo son compatibles con otros tipos de instancias Graviton (C6g, M6g, R6g, R6gd). No se pueden combinar instancias Graviton y no Graviton en el mismo clúster.

Tipo de instancia	instancias	Restricciones

C5	`c5.large.search`
	`c5.xlarge.search`
	`c5.2xlarge.search`
	`c5.4xlarge.search`
	`c5.9xlarge.search`
	`c5.18xlarge.search`
		Los tipos de instancias C5 requieren Elasticsearch 5.1 o posterior o cualquier versión de. OpenSearch

Tipo de instancia	instancias	Restricciones

C6g	`c6g.large.search`
	`c6g.xlarge.search`
	`c6g.2xlarge.search`
	`c6g.4xlarge.search`
	`c6g.8xlarge.search`
	`c6g.12xlarge.search`
		• Los tipos de instancia C6g requieren Elasticsearch 7.9 o posterior o cualquier versión de. OpenSearch
		• Las instancias C6g solo son compatibles con otros tipos de instancias Graviton (Im4gn, M6g, R6g, R6gd). No se pueden combinar instancias Graviton y no Graviton en el mismo clúster.

Tipo de instancia	instancias	Restricciones

I3	`i3.large.search`
	`i3.xlarge.search`
	`i3.2xlarge.search`
	`i3.4xlarge.search`
	`i3.8xlarge.search`
	`i3.16xlarge.search`
		Los tipos de instancias I3 requieren Elasticsearch 5.1 o posterior o cualquier versión de OpenSearch, y no son compatibles con los volúmenes de almacenamiento de EBS.

M5	`m5.large.search`
	`m5.xlarge.search`
	`m5.2xlarge.search`
	`m5.4xlarge.search`
	`m5.12xlarge.search`
		Los tipos de instancias M5 requieren Elasticsearch 5.1 o posterior o cualquier versión de. OpenSearch

Tipo de instancia	instancias	Restricciones

M6g	`m6g.large.search`
	`m6g.xlarge.search`
	`m6g.2xlarge.search`
	`m6g.4xlarge.search`
	`m6g.8xlarge.search`
	`m6g.12xlarge.search`
		• Los tipos de instancias M6g requieren Elasticsearch 7.9 o posterior o cualquier versión de. OpenSearch
		• Las instancias M6g solo son compatibles con otros tipos de instancias Graviton (Im4gn, C6g, R6g, R6gd). No se pueden combinar instancias Graviton y no Graviton en el mismo clúster.

Tipo de instancia	instancias	Restricciones

R5	`r5.large.search`
	`r5.xlarge.search`
	`r5.2xlarge.search`
	`r5.4xlarge.search`
	`r5.12xlarge.search`
		Los tipos de instancia R5 requieren Elasticsearch 5.1 o posterior o cualquier versión de. OpenSearch

Tipo de instancia	instancias	Restricciones

R6g	`r6g.large.search`
	`r6g.xlarge.search`
	`r6g.2xlarge.search`
	`r6g.4xlarge.search`
	`r6g.8xlarge.search`
	`r6g.12xlarge.search`
		• Los tipos de instancias R6g requieren Elasticsearch 7.9 o posterior o cualquier versión de. OpenSearch
		• Las instancias R6g solo son compatibles con otros tipos de instancias Graviton (Im4gn, C6g, M6g, R6gd). No se pueden combinar instancias Graviton y no Graviton en el mismo clúster.

Tipo de instancia	instancias	Restricciones

R6gd	`r6gd.large.search`
	`r6gd.xlarge.search`
	`r6gd.2xlarge.search`
	`r6gd.4xlarge.search`
	`r6gd.8xlarge.search`
	`r6gd.12xlarge.search`
	`r6gd.16xlarge.search`
		• Los tipos de instancia R6gd requieren Elasticsearch 7.9 o posterior o cualquier versión de, y no son compatibles con los volúmenes de almacenamiento de OpenSearch EBS.
		• Las instancias R6gd solo son compatibles con otros tipos de instancias Graviton (Im4gn, C6g, M6g, R6g). No se pueden combinar instancias Graviton y no Graviton en el mismo clúster.

Tipo de instancia	instancias	Restricciones
T3	`t3.small.search` `t3.medium.search`	• Los tipos de instancias T3 requieren Elasticsearch 5.6 o posterior o cualquier versión de. OpenSearch • Puedes usar los tipos de instancias T3 solo si tu dominio está aprovisionado sin opciones de espera. Para obtener más información, consulte the section called “Multi-AZ sin modo de espera”. • Solo puedes usar los tipos de instancias T3 si el número de instancias de tu dominio es de 10 o menos. • Los tipos de instancias T3 no admiten el UltraWarm almacenamiento, el almacenamiento en frío ni el ajuste automático.

Tipos de instancias de generación anterior

OpenSearch El servicio ofrece tipos de instancias de generaciones anteriores para los usuarios que han optimizado sus aplicaciones en función de ellos y que aún no las han actualizado. Le recomendamos que utilice los tipos de instancia de la generación actual para obtener un rendimiento óptimo, pero seguimos admitiendo los siguientes tipos de instancia de la generación anterior.

Tipo de instancia	instancias	Restricciones

C4	`c4.large.search`
	`c4.xlarge.search`
	`c4.2xlarge.search`
	`c4.4xlarge.search`	

Tipo de instancia	instancias	Restricciones
	`c4.8xlarge.search`	
I2	`i2.xlarge.search` `i2.2xlarge.search`	

M3	`m3.medium.search`
	`m3.large.search`
	`m3.xlarge.search`
	`m3.2xlarge.search`
		• Los tipos de instancia M3 no admiten el cifrado de datos en reposo, el control de acceso detallado ni la búsqueda en clústeres.
		• Los tipos de instancias M3 tienen restricciones adicionales según OpenSearch la versión. Para más información, consulte the section called “Tipo de instancia M3 no válido”.

M4	`m4.large.search`
	`m4.xlarge.search`
	`m4.2xlarge.search`
	`m4.4xlarge.search`
	`m4.10xlarge.search`	

Tipo de instancia	instancias	Restricciones

R3	`r3.large.search`
	`r3.xlarge.search`
	`r3.2xlarge.search`
	`r3.4xlarge.search`
	`r3.8xlarge.search`
		Los tipos de instancia R3 no admiten el cifrado de datos en reposo ni el control de acceso detallado.

R4	`r4.large.search`
	`r4.xlarge.search`
	`r4.2xlarge.search`
	`r4.4xlarge.search`
	`r4.8xlarge.search`
	`r4.16xlarge.search`	

Tipo de instancia	instancias	Restricciones

T2	`t2.micro.search`
	`t2.small.search`
	`t2.medium.search`
		• Solo puede usar los tipos de instancias T2 cuando el recuento de instancias del dominio sea 10 o menos.
		• El tipo de instancia `t2.micro.search` solo admite Elasticsearch 1.5 y 2.3.
		• Los tipos de instancias T2 no admiten el cifrado de datos en reposo, el control de acceso detallado, el almacenamiento, el UltraWarm almacenamiento en frío, la búsqueda entre clústeres ni el ajuste automático.

> **Tip**
>
> Recomendamos utilizar tipos de instancias diferentes para nodos maestros dedicados y nodos de datos.

Características por versión de motor en Amazon OpenSearch Service

Muchas funciones OpenSearch del servicio requieren una OpenSearch versión mínima o una versión antigua de Elasticsearch OSS. Si cumple la versión mínima de una característica, pero la característica no está disponible en el dominio, actualice el software de servicio.

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Compatibilidad con VPC	1.0	1.0
Requerir HTTPS para todo		

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
el tráfico al dominio		
Compatibilidad con Multi-AZ		
Nodos maestros dedicados		
Paquetes personalizados		
Puntos de conexión personalizados		
Publicación de registros lentos		
Registro de errores de publicación	1.0	5.1
Cifrado de datos en reposo		

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Autenticación de Cognito para paneles OpenSearch		
Actualizaciones locales		
Compatibilidad con Curator	No incluido	5.1
Instantáneas automatizadas por hora	1.0	5.3
Sin cifrado ode-to-node	1.0	6.0
Compatibilidad con cliente REST de alto nivel de Java		

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Compresión de solicitud y respuesta HTTP		
Alertas	1.0	6.2
SQL	1.0	6.5
Búsqueda en clústeres	1.0	6.7
Control de acceso detallado		
Autenticación SAML para paneles OpenSearch		
Ajuste automático		
Reindexación remota		
UltraWarm	1.0	6.8
Administración de estados de índice		

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
k-NN por distancia euclidiana	1.0	7.1
Detección de anomalías	1.0	7.4
k-NN por similitud coseno	1.0	7.7
Aprender a clasificar		
Lenguaje de procesamiento de canalizaciones	1.0	7.9
OpenSearch Informes de cuadros de mando		
OpenSearch Paneles de mando: Trace Analytics		

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Instancias de Graviton basadas en ARM		
Almacenamiento en frío		
Distancia de Hamming, distancia de norma L1 y scripting Painless para k-NN	1.0	7.10
Búsqueda asíncrona		
Transformaciones de índices	1.0	No incluido
Replicación entre clústeres	1.1	7.10
ML Commons	1.3	No incluido
Notificaciones	2.3	No incluido
Búsqueda puntual	2,5	No incluido

Característica	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Buscar canalizaciones	2.9	No incluido
Nuevos conectores de machine learning	2.9	No incluido
Búsqueda semántica multimodal	2.11	No incluido
Orígenes de datos de consulta directa para Amazon S3	2.11	No incluido

Para obtener información acerca de los complementos, que habilitan algunas de estas características y funcionalidades adicionales, consulte the section called “Complementos por versión de motor”. Para obtener información sobre la OpenSearch API de cada versión, consultethe section called “Operaciones admitidas”.

Plugins por versión de motor en Amazon OpenSearch Service

Los dominios OpenSearch de Amazon Service vienen preempaquetados con complementos de la OpenSearch comunidad. El servicio implementa y administra los complementos automáticamente, pero implementa complementos diferentes según la versión del sistema operativo Elasticsearch OpenSearch heredado que elija para su dominio.

En la siguiente tabla se enumeran los complementos por OpenSearch versión, así como las versiones compatibles del sistema operativo Elasticsearch heredado. Solo incluye los complementos con los que puede interactuar; no es exhaustiva. OpenSearch El servicio utiliza complementos

adicionales para habilitar las funciones principales del servicio, como el complemento S3 Repository para las instantáneas y el complemento OpenSearchPerformance Analyzer para la optimización y la supervisión. Para obtener una lista completa de todos los complementos que se ejecutan en un dominio, realice la siguiente solicitud:

```
GET _cat/plugins?v
```

Complemento	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
ICU Analysis	1.0	Incluido en todos los dominios
Japanese (kuromoji) Analysis		
Phonetic Analysis	1.0	2.3
Seunjeon Korean Analysis	1.0	5.1
Smart Chinese Analysis		
Stempel Polish Analysis		
Ingest Attachment Processor		

Complemento	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
Ingest User Agent Processor		
Mapper Murmur3		
Mapper Size	1.0	5.3
Ukrainian Analysis		
OpenSearch alertando	1.0	6.2
OpenSearch SQL	1.0	6.5
OpenSearch seguridad	1.0	6.7
OpenSearch Index State Management	1.0	6.8
OpenSearch k-NN	1.0	7.1
OpenSearch detección de anomalías	1.0	7.4

Complemento	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
IK (Chinese) Analysis	1.0	7.7
Vietnamese Analysis		
Thai Analysis		
Learning to Rank		
OpenSearch búsqueda asíncrona	1.0	7.10
OpenSearch replicación entre clústeres	1.1	7.10
OpenSearch observabilidad	1.2	No compatible
Análisis Nori	1.3	No compatible
Análisis de Pinyin	1.3	No compatible
StConvert	1.3	No compatible
Análisis de Sudachi	1.3	No compatible

Complemento	Versión mínima requerida OpenSearch	Versión mínima requerida de Elasticsearch
ML Commons	1.3	No compatible
OpenSearch notificaciones	2.3	No compatible
Security Analytics	2,5	No compatible
Búsqueda neuronal	2.9	No compatible
Ranking de búsqueda de Amazon Personalize	2.9	No compatible

Complementos opcionales

Además de los complementos predeterminados que vienen preinstalados, Amazon OpenSearch Service admite varios complementos de análisis de idiomas. Estos complementos están marcados como opcionales en la tabla anterior. Puedes usar AWS Management Console y AWS CLI para asociar un complemento a un dominio, desasociar un complemento de un dominio y enumerar todos los complementos. Un paquete de complementos opcional es compatible con una OpenSearch versión específica y solo se puede asociar a los dominios con esa versión.

Tenga en cuenta que para el complemento Sudachi, al volver a asociar un archivo de diccionario, no se refleja inmediatamente en el dominio. El diccionario se actualiza cuando se ejecuta la siguiente implementación azul/verde en el dominio como parte de un cambio de configuración u otra actualización. Como alternativa, puede crear un índice nuevo, volver a indexar el índice existente en el nuevo índice y, a continuación, eliminar el índice anterior. Si prefiere utilizar el enfoque de reindexación, utilice un alias de índice para que no se interrumpa el tráfico.

Los complementos opcionales utilizan el tipo de paquete `ZIP-PLUGIN`. Para obtener más información sobre los complementos opcionales, consulte the section called “Paquetes personalizados”.

Operaciones compatibles en Amazon OpenSearch Service

OpenSearch El servicio es compatible con muchas versiones OpenSearch y versiones antiguas del sistema operativo Elasticsearch. En las siguientes secciones, se muestran las operaciones que admite OpenSearch Service para cada versión.

Temas

- Elasticsearch versión 6.0
- Elasticsearch versión 5.6
- Elasticsearch versión 5.5
- Elasticsearch versión 5.3
- Elasticsearch versión 5.1
- Elasticsearch versión 2.3
- Elasticsearch versión 1.5

Diferencias de API destacadas

Configuración y estadísticas

OpenSearch El servicio solo acepta solicitudes PUT a la `_cluster/settings` API que utilizan el formulario de configuración «plano». Rechaza las solicitudes que utilizan el formato de configuración expandido.

```
// Accepted
PUT _cluster/settings
{
  "persistent" : {
    "action.auto_create_index" : false
  }
}

// Rejected
PUT _cluster/settings
{
  "persistent": {
    "action": {
      "auto_create_index": false
    }
  }
}
```

El cliente REST Java de alto nivel utiliza el formato expandido, por lo que, si necesita enviar solicitudes de configuración, use el cliente de bajo nivel.

Antes de Elasticsearch 5.3, la `_cluster/settings` API de los dominios de OpenSearch servicio solo admitía el `PUT` método HTTP, no el `GET` método. OpenSearch y las versiones posteriores de Elasticsearch admiten `GET` este método, como se muestra en el siguiente ejemplo:

```
GET https://domain-name.region.es.amazonaws.com/_cluster/settings?pretty
```

A continuación se muestra un ejemplo de rentabilidad:

```
{
  "persistent": {
    "cluster": {
      "routing": {
        "allocation": {
          "cluster_concurrent_rebalance": "2",
          "node_concurrent_recoveries": "2",
          "disk": {
            "watermark": {
              "low": "1.35gb",
              "flood_stage": "0.45gb",
              "high": "0.9gb"
            }
          },
          "node_initial_primarirecoveries": "4"
        }
      }
    },
    "indices": {
      "recovery": {
        "max_bytper_sec": "40mb"
      }
    }
  }
}
```

Si comparas las respuestas de un OpenSearch clúster de código abierto y de un OpenSearch servicio para determinadas API de configuración y estadísticas, es posible que veas que faltan campos. OpenSearch El servicio redacta determinada información que expone aspectos internos del servicio, como la ruta de acceso a los datos del sistema de archivos `_nodes/stats` o el nombre y la versión del sistema operativo. `_nodes`

Reducir

La API `_shrink` puede hacer que las actualizaciones, los cambios de configuración y las eliminaciones de dominio no se lleven a cabo correctamente. No recomendamos utilizarla en dominios que ejecuten las versiones 5.3 o 5.1 de Elasticsearch. Estas versiones tienen un error que puede causar un error en la restauración de instantáneas de índices encogidos.

Si utilizas la `_shrink` API en otras OpenSearch versiones o en otras versiones de Elasticsearch, realiza la siguiente solicitud antes de iniciar la operación de reducción:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": "name-of-the-node-to-shrink-to",
    "index.blocks.read_only": true
  }
}
```

A continuación, realice la siguiente solicitud después de completar la operación de reducción:

```
PUT https://domain-name.region.es.amazonaws.com/source-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}

PUT https://domain-name.region.es.amazonaws.com/shrunken-index/_settings
{
  "settings": {
    "index.routing.allocation.require._name": null,
    "index.blocks.read_only": false
  }
}
```

OpenSearch versión 2.11

Para la OpenSearch versión 2.11, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* /_forcemerge , */index-name* /update/*id* y */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search/pipeline
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `/_count`
- `/_dashboards`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 2.9

Para la OpenSearch versión 2.9, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/pipeline`

- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_notifications
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_search/point_in_time
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este

encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.

3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 2.7

En la OpenSearch versión 2.7, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`

- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_security_analytics`
- `/_plugins/_sm`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.

5. Consulte the section called “Reducir”.

OpenSearch versión 2.5

Para la OpenSearch versión 2.5, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `/_plugins/_notifications`
- `/_plugins/_ppl`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search/point_in_time`
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_security
- /_plugins/_security_analytics
- /_plugins/_sm
- /_plugins/_sql
- /_percolate
- /_rank_eval

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 2.3

En el OpenSearch caso de la versión 2.3, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ml`
- `_plugins/_notifications`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `/_count`
- `/_dashboards`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 1.3

En el OpenSearch caso de la versión 1.3, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como `/index-name /_forcemerge` , `/index-name /update/id` y `/index-name /_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`

- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ml
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_percolate
- /_rank_eval
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este

encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.

3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 1.2

Para la OpenSearch versión 1.2, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`

- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_dashboards`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_percolate`
- `/_rank_eval`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.

5. Consulte the section called “Reducir”.

OpenSearch versión 1.1

En el OpenSearch caso de la versión 1.1, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_plugins/_asynchronous_search`
- `/_plugins/_alerting`
- `/_plugins/_anomaly_detection`
- `/_plugins/_ism`
- `/_plugins/_ppl`
- `/_plugins/_security`
- `/_plugins/_sql`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_dashboards
- /_plugins/_transforms
- /_percolate
- /_rank_eval

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

OpenSearch versión 1.0

Para la OpenSearch versión 1.0, el OpenSearch servicio admite las siguientes operaciones. Para obtener información sobre la mayoría de las operaciones, consulta la referencia de la API de OpenSearch REST o la referencia de la API del complemento específico.

- Todas las operaciones de la ruta de índice (como */index-name* /_forcemerge , */index-name* /update/*id* y */index-name* /_close)
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_ltr
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_plugins/_asynchronous_search
- /_plugins/_alerting
- /_plugins/_anomaly_detection
- /_plugins/_ism
- /_plugins/_ppl
- /_plugins/_security
- /_plugins/_sql
- /_plugins/_transforms
- /_percolate
- /_rank_eval
- /_refresh
- /_reindex [1]
- /_render
- /_resolve/index
- /_rollover
- /_scripts [3]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

- `/_count`
- `/_dashboards`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres de los `scroll_id` valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 7.10

Para Elasticsearch 7.10, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_index_template`
- `/_ltr`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`

- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_cluster/state
- /_cluster/stats
- /_count
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_asynchronous_search
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_ppl
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_plugins/_replication
- /_rank_eval
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template [6]
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en scroll_id los valores, utilice el cuerpo de la solicitud, no la cadena de consulta, para pasar scroll_id los valores a Service. OpenSearch

3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método PUT. Para obtener información acerca del método GET, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.
6. Las plantillas de índice heredadas (`_template`) fueron reemplazadas por plantillas que se pueden combinar (`_index_template`), a partir de Elasticsearch 7.8. Las plantillas que se pueden combinar tienen prioridad sobre las plantillas heredadas. Si ninguna plantilla que se puede combinar coincide con un índice determinado, una plantilla heredada puede coincidir y ser aplicada. La `_template` operación sigue funcionando en las versiones posteriores de Elasticsearch OSS OpenSearch y en las versiones posteriores, pero las llamadas GET a los dos tipos de plantillas arrojan resultados diferentes.

Elasticsearch versión 7.9

Para Elasticsearch 7.9, OpenSearch Service admite las siguientes operaciones.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_resolve/index`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`

- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `cluster.max_shards_per_node`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_ppl`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las OpenSearch operaciones genéricas que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.

5. Consulte the section called “Reducir”.
6. Las plantillas de índice heredadas (`_template`) fueron reemplazadas por plantillas que se pueden combinar (`_index_template`), a partir de Elasticsearch 7.8. Las plantillas que se pueden combinar tienen prioridad sobre las plantillas heredadas. Si ninguna plantilla que se puede combinar coincide con un índice determinado, una plantilla heredada puede coincidir y ser aplicada. La `_template` operación sigue funcionando en las versiones posteriores de Elasticsearch OSS OpenSearch y en las versiones posteriores, pero las llamadas GET a los dos tipos de plantillas arrojan resultados diferentes.

Elasticsearch versión 7.8

En el caso de Elasticsearch 7.8, OpenSearch Service admite las siguientes operaciones.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_index_template` [6]
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template` [6]
- `/_update_by_query` [1]
- `/_validate`

- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.
6. Las plantillas de índice heredadas (`_template`) fueron reemplazadas por plantillas que se pueden combinar (`_index_template`), a partir de Elasticsearch 7.8. Las plantillas que se pueden combinar tienen prioridad sobre las plantillas heredadas. Si ninguna plantilla que se puede combinar coincide con un índice determinado, una plantilla heredada puede coincidir y ser aplicada. La `_template` operación sigue funcionando en las versiones posteriores de Elasticsearch OSS OpenSearch y en las versiones posteriores, pero las llamadas GET a los dos tipos de plantillas arrojan resultados diferentes.

Elasticsearch versión 7.7

En el caso de Elasticsearch 7.7, OpenSearch Service admite las siguientes operaciones.

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_ltr`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_anomaly_detection`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `cluster.max_shards_per_node`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 7.4

En el caso de Elasticsearch 7.4, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones de la ruta de índice (como */index-name* `/_forcemerge` , */index-name* `/update/`*id* y */index-name* `/_close`)
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]

- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_anomaly_detection
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en scroll_id los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar scroll_id los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método PUT. Para obtener información acerca del método GET, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones

genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.

5. Consulte the section called “Reducir”.

Elasticsearch versión 7.1

En el caso de Elasticsearch 7.1, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_ism`
- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- indices.breaker.request.limit
- indices.breaker.total.limit
- cluster.max_shards_per_node

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.8

En el caso de Elasticsearch 6.8, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]

- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
  - cluster.max_shards_per_node
  - cluster.blocks.read_only
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_opendistro/_alerting
- /_opendistro/_ism
- /_opendistro/_security
- /_opendistro/_sql
- /_percolate
- /_plugin/kibana
- /_rank_eval
- /_search profile
- /_shard_stores
- /_shrink[5]
- /_snapshot
- /_split
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este

encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.

3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.7

En el caso de Elasticsearch 6.7, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `action.auto_create_index`
- `action.search.shard_count.limit`
- `indices.breaker.fielddata.limit`
- `indices.breaker.request.limit`
- `indices.breaker.total.limit`
- `cluster.max_shards_per_node`

- `/_opendistro/_security`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.5

En el caso de Elasticsearch 6.5, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_opendistro/_sql`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.

2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.4

En el caso de Elasticsearch 6.4, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.3

En el caso de Elasticsearch 6.3, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.

2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.2

En el caso de Elasticsearch 6.2, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_opendistro/_alerting`
- `/_refresh`
- `/_reindex` [1]
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search`[2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink`[5]
- `/_snapshot`
- `/_split`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`

- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_percolate`
- `/_plugin/kibana`
- `/_rank_eval`
- `/_update_by_query` [1]
- `/_validate`

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 6.0

En el caso de Elasticsearch 6.0, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* */_forcemerge* y */index-name* */update/id*) excepto */index-name* */_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search [2]
- /_search profile
- /_shard_stores
- /_shrink [5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.

2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 5.6

En el caso de Elasticsearch 5.6, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_render`
- `/_rollover`
- `/_scripts` [3]
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [5]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `/_cluster/settings` para varias propiedades [4]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 5.5

En el caso de Elasticsearch 5.5, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* */_forcemerge* y */index-name* */update/id*) excepto */index-name* */_close*
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades [4]:
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_cluster/state
- /_cluster/stats
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_render
- /_rollover
- /_scripts [3]
- /_search [2]
- /_search profile
- /_shard_stores
- /_shrink [5]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.

2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Consulte the section called “Otros recursos admitidos” para ver consideraciones sobre la utilización de scripts.
4. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
5. Consulte the section called “Reducir”.

Elasticsearch versión 5.3

En el caso de Elasticsearch 5.3, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/update/`*id*) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/allocation/explain`
- `/_cluster/health`
- `/_cluster/pending_tasks`
- `/_cluster/state`
- `/_cluster/stats`
- `/_count`
- `/_delete_by_query` [1]
- `/_explain`
- `/_field_caps`
- `/_field_stats`
- `/_flush`
- `/_ingest/pipeline`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_mtermvectors`
- `/_nodes`
- `/_percolate`
- `/_render`
- `/_rollover`
- `/_search` [2]
- `/_search profile`
- `/_shard_stores`
- `/_shrink` [4]
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_tasks`
- `/_template`
- `/_update_by_query` [1]
- `/_validate`

- `/_cluster/settings` para varias propiedades[3]:
  - `action.auto_create_index`
  - `action.search.shard_count.limit`
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
- `/_plugin/kibana`
- `/_refresh`
- `/_reindex` [1]

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación `/_tasks` combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para `/_search/scroll` con un cuerpo de mensaje deben especificar `"Content-Length"` en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en `scroll_id` los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.
3. Se refiere al método `PUT`. Para obtener información acerca del método `GET`, consulte the section called “Diferencias de API destacadas”. Esta lista solo hace referencia a las operaciones genéricas de Elasticsearch que admite OpenSearch Service y no incluye las operaciones compatibles específicas de los complementos para la detección de anomalías, el ISM, etc.
4. Consulte the section called “Reducir”.

Elasticsearch versión 5.1

En el caso de Elasticsearch 5.1, Service admite las siguientes operaciones. OpenSearch

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-*
- `/_cluster/state`
- `/_cluster/stats`
- `/_render`
- `/_rollover`

name /update/*id*) excepto */index-name* /_close
- /_alias
- /_aliases
- /_all
- /_analyze
- /_bulk
- /_cat (excepto /_cat/nodeattrs)
- /_cluster/allocation/explain
- /_cluster/health
- /_cluster/pending_tasks
- /_cluster/settings para varias propiedades (solo PUT):
  - action.auto_create_index
  - action.search.shard_count.limit
  - indices.breaker.fielddata.limit
  - indices.breaker.request.limit
  - indices.breaker.total.limit
- /_count
- /_delete_by_query [1]
- /_explain
- /_field_caps
- /_field_stats
- /_flush
- /_ingest/pipeline
- /_mapping
- /_mget
- /_msearch
- /_mtermvectors
- /_nodes
- /_percolate
- /_plugin/kibana
- /_refresh
- /_reindex [1]
- /_search[2]
- /_search profile
- /_shard_stores
- /_shrink[3]
- /_snapshot
- /_stats
- /_status
- /_tasks
- /_template
- /_update_by_query [1]
- /_validate

1. Los cambios en la configuración de un clúster pueden interrumpir estas operaciones antes de que finalicen. Recomendamos utilizar la operación /_tasks combinada con estas operaciones para verificar que las solicitudes se hayan llevado a cabo correctamente.
2. Las solicitudes DELETE para /_search/scroll con un cuerpo de mensaje deben especificar "Content-Length" en el encabezado HTTP. La mayoría de los clientes agregan este encabezado de forma predeterminada. Para evitar problemas con los = caracteres en scroll_id

los valores, usa el cuerpo de la solicitud, no la cadena de consulta, para pasar `scroll_id` los valores a OpenSearch Service.

3. Consulte the section called “Reducir”.

Elasticsearch versión 2.3

Para Elasticsearch 2.3, OpenSearch Service admite las siguientes operaciones.

- Todas las operaciones en la ruta de índice (como */index-name* `/_forcemerge` y */index-name* `/_recovery`) excepto */index-name* `/_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cache/clear` (solo índice)
- `/_cat` (excepto `/_cat/nodeattrs`)
- `/_cluster/health`
- `/_cluster/settings` para varias propiedades (solo PUT):
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
  - `threadpool.bulk.queue_size`
  - `threadpool.index.queue_size`
  - `threadpool.percolate.queue_size`
  - `threadpool.search.queue_size`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_refresh`
- `/_render`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

- `threadpool.suggest.queue_size`

Elasticsearch versión 1.5

Para Elasticsearch 1.5, OpenSearch Service admite las siguientes operaciones.

- Todas las operaciones de la ruta de índice, como `/index-name /_optimize` y `/index-name /_warmer`, excepto `/index-name /_close`
- `/_alias`
- `/_aliases`
- `/_all`
- `/_analyze`
- `/_bulk`
- `/_cat`
- `/_cluster/health`
- `/_cluster/settings` para varias propiedades (solo PUT):
  - `indices.breaker.fielddata.limit`
  - `indices.breaker.request.limit`
  - `indices.breaker.total.limit`
  - `threadpool.get.queue_size`
  - `threadpool.bulk.queue_size`
  - `threadpool.index.queue_size`
  - `threadpool.percolate.queue_size`
  - `threadpool.search.queue_size`
  - `threadpool.suggest.queue_size`
- `/_cluster/stats`
- `/_count`
- `/_flush`
- `/_mapping`
- `/_mget`
- `/_msearch`
- `/_nodes`
- `/_percolate`
- `/_plugin/kibana`
- `/_plugin/kibana3`
- `/_plugin/migration`
- `/_refresh`
- `/_search`
- `/_snapshot`
- `/_stats`
- `/_status`
- `/_template`

Cuotas OpenSearch de Amazon Service

Tu AWS cuenta tiene cuotas predeterminadas, anteriormente denominadas límites, para cada AWS servicio. A menos que se indique lo contrario, cada cuota es específica de la región de .

Para ver las cuotas de los dominios e instancias de OpenSearch servicio, Amazon OpenSearch Serverless y Amazon OpenSearch Ingestion, consulte las cuotas de Amazon OpenSearch Service en. Referencia general de AWS

Para ver las cuotas de OpenSearch Service en AWS Management Console, abra la consola Service Quotas. En el panel de navegación, elige AWS servicios y selecciona Amazon OpenSearch Service. Para solicitar un aumento de cuota, consulte Solicitud de un aumento de cuota en la Guía de usuario de Service Quotas.

Temas

UltraWarm cuotas de almacenamiento

En la siguiente tabla, se muestran los tipos de UltraWarm instancias y la cantidad máxima de almacenamiento que puede utilizar cada tipo. Para obtener más información al respecto UltraWarm, consultethe section called “UltraWarm almacenamiento”.

Tipo de instancia	Almacenamiento máximo
`ultrawarm1.medium.search`	1,5 TiB
`ultrawarm1.large.search`	20 TiB

Cuotas de tamaño del volumen de EBS

En la siguiente tabla se muestran los tamaños mínimo y máximo de los volúmenes de EBS para cada tipo de instancia que admite el OpenSearch servicio. Para obtener información sobre qué tipos de instancias incluyen almacenamiento de instancias y detalles de hardware adicionales, consulta los precios OpenSearch de Amazon Service.

- Si elige el almacenamiento magnético en EBS volume type (Tipo de volumen de EBS) al crear un dominio, el tamaño de volumen máximo es de 100 GiB para todos los tipos de instancias, excepto `t2.small` y `t2.medium`, y todas las instancias de Graviton (M6g, C6g, R6g y R6gd) que no admiten almacenamiento magnético. Para el tamaño máximo que se muestra en la tabla siguiente, elija una de las opciones de SSD.
- Algunos tipos de instancias de generaciones anteriores incluyen almacenamiento de la instancia, pero también admiten el almacenamiento de EBS. Si elige el almacenamiento de EBS para uno de estos tipos de instancia, los volúmenes de almacenamiento no se suman. Puede utilizar el almacenamiento de la instancia o un volumen de EBS, no ambos.

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
`t2.micro.search`	10 GiB	35 GiB	N/A
`t2.small.search`	10 GiB	35 GiB	N/A
`t2.medium.search`	10 GiB	35 GiB	N/A
`t3.small.search`	10 GiB	100 GiB	100 GiB
`t3.medium.search`	10 GiB	200 GiB	200 GiB
`m3.medium.search`	10 GiB	100 GiB	N/A
`m3.large.search`	10 GiB	512 GiB	N/A
`m3.xlarge.search`	10 GiB	512 GiB	N/A
`m3.2xlarge.search`	10 GiB	512 GiB	N/A

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
m4.large.search	10 GiB	512 GiB	N/A
m4.xlarge.search	10 GiB	1 TiB	N/A
m4.2xlarge.search	10 GiB	1,5 TiB	N/A
m4.4xlarge.search	10 GiB	1,5 TiB	N/A
m4.10xlarge.search	10 GiB	1,5 TiB	N/A
m5.large.search	10 GiB	512 GiB	1 TiB
m5.xlarge.search	10 GiB	1 TiB	2 TiB
m5.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m5.4xlarge.search	10 GiB	3 TiB	6 TiB
m5.12xlarge.search	10 GiB	9 TiB	18 TiB
m6g.large.search	10 GiB	512 GiB	1 TiB
m6g.xlarge.search	10 GiB	1 TiB	2 TiB
m6g.2xlarge.search	10 GiB	1,5 TiB	3 TiB
m6g.4xlarge.search	10 GiB	3 TiB	6 TiB
m6g.8xlarge.search	10 GiB	6 TiB	12 TiB
m6g.12xlarge.search	10 GiB	9 TiB	18 TiB
c4.large.search	10 GiB	100 GiB	N/A
c4.xlarge.search	10 GiB	512 GiB	N/A
c4.2xlarge.search	10 GiB	1 TiB	N/A

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
c4.4xlarge.search	10 GiB	1,5 TiB	N/A
c4.8xlarge.search	10 GiB	1,5 TiB	N/A
c5.large.search	10 GiB	256 GiB	256 GiB
c5.xlarge.search	10 GiB	512 GiB	512 GiB
c5.2xlarge.search	10 GiB	1 TiB	1 TiB
c5.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c5.9xlarge.search	10 GiB	3,5 TiB	3,5 TiB
c5.18xlarge.search	10 GiB	7 TiB	7 TiB
c6g.large.search	10 GiB	256 GiB	256 GiB
c6g.xlarge.search	10 GiB	512 GiB	512 GiB
c6g.2xlarge.search	10 GiB	1 TiB	1 TiB
c6g.4xlarge.search	10 GiB	1,5 TiB	1,5 TiB
c6g.8xlarge.search	10 GiB	3 TiB	3 TiB
c6g.12xlarge.search	10 GiB	4,5 TiB	4,5 TiB
r3.large.search	10 GiB	512 GiB	N/A
r3.xlarge.search	10 GiB	512 GiB	N/A
r3.2xlarge.search	10 GiB	512 GiB	N/A
r3.4xlarge.search	10 GiB	512 GiB	N/A
r3.8xlarge.search	10 GiB	512 GiB	N/A

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
r4.large.search	10 GiB	1 TiB	N/A
r4.xlarge.search	10 GiB	1,5 TiB	N/A
r4.2xlarge.search	10 GiB	1,5 TiB	N/A
r4.4xlarge.search	10 GiB	1,5 TiB	N/A
r4.8xlarge.search	10 GiB	1,5 TiB	N/A
r4.16xlarge.search	10 GiB	1,5 TiB	N/A
r5.large.search	10 GiB	1 TiB	2 TiB
r5.xlarge.search	10 GiB	1,5 TiB	3 TiB
r5.2xlarge.search	10 GiB	3 TiB	6 TiB
r5.4xlarge.search	10 GiB	6 TiB	12 TiB
r5.12xlarge.search	10 GiB	12 TiB	24 TiB
r6g.large.search	10 GiB	1 TiB	2 TiB
r6g.xlarge.search	10 GiB	1,5 TiB	3 TiB
r6g.2xlarge.search	10 GiB	3 TiB	6 TiB
r6g.4xlarge.search	10 GiB	6 TiB	12 TiB
r6g.8xlarge.search	10 GiB	8 TiB	16 TiB
r6g.12xlarge.search	10 GiB	12 TiB	24 TiB
r6gd.large.search	N/A	N/A	N/A
r6gd.xlarge.search	N/A	N/A	N/A

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
r6gd.2xlarge.search	N/A	N/A	N/A
r6gd.4xlarge.search	N/A	N/A	N/A
r6gd.8xlarge.search	N/A	N/A	N/A
r6gd.12xlarge.search	N/A	N/A	N/A
r6gd.16xlarge.search	N/A	N/A	N/A
i2.xlarge.search	10 GiB	512 GiB	N/A
i2.2xlarge.search	10 GiB	512 GiB	N/A
i3.large.search	N/A	N/A	N/A
i3.xlarge.search	N/A	N/A	N/A
i3.2xlarge.search	N/A	N/A	N/A
i3.4xlarge.search	N/A	N/A	N/A
i3.8xlarge.search	N/A	N/A	N/A
i3.16xlarge.search	N/A	N/A	N/A
or1.medium.search	20 GiB	N/A	768 GiB
or1.large.search	20 GiB	N/A	1532 GiB
or1.xlarge.search	20 GiB	N/A	3 TiB
or1.2xlarge.search	20 GiB	N/A	6 TiB
or1.4xlarge.search	20 GiB	N/A	12 TiB
or1.8xlarge.search	20 GiB	N/A	16 TiB

Tipo de instancia	Tamaño mínimo de EBS	Tamaño máximo de EBS (gp2)	Tamaño máximo de EBS (gp3)
or1.12xlarge.search	20 GiB	N/A	24 TiB
or1.16xlarge.search	20 GiB	N/A	36 TiB
im4gn.large.search	N/A	N/A	N/A
im4gn.xlarge.search	N/A	N/A	N/A
im4gn.2xlarge.search	N/A	N/A	N/A
im4gn.4xlarge.search	N/A	N/A	N/A
im4gn.8xlarge.search	N/A	N/A	N/A
im4gn.16xlarge.search	N/A	N/A	N/A

Cuotas de red

La siguiente tabla muestra el tamaño máximo de las cargas de solicitudes HTTP.

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
t2.micro.search	10 MiB
t2.small.search	10 MiB
t2.medium.search	10 MiB
t3.small.search	10 MiB
t3.medium.search	10 MiB
m3.medium.search	10 MiB
m3.large.search	10 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
m3.xlarge.search	100 MiB
m3.2xlarge.search	100 MiB
m4.large.search	10 MiB
m4.xlarge.search	100 MiB
m4.2xlarge.search	100 MiB
m4.4xlarge.search	100 MiB
m4.10xlarge.search	100 MiB
m5.large.search	10 MiB
m5.xlarge.search	100 MiB
m5.2xlarge.search	100 MiB
m5.4xlarge.search	100 MiB
m5.12xlarge.search	100 MiB
m6g.large.search	10 MiB
m6g.xlarge.search	100 MiB
m6g.2xlarge.search	100 MiB
m6g.4xlarge.search	100 MiB
m6g.8xlarge.search	100 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
m6g.12xlarge.search	100 MiB
c4.large.search	10 MiB
c4.xlarge.search	100 MiB
c4.2xlarge.search	100 MiB
c4.4xlarge.search	100 MiB
c4.8xlarge.search	100 MiB
c5.large.search	10 MiB
c5.xlarge.search	100 MiB
c5.2xlarge.search	100 MiB
c5.4xlarge.search	100 MiB
c5.9xlarge.search	100 MiB
c5.18xlarge.search	100 MiB
c6g.large.search	10 MiB
c6g.xlarge.search	100 MiB
c6g.2xlarge.search	100 MiB
c6g.4xlarge.search	100 MiB
c6g.8xlarge.search	100 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
c6g.12xlarge.search	100 MiB
r3.large.search	10 MiB
r3.xlarge.search	100 MiB
r3.2xlarge.search	100 MiB
r3.4xlarge.search	100 MiB
r3.8xlarge.search	100 MiB
r4.large.search	100 MiB
r4.xlarge.search	100 MiB
r4.2xlarge.search	100 MiB
r4.4xlarge.search	100 MiB
r4.8xlarge.search	100 MiB
r4.16xlarge.search	100 MiB
r5.large.search	100 MiB
r5.xlarge.search	100 MiB
r5.2xlarge.search	100 MiB
r5.4xlarge.search	100 MiB
r5.12xlarge.search	100 MiB
r6g.large.search	100 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
r6g.xlarge.search	100 MiB
r6g.2xlarge.search	100 MiB
r6g.4xlarge.search	100 MiB
r6g.8xlarge.search	100 MiB
r6g.12xlarge.search	100 MiB
r6gd.large.search	100 MiB
r6gd.xlarge.search	100 MiB
r6gd.2xlarge.search	100 MiB
r6gd.4xlarge.search	100 MiB
r6gd.8xlarge.search	100 MiB
r6gd.12xlarge.search	100 MiB
r6gd.16xlarge.search	100 MiB
i2.xlarge.search	100 MiB
i2.2xlarge.search	100 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
i3.large.search	100 MiB
i3.xlarge.search	100 MiB
i3.2xlarge.search	100 MiB
i3.4xlarge.search	100 MiB
i3.8xlarge.search	100 MiB
i3.16xlarge.search	100 MiB
or1.medium.search	10 MiB
or1.large.search	100 MiB
or1.xlarge.search	100 MiB
or1.2xlarge.search	100 MiB
or1.4xlarge.search	100 MiB
or1.8xlarge.search	100 MiB
or1.12xlarge.search	100 MiB
or1.16xlarge.search	100 MiB
im4gn.large.search	100 MiB
im4gn.xlarge.search	100 MiB

Tipo de instancia	Tamaño máximo de las cargas de solicitud HTTP
`im4gn.2xlarge.search`	100 MiB
`im4gn.4xlarge.search`	100 MiB
`im4gn.8xlarge.search`	100 MiB
`im4gn.16xlarge.search`	100 MiB

Cuotas de tamaño de la partición

En la siguiente sección, se enumeran los tamaños máximos de las particiones para varias familias de instancias.

Tipo de instancia	Multi-AZ sin modo de espera	Multi-AZ con modo de espera
R5, C5, M5	N/A	65 GiB
I3	N/A	65 GiB
R6g, C6g, M6g, R6gd	N/A	65 GiB
OR1	100 GiB	65 GiB
Im4gn	N/A	65 GiB

Para solicitar un aumento de cuota, póngase en contacto con AWS Support.

Cuota de procesamiento de Java

OpenSearch El servicio limita los procesos de Java a un tamaño de pila de 32 GiB. Los usuarios avanzados pueden especificar el porcentaje del montón usado para los datos de campo. Para más

información, consulte the section called “Configuración avanzada de clústeres” y the section called “OutOfMemoryError de JVM”.

Cuota de políticas de dominio

OpenSearch El servicio limita las políticas de acceso a los dominios a 100 KiB.

Instancias reservadas en Amazon OpenSearch Service

Las instancias reservadas (RI) en Amazon OpenSearch Service ofrecen descuentos importantes en comparación con las instancias bajo demanda. Las instancias en sí son idénticas; las instancias reservadas simplemente suponen que se aplica un descuento de facturación con respecto al uso de instancias bajo demanda en su cuenta. Para las aplicaciones de larga duración con un uso predecible, las instancias reservadas pueden proporcionar un ahorro considerable a lo largo del tiempo.

Las RI de OpenSearch Service requieren condiciones de uno o tres años y tienen tres opciones de pago que afectan a la tarifa de descuento:

- Sin pago inicial: no se paga nada por adelantado. Se paga una tarifa por hora con descuento por cada hora dentro del periodo estipulado.
- Pago inicial parcial: se paga una parte del costo por adelantado y después una tarifa por hora con descuento por cada hora dentro del periodo estipulado.
- Pago total anticipado: se paga la totalidad del costo por adelantado. No hay que pagar una tarifa por hora durante el periodo estipulado.

Por regla general, un pago inicial más grande significa un mayor descuento. Las instancias reservadas no se pueden cancelar: cuando se reservan, se compromete a pagar por el periodo completo, y los pagos iniciales no son reembolsables.

Las RI no son flexibles; solo se aplican al tipo de instancia exacto que se reserva. Por ejemplo, una reserva para ocho instancias `c5.2xlarge.search` no se aplica a dieciséis instancias `c5.xlarge.search` o cuatro instancias `c5.4xlarge.search`. Para obtener información completa, consulte Precios de Amazon OpenSearch Service y Preguntas frecuentes.

Temas

- Comprar instancias reservadas (consola)

- Comprar instancias reservadas (CLI de AWS)
- Comprar instancias reservadas (SDK de AWS)
- Examinar los costos

Comprar instancias reservadas (consola)

La consola le permite ver las instancias reservadas que tiene y adquirir otras nuevas.

Para comprar una reserva

1. Visite https://aws.amazon.com y, a continuación, elija Sign In to the Console (Inicie sesión en la consola).
2. En Analytics (Análisis), elija Amazon OpenSearch Service.
3. Elija Reserved Instance Leases (Asignaciones de instancias reservadas) en el panel de navegación.

   En esta página, puede ver la reservas que tiene. Si tiene muchas, puede filtrarlas para identificar y ver más fácilmente una reserva en concreto.

   > **Tip**
   >
   > Si no ve el enlace de Reserved Instances Leases (Asignaciones de instancias reservadas), cree un dominio en la Región de AWS.

4. Elija Order reserved instance (Pedir instancia reservada).
5. Proporcione un nombre único y descriptivo.
6. Elija un tipo de instancia y el número de instancias. Para obtener instrucciones, consulte the section called “Determinación del tamaño de dominios”.
7. Elija la duración del periodo y una opción de pago. Revise los datos de pago con cuidado.
8. Elija Next (Siguiente).
9. Revise el resumen de compra con cuidado. Las compras de instancias reservadas no son reembolsables.
10. Elija Order (Pedir).

Comprar instancias reservadas (CLI de AWS)

La AWS CLI tiene comandos para ver las ofertas, comprar una reserva y consultar las reservas que se tienen. El comando y la respuesta de muestra siguientes muestran las ofertas para una determinada Región de AWS:

```
aws opensearch describe-reserved-instance-offerings --region us-east-1
{
  "ReservedInstanceOfferings": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "UsagePrice": 0.0,
      "PaymentOption": "PARTIAL_UPFRONT",
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

Para ver una explicación de cada valor de retorno, consulte la tabla siguiente.

Campo	Descripción
`FixedPrice`	El costo inicial de la reserva.
`ReservedInstanceOfferingId`	El ID de la oferta. Anote este valor si desea reservar la oferta.
`RecurringCharges`	La tarifa por hora de la reserva.
`UsagePrice`	Campo heredado. Para OpenSearch Service, este valor siempre es 0.

Campo	Descripción
`PaymentOption`	No Upfront (Sin pago inicial), Partial Upfront (Pago inicial parcial) o All Upfront (Pago inicial total).
`Duration`	La duración en segundos: • 31536000 segundos equivale a un año. • 94608000 segundos equivale a tres años.
`InstanceType`	El tipo de instancia de la reserva. Para obtener información sobre los recursos de equipo que se asignan a cada tipo de instancia, consulte Precios de Amazon OpenSearch Service.
`CurrencyCode`	La divisa para `FixedPrice` y `RecurringChargeAmount`.

El siguiente ejemplo adquiere una reserva:

```
aws opensearch purchase-reserved-instance-offering --reserved-instance-offering-
id 1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a --reservation-name my-reservation --instance-
count 3 --region us-east-1
{
  "ReservationName": "my-reservation",
  "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a"
}
```

Por último, puede obtener una lista de las reservas para una región determinada mediante el siguiente ejemplo:

```
aws opensearch describe-reserved-instances --region us-east-1
{
  "ReservedInstances": [
    {
      "FixedPrice": x,
      "ReservedInstanceOfferingId": "1a2a3a4a5-1a2a-3a4a-5a6a-1a2a3a4a5a6a",
      "ReservationName": "my-reservation",
```

```
      "PaymentOption": "PARTIAL_UPFRONT",
      "UsagePrice": 0.0,
      "ReservedInstanceId": "9a8a7a6a-5a4a-3a2a-1a0a-9a8a7a6a5a4a",
      "RecurringCharges": [
        {
          "RecurringChargeAmount": y,
          "RecurringChargeFrequency": "Hourly"
        }
      ],
      "State": "payment-pending",
      "StartTime": 1522872571.229,
      "InstanceCount": 3,
      "Duration": 31536000,
      "InstanceType": "m4.2xlarge.search",
      "CurrencyCode": "USD"
    }
  ]
}
```

> **Note**
>
> `StartTime` se expresa en formato de tiempo Unix, que es el número de segundos que han transcurrido desde la medianoche UTC del 1 de enero de 1970. Por ejemplo, 1522872571 en formato de tiempo Unix son las 20:09:31 UTC del 4 de abril de 2018. Puede utilizar convertidores online.

Para obtener más información acerca de los comandos utilizados en los ejemplos anteriores, consulte la Referencia de comandos de la AWS CLI.

Comprar instancias reservadas (SDK de AWS)

Los AWS SDK (excepto los SDK de Android e iOS) admiten todas las operaciones definidas en la Referencia de la API de configuración de Amazon OpenSearch Service, incluidas las siguientes:

- `DescribeReservedInstanceOfferings`
- `PurchaseReservedInstanceOffering`
- `DescribeReservedInstances`

En este ejemplo de script se utiliza el cliente Python de bajo nivel OpenSearchService desde AWS SDK for Python (Boto3) para adquirir instancias reservadas. Se debe proporcionar un valor para `instance_type`.

```
import boto3
from botocore.config import Config

# Build the client using the default credential configuration.
# You can use the CLI and run 'aws configure' to set access key, secret
# key, and default region.

my_config = Config(
    # Optionally lets you specify a region other than your default.
    region_name='us-east-1'
)

client = boto3.client('opensearch', config=my_config)

instance_type = '' # e.g. m4.2xlarge.search


def describe_RI_offerings(client):
    """Gets the Reserved Instance offerings for this account"""

    response = client.describe_reserved_instance_offerings()
    offerings = (response['ReservedInstanceOfferings'])
    return offerings


def check_instance(offering):
    """Returns True if instance type is the one you specified above"""

    if offering['InstanceType'] == instance_type:
        return True

    return False


def get_instance_id():
    """Iterates through the available offerings to find the ID of the one you
 specified"""

    instance_type_iterator = filter(
```

```
        check_instance, describe_RI_offerings(client))
    offering = list(instance_type_iterator)
    id = offering[0]['ReservedInstanceOfferingId']
    return id


def purchase_RI_offering(client):
    """Purchase Reserved Instances"""

    response = client.purchase_reserved_instance_offering(
        ReservedInstanceOfferingId = get_instance_id(),
        ReservationName = 'my-reservation',
        InstanceCount = 1
    )
    print('Purchased reserved instance offering of type ' + instance_type)
    print(response)


def main():
    """Purchase Reserved Instances"""
    purchase_RI_offering(client)
```

Para obtener más información acerca de cómo instalar y utilizar los SDK de AWS, consulte los Kits de desarrollo de software de AWS.

Examinar los costos

Cost Explorer es una herramienta gratuita que puede utilizar para ver sus datos de gasto de los últimos 13 meses. El análisis de estos datos le ayuda a identificar tendencias y a comprender si las instancias reservadas se adaptan a su caso de uso. Si ya tiene RI, puede agrupar por Purchase Option (Opción de compra) y mostrar los costos amortizados para comparar ese gasto con su gasto en instancias bajo demanda. También puede definir presupuestos de utilización para asegurarse de que aprovecha al máximo sus reservas. Para obtener más información, consulte Análisis de los costos con Cost Explorer en la Guía del usuario de AWS Billing.

Otros recursos compatibles en Amazon OpenSearch Service

En este tema se describen los recursos adicionales compatibles con Amazon OpenSearch Service.

bootstrap.memory_lock

OpenSearch El servicio se activa `bootstrap.memory_lock`opensearch.`yml`, lo que bloquea la memoria de la JVM e impide que el sistema operativo la cambie al disco. Esto se aplica a todos los tipos de instancias admitidos excepto a los siguientes:

- `t2.micro.search`
- `t2.small.search`
- `t2.medium.search`
- `t3.small.search`
- `t3.medium.search`

Módulo de scripting

OpenSearch El servicio admite la creación de scripts para Elasticsearch 5. x y dominios posteriores. No admite scripting para las versiones 1.5 o 2.3.

Las opciones de scripting admitidas incluyen lo siguiente:

- Painless
- Lucene Expressions
- Mustache

Para los dominios de Elasticsearch 5.5 y versiones posteriores, y para todos los OpenSearch dominios, OpenSearch Service admite los scripts almacenados mediante el `_scripts` punto final. Los dominios de Elasticsearch 5.3 y 5.1 solo admiten scripts incorporados.

Transporte TLS

OpenSearch El servicio admite HTTP en el puerto 80 y HTTPS en el puerto 443, pero no admite el transporte TLS.

Tutoriales de Amazon OpenSearch Service

Este capítulo incluye varios tutoriales completos para trabajar con Amazon OpenSearch Service, incluyendo cómo migrar al servicio, crear una aplicación de búsqueda simple y crear una visualización en OpenSearch Dashboards.

Temas

- Tutorial: Creación y búsqueda de documentos en Amazon OpenSearch Service
- Tutorial: Migración a Amazon OpenSearch Service
- Tutorial: Creación de una aplicación de búsqueda con Amazon OpenSearch Service
- Tutorial: Visualización de llamadas de soporte al cliente con OpenSearch Service y OpenSearch Dashboards

Tutorial: Creación y búsqueda de documentos en Amazon OpenSearch Service

En este tutorial, aprenderá a crear y buscar un documento en Amazon OpenSearch Service. Agregue datos a un índice en forma de documento JSON. OpenSearch Service crea un índice alrededor del primer documento que agrega.

Este tutorial explica cómo llevar a cabo solicitudes HTTP para crear documentos, generar automáticamente un ID para un documento y hacer búsquedas básicas y avanzadas en los documentos.

> **Note**
>
> En este tutorial, se utiliza un dominio de acceso abierto. Para obtener el máximo nivel de seguridad, es recomendable que coloque su dominio dentro de una nube privada virtual (VPC).

Requisitos previos

Este tutorial tiene los requisitos previos siguientes:

- Debe tener una Cuenta de AWS.
- Debe tener un dominio de OpenSearch Service activo.

Adición de un documento a un índice

Para agregar un documento a un índice, puede utilizar cualquier herramienta HTTP, como Postman, cURL o la consola de paneles de OpenSearch. En estos ejemplos, se supone que está utilizando la consola para desarrolladores en los paneles de OpenSearch. Si utiliza una herramienta diferente, ajústela según corresponda proporcionando la URL completa y las credenciales, si es necesario.

Para agregar un documento a un índice

1. Desplácese hasta la URL de OpenSearch Dashboards para su dominio. Puede encontrar la URL en el panel del dominio en la consola de OpenSearch Service. La URL tiene este formato:

   ```
   domain-endpoint/_dashboards/
   ```

2. Inicie sesión con su nombre de usuario y contraseña principales.
3. Abra el panel de navegación izquierdo y elija Herramientas para desarrolladores.
4. El verbo HTTP para crear un nuevo recurso es PUT, que es lo que se utiliza para crear un nuevo documento e índice. Ingrese el siguiente comando en la consola:

   ```
   PUT fruit/_doc/1
   {
     "name":"strawberry",
     "color":"red"
   }
   ```

   La solicitud PUT crea un índice llamado fruit (fruta) y agrega un solo documento al índice con un ID de 1. Produce la siguiente respuesta:

   ```
   {
     "_index" : "fruit",
     "_type" : "_doc",
     "_id" : "1",
     "_version" : 1,
     "result" : "created",
     "_shards" : {
       "total" : 2,
   ```

```
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Creación de ID de generación automática

OpenSearch Service puede generar automáticamente un ID para sus documentos. El comando para generar ID utiliza una solicitud POST en lugar de una solicitud PUT y no requiere ningún ID de documento (en comparación con la solicitud anterior).

Ingrese la siguiente solicitud en la consola para desarrolladores:

```
POST veggies/_doc
{
  "name":"beet",
  "color":"red",
  "classification":"root"
}
```

Esta solicitud crea un índice denominado veggies (verduras) y agrega el documento al índice. Produce la siguiente respuesta:

```
{
  "_index" : "veggies",
  "_type" : "_doc",
  "_id" : "3WgyS4IB5DLqbRIvLxtF",
  "_version" : 1,
  "result" : "created",
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 0,
  "_primary_term" : 1
}
```

Tenga en cuenta el campo `_id` adicional de la respuesta, que indica que se creó un ID automáticamente.

> **Note**
>
> No proporcione nada después de `_doc` en la URL, donde normalmente va el ID. Como va a crear un documento con un ID generado, aún no debe proporcionar uno. Eso está reservado para actualizaciones.

Actualización de un documento con un comando POST

Para actualizar un documento, se utiliza un comando `POST` de HTTP con el número de ID.

En primer lugar, cree un documento con un ID de `42`:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow"
}
```

A continuación, utilice ese ID para actualizar el documento:

```
POST fruits/_doc/42
{
  "name":"banana",
  "color":"yellow",
  "classification":"berries"
}
```

Este comando actualiza el documento con el nuevo campo `classification`. Produce la siguiente respuesta:

```
{
  "_index" : "fruits",
  "_type" : "_doc",
  "_id" : "42",
  "_version" : 2,
  "result" : "updated",
  "_shards" : {
```

```
    "total" : 2,
    "successful" : 2,
    "failed" : 0
  },
  "_seq_no" : 1,
  "_primary_term" : 1
}
```

> **Note**
>
> Si intenta actualizar un documento que no existe, OpenSearch Service crea el documento.

Ejecución de acciones por lotes

Puede utilizar la operación de la API de `POST _bulk` para llevar a cabo varias acciones en uno o más índices en una solicitud. Los comandos de acción por lotes tienen el siguiente formato:

```
POST /_bulk
<action_meta>\n
<action_data>\n
<action_meta>\n
<action_data>\n
```

Cada acción requiere dos líneas de JSON. Primero, debe proporcionar la descripción de la acción o los metadatos. En la línea siguiente, debe proporcionar los datos. Cada parte está separada por una nueva línea (\n). La descripción de una acción de una inserción podría verse de la siguiente manera:

```
{ "create" : { "_index" : "veggies", "_type" : "_doc", "_id" : "7" } }
```

La línea siguiente que contiene los datos podría verse de la siguiente manera:

```
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

En conjunto, los metadatos y los datos representan una sola acción en una operación masiva. Puede llevar a cabo muchas operaciones en una sola solicitud, como esta:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "35" } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
```

```
{ "create" : { "_index" : "veggies", "_id" : "36" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "37" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "38" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "39" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
{ "delete" : { "_index" : "vegetables", "_id" : "1" } }
```

Observe que la última acción es `delete`. No hay datos después de la acción `delete`.

Búsqueda de documentos

Ya que existen datos en el clúster, puede buscarlos. Por ejemplo, es posible que quiera buscar todos los tubérculos, obtener un recuento de todos los vegetales de hoja verde o encontrar la cantidad de errores registrados por hora.

Búsquedas básicas

Una búsqueda básica tiene un aspecto similar a este:

```
GET veggies/_search?q=name:l*
```

La solicitud produce una respuesta JSON que contiene el documento de lechuga.

Búsquedas avanzadas

Puede hacer búsquedas más avanzadas si proporciona las opciones de consulta como JSON en el cuerpo de la solicitud:

```
GET veggies/_search
{
  "query": {
    "term": {
      "name": "lettuce"
    }
  }
}
```

Este ejemplo también produce una respuesta JSON con el documento de lechuga.

Ordenar

Puede llevar a cabo más consultas de este tipo mediante la acción de ordenar. En primer lugar, debe volver a crear el índice porque la asignación automática de campos eligió tipos que no se pueden ordenar de forma predeterminada. Envíe las siguientes solicitudes para eliminar y volver a crear el índice:

```
DELETE /veggies

PUT /veggies
{
   "mappings":{
      "properties":{
         "name":{
            "type":"keyword"
         },
         "color":{
            "type":"keyword"
         },
         "classification":{
            "type":"keyword"
         }
      }
   }
}
```

A continuación, rellene el índice con datos:

```
POST /_bulk
{ "create" : { "_index" : "veggies", "_id" : "7"  } }
{ "name":"kale", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "8" } }
{ "name":"spinach", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "9" } }
{ "name":"arugula", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "10" } }
{ "name":"endive", "color":"green", "classification":"leafy-green" }
{ "create" : { "_index" : "veggies", "_id" : "11" } }
{ "name":"lettuce", "color":"green", "classification":"leafy-green" }
```

Ya puede buscar con un orden. Esta solicitud agrega un orden ascendente por clasificación:

```
GET veggies/_search
{
```

```
  "query" : {
    "term": { "color": "green" }
  },
  "sort" : [
      "classification"
  ]
}
```

Recursos relacionados

Para obtener más información, consulte los siguientes recursos:

- Introducción
- Indexación de datos
- Buscar datos

Tutorial: Migración a Amazon OpenSearch Service

Las instantáneas de índice son una forma popular de migrar desde un clúster de OpenSearch autoadministrado o Elasticsearch heredado a Amazon OpenSearch Service. En términos generales, el proceso consta de los siguientes pasos:

1. Tome una instantánea del clúster existente y cargue la instantánea en un bucket de Amazon S3.
2. Cree un dominio de OpenSearch Service.
3. Conceda permisos a OpenSearch Service para acceder al bucket, y asegúrese de disponer de permisos para trabajar con instantáneas.
4. Restaure la instantánea en el dominio de OpenSearch Service.

Este tutorial proporciona pasos más detallados y opciones alternativas, cuando corresponda.

Tomar y cargar la instantánea

Aunque puede utilizar el complemento repository-s3 para tomar instantáneas directamente a S3, tiene que instalar el complemento en cada nodo, ajustar `opensearch.yml` (o `elasticsearch.yml` si usa un clúster Elasticsearch), reiniciar cada nodo, agregar sus credenciales de AWS y, finalmente, tomar la instantánea. El complemento es una gran opción para uso continuo o para migrar clústeres más grandes.

En clústeres más pequeños, un enfoque único consiste en tomar una instantánea del sistema de archivos compartida y, luego, utilizar la AWS CLI para cargarla a S3. Si ya tiene una instantánea, vaya al paso 4.

Para tomar una instantánea y cargarla a Amazon S3

1. Agregue la configuración `path.repo` a `opensearch.yml` (o `Elasticsearch.yml`) en todos los nodos y, a continuación, reinicie cada nodo.

   ```
   path.repo: ["/my/shared/directory/snapshots"]
   ```

2. Registre un repositorio de instantáneas, necesario antes de tomar una instantánea. Un repositorio es solo una ubicación de almacenamiento: un sistema de archivos compartido, Amazon S3, un sistema de archivos distribuido de Hadoop (HDFS), etc. En este caso, utilizaremos un sistema de archivos compartido (“fs”):

   ```
   PUT _snapshot/my-snapshot-repo-name
   {
     "type": "fs",
     "settings": {
       "location": "/my/shared/directory/snapshots"
     }
   }
   ```

3. Tomar la instantánea:

   ```
   PUT _snapshot/my-snapshot-repo-name/my-snapshot-name
   {
     "indices": "migration-index1,migration-index2,other-indices-*",
     "include_global_state": false
   }
   ```

4. Instale la AWS CLI y ejecute `aws configure` para agregar sus credenciales.

5. Desplácese hasta el directorio de instantáneas. A continuación, ejecute los siguientes comandos para crear un nuevo bucket de S3 y cargar el contenido del directorio de instantáneas en ese bucket:

   ```
   aws s3 mb s3://bucket-name --region us-west-2
   aws s3 sync . s3://bucket-name --sse AES256
   ```

En función del tamaño de la instantánea y la velocidad de su conexión a internet, esta operación puede tardar un tiempo.

Crear un dominio

Aunque la consola es la forma más fácil de crear un dominio, en este caso, ya tiene el terminal abierto y la AWS CLI instalada. Modifique el siguiente comando para crear un dominio que se ajuste a sus necesidades:

```
aws opensearch create-domain \
  --domain-name migration-domain \
  --engine-version OpenSearch_1.0 \
  --cluster-config InstanceType=c5.large.search,InstanceCount=2 \
  --ebs-options EBSEnabled=true,VolumeType=gp2,VolumeSize=100 \
  --node-to-node-encryption-options Enabled=true \
  --encryption-at-rest-options Enabled=true \
  --domain-endpoint-options EnforceHTTPS=true,TLSSecurityPolicy=Policy-Min-
TLS-1-2-2019-07 \
  --advanced-security-options
 Enabled=true,InternalUserDatabaseEnabled=true,MasterUserOptions='{MasterUserName=master-
user,MasterUserPassword=master-user-password}' \
  --access-policies '{"Version":"2012-10-17","Statement":
[{"Effect":"Allow","Principal":{"AWS":["*"]},"Action":
["es:ESHttp*"],"Resource":"arn:aws:es:us-west-2:123456789012:domain/migration-domain/
*"}]}' \
  --region us-west-2
```

Tal como está, el comando crea un dominio accesible a Internet con dos nodos de datos, cada uno con 100 GiB de almacenamiento. También habilita el control de acceso detallado con autenticación básica HTTP y toda la configuración de cifrado. Utilice la consola de OpenSearch Service si necesita una configuración de seguridad más avanzada, como una VPC.

Antes de ejecutar el comando, cambie el nombre de dominio, las credenciales del usuario maestro y el número de cuenta. Especifique la misma Región de AWS que utilizó para el bucket de S3 y una versión de OpenSearch/Elasticsearch que sea compatible con la instantánea.

> **Important**
>
> Las instantáneas solo son compatibles con versiones posteriores y solo con una versión principal. Por ejemplo, no puede restaurar una instantánea desde un clúster OpenSearch

1.x en un clúster Elasticsearch 7.x, solo un clúster OpenSearch 1.x o 2.x. La versión secundaria también importa. No se puede restaurar una instantánea desde un clúster 5.3.3 autoadministrado en un dominio de OpenSearch Service 5.3.2. Recomendamos elegir la versión más reciente de OpenSearch o Elasticsearch que admita la instantánea. Para obtener una tabla de versiones compatibles, consulte the section called “Uso de una instantánea para migrar datos”.

Conceda permisos al bucket de S3.

En la consola AWS Identity and Access Management (IAM), cree un rol con los siguientes permisos y relación de confianza. Al crear un rol, elija S3 como el Servicio de AWS. Asigne al rol el nombre `OpenSearchSnapshotRole` para que sea fácil de encontrar.

Permisos

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

Relación de confianza

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

Después, conceda permisos a su rol de IAM personal para asumir `OpenSearchSnapshotRole`. Cree la siguiente política y adjúntela a su identidad.

Permisos

```
{
  "Version": "2012-10-17",
  "Statement": [{
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
    }
  ]
}
```

Asigne el rol de instantánea en OpenSearch Dashboards (si utiliza el control de acceso detallado)

Si ha habilitado el control de acceso detallado, incluso si utiliza autenticación HTTP básica para todos los demás fines, debe asignar el rol `manage_snapshots` al rol de IAM para poder trabajar con instantáneas.

Para otorgar permisos a la identidad a fin de trabajar con instantáneas

1. Inicie sesión en el panel con las credenciales de usuario maestro que especificó al crear el dominio de OpenSearch Service. Puede encontrar la URL del panel en la consola de OpenSearch Service. Adopta el formato `https://domain-endpoint/_dashboards/`.

2. En el menú principal, elija Seguridad, Roles y seleccione el rol manage_snapshots.
3. Elija Usuarios asignados, Administrar mapeo.
4. Agregue el ARN del dominio de su rol de IAM personal en el campo apropiado. El ARN está en uno de los siguientes formatos:

```
arn:aws:iam::123456789123:user/user-name
```

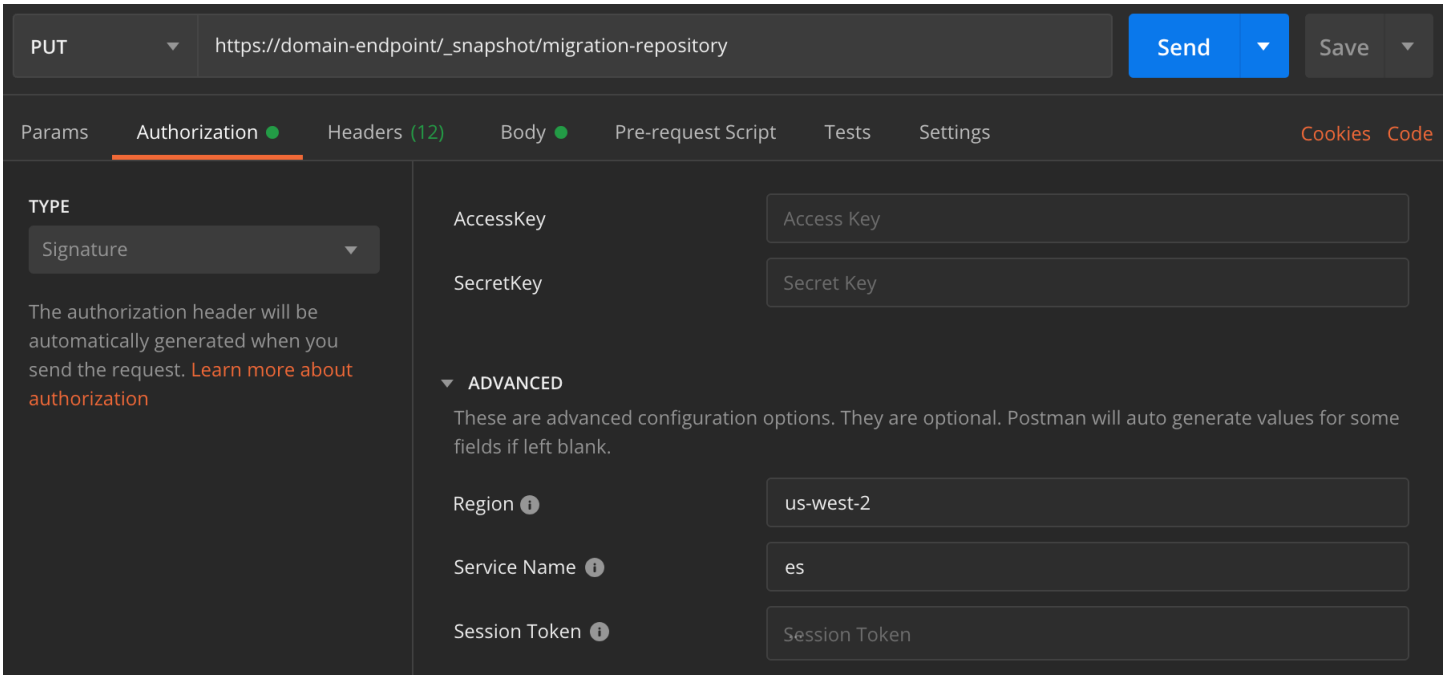
```
arn:aws:iam::123456789123:role/role-name
```

5. Seleccione Asignar y confirme que el rol aparece en Usuarios asignados.

Restaurar la instantánea

En este punto, tiene dos formas de acceder a su dominio de OpenSearch Service: la autenticación básica HTTP con sus credenciales de usuario maestro o la autenticación de AWS con las credenciales de IAM. Dado que las instantáneas utilizan Amazon S3, que no tiene un concepto de usuario maestro, debe utilizar sus credenciales de IAM para registrar el repositorio de instantáneas en su dominio de OpenSearch Service.

La mayoría de los lenguajes de programación tienen bibliotecas para ayudar con las solicitudes de firma, pero el enfoque más simple es utilizar una herramienta como Postman y poner sus credenciales de IAM en la sección Autorización.



Para restaurar la instantánea

1. Independientemente de cómo elija firmar sus solicitudes, el primer paso es registrar el repositorio:

```
PUT _snapshot/my-snapshot-repo-name
{
  "type": "s3",
  "settings": {
    "bucket": "bucket-name",
    "region": "us-west-2",
    "role_arn": "arn:aws:iam::123456789012:role/OpenSearchSnapshotRole"
  }
}
```

2. A continuación, enumere las instantáneas en el repositorio y busque la que desea restaurar. En este punto, puede continuar utilizando Postman o cambiar a una herramienta como curl.

   Abreviado

```
GET _snapshot/my-snapshot-repo-name/_all
```

   curl

```
curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/_all
```

3. Restaurare la instantánea.

   Abreviado

```
POST _snapshot/my-snapshot-repo-name/my-snapshot-name/_restore
{
  "indices": "migration-index1,migration-index2,other-indices-*",
  "include_global_state": false
}
```

   curl

```
curl -XPOST -u 'master-user:master-user-password' https://domain-endpoint/
_snapshot/my-snapshot-repo-name/my-snapshot-name/_restore \
```

```
  -H 'Content-Type: application/json' \
  -d '{"indices":"migration-index1,migration-index2,other-indices-
*","include_global_state":false}'
```

4. Finalmente, verifique que sus índices se restablecieron como se esperaba.

   Abreviado

   ```
   GET _cat/indices?v
   ```

   curl

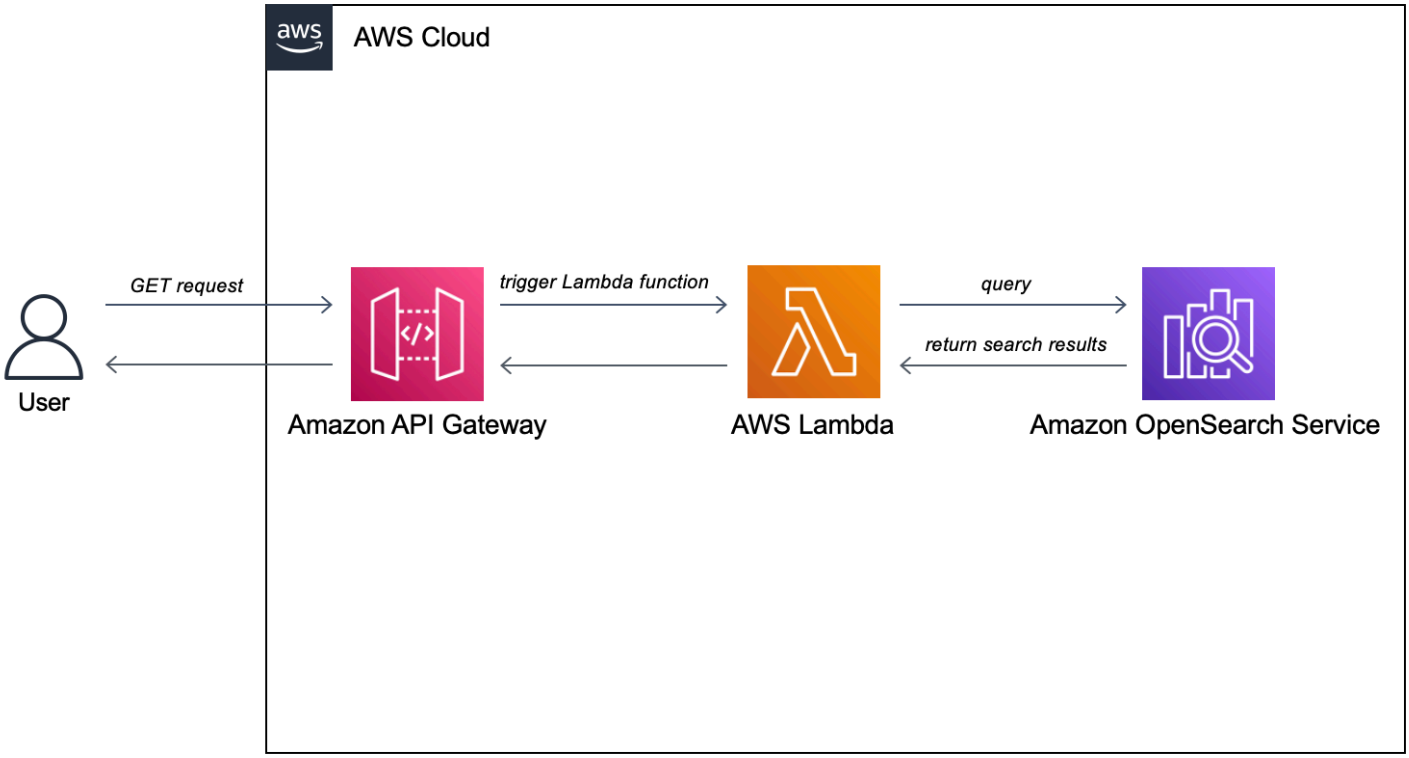
   ```
   curl -XGET -u 'master-user:master-user-password' https://domain-endpoint/_cat/
   indices?v
   ```

En este punto, la migración está completa. Puede configurar sus clientes para que utilicen el nuevo punto de conexión de OpenSearch Service, cambiar el tamaño del dominio para adaptarse a su carga de trabajo, comprobar el recuento de particiones de sus índices, cambiar a un usuario maestro de IAM o comenzar a crear visualizaciones en OpenSearch Dashboards.

Tutorial: Creación de una aplicación de búsqueda con Amazon OpenSearch Service

Una forma común para crear una aplicación de búsqueda con Amazon OpenSearch Service es utilizar formularios web para enviar consultas de usuarios a un servidor. A continuación, puede autorizar el servidor para llamar a las API de OpenSearch Service directamente y que el servidor envíe solicitudes a OpenSearch Service. Pero si desea escribir un código del lado del cliente que no dependa de un servidor, debe compensar los riesgos de seguridad y rendimiento. Permitir acceso público sin firma a las API de OpenSearch es inadmisible. Los usuarios pueden acceder a puntos de conexión no protegidos o influir en el rendimiento del clúster a través de consultas demasiado complejas (o demasiadas consultas).

Este capítulo se presenta una solución: utilizar Amazon API Gateway para restringir a los usuarios un subconjunto de API de OpenSearch y que AWS Lambda firme solicitudes de API Gateway a OpenSearch Service.



> **Note**
>
> Se aplican precios estándar de API Gateway y Lambda, pero dentro del uso limitado de este tutorial, los costos deben ser insignificantes.

Requisitos previos

Un requisito previo para este tutorial es un dominio de OpenSearch Service. Si todavía no tiene uno, siga los pasos de Creación de un dominio de OpenSearch Service para crear uno.

Paso 1: Indexe los datos de muestra

Descargue sample-movies.zip, descomprímalo y utilice la operación _bulk de la API para agregar 5000 documentos al índice `movies`:

```
POST https://search-my-domain.us-west-1.es.amazonaws.com/_bulk
{ "index": { "_index": "movies", "_id": "tt1979320" } }
{"directors":["Ron
 Howard"],"release_date":"2013-09-02T00:00:00Z","rating":8.3,"genres":
```

```
["Action","Biography","Drama","Sport"],"image_url":"http://ia.media-imdb.com/images/
M/MV5BMTQyMDE0MTY0OV5BMl5BanBnXkFtZTcwMjI2OTI0OQ@@._V1_SX400_.jpg","plot":"A re-
creation of the merciless 1970s rivalry between Formula One rivals James Hunt and
 Niki Lauda.","title":"Rush","rank":2,"running_time_secs":7380,"actors":["Daniel
 Brühl","Chris Hemsworth","Olivia Wilde"],"year":2013,"id":"tt1979320","type":"add"}
{ "index": { "_index": "movies", "_id": "tt1951264" } }
{"directors":["Francis Lawrence"],"release_date":"2013-11-11T00:00:00Z","genres":
["Action","Adventure","Sci-Fi","Thriller"],"image_url":"http://ia.media-imdb.com/
images/M/
MV5BMTAyMjQ3OTAxMzNeQTJeQWpwZ15BbWU4MDU0NzA1MzAx._V1_SX400_.jpg","plot":"Katniss
 Everdeen and Peeta Mellark become targets of the Capitol after
 their victory in the 74th Hunger Games sparks a rebellion in
 the Districts of Panem.","title":"The Hunger Games: Catching
 Fire","rank":4,"running_time_secs":8760,"actors":["Jennifer Lawrence","Josh
 Hutcherson","Liam Hemsworth"],"year":2013,"id":"tt1951264","type":"add"}
...
```

Tenga en cuenta que lo anterior es un comando de ejemplo con un pequeño subconjunto de datos disponibles. Para realizar la operación `_bulk`, debe copiar y pegar todo el contenido del archivo `sample-movies`. Para obtener más instrucciones, consulte the section called “Opción 2: cargar varios documentos”.

También puede utilizar el siguiente comando curl para conseguir el mismo resultado:

```
curl -XPOST -u 'master-user:master-user-password' 'domain-endpoint/_bulk' --data-binary
 @bulk_movies.json -H 'Content-Type: application/json'
```

Paso 2: Cree e implemente una función de Lambda

Antes de crear su API en API Gateway, cree la función de Lambda a la que pasa las solicitudes.

Crear la función de Lambda

En esta solución, API Gateway pasa solicitudes a una función de Lambda, que consulta OpenSearch Service y devuelve los resultados. Dado que esta función de ejemplo utiliza bibliotecas externas, debe crear un paquete de implementación y cargarlo en Lambda.

Creación del paquete de implementación

1. Abra un símbolo del sistema y cree un directorio del proyecto `my-opensearch-function`. Por ejemplo, en macOS:

```
mkdir my-opensearch-function
```

2. Desplácese hasta el directorio del proyecto `my-sourcecode-function`.

```
cd my-opensearch-function
```

3. Copie el contenido del siguiente código Python de ejemplo y guárdelo en un nuevo archivo denominado `opensearch-lambda.py`. Añada su región y el punto de conexión del host al archivo.

```
import boto3
import json
import requests
from requests_aws4auth import AWS4Auth

region = '' # For example, us-west-1
service = 'es'
credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

host = '' # The OpenSearch domain endpoint with https:// and without a trailing
 slash
index = 'movies'
url = host + '/' + index + '/_search'

# Lambda execution starts here
def lambda_handler(event, context):

    # Put the user query into the query DSL for more accurate search results.
    # Note that certain fields are boosted (^).
    query = {
        "size": 25,
        "query": {
            "multi_match": {
                "query": event['queryStringParameters']['q'],
                "fields": ["title^4", "plot^2", "actors", "directors"]
            }
        }
    }

    # Elasticsearch 6.x requires an explicit Content-Type header
```

```
    headers = { "Content-Type": "application/json" }

    # Make the signed HTTP request
    r = requests.get(url, auth=awsauth, headers=headers, data=json.dumps(query))

    # Create the response and add some extra content to support CORS
    response = {
        "statusCode": 200,
        "headers": {
            "Access-Control-Allow-Origin": '*'
        },
        "isBase64Encoded": False
    }

    # Add the search results to the response
    response['body'] = r.text
    return response
```

4. Instale las bibliotecas externas en un nuevo directorio `package`.

```
pip3 install --target ./package boto3
pip3 install --target ./package requests
pip3 install --target ./package requests_aws4auth
```

5. Cree un paquete de implementación con las bibliotecas instaladas en la raíz. El siguiente comando genera un archivo `my-deployment-package.zip` en el directorio de su proyecto.

```
cd package
zip -r ../my-deployment-package.zip .
```

6. Agregue el archivo `opensearch-lambda.py` a la raíz del archivo zip.

```
cd ..
zip my-deployment-package.zip opensearch-lambda.py
```

Para obtener más información sobre cómo crear funciones de Lambda y paquetes de implementación, consulte Implementar funciones de Lambda de Python con archivos .zip en la Guía para desarrolladores de AWS Lambda y the section called “Crear el paquete de implementación de Lambda” en esta guía.

Para crear la función usando la consola de Lambda

1. Navegue hasta la consola de Lambda en https://console.aws.amazon.com/lambda/home. En el panel de navegación izquierdo, elija Funciones.
2. Seleccione Crear función.
3. Configure los siguientes campos:

   - Nombre de función: opensearch-function
   - Tiempo de ejecución: Python 3.9
   - Arquitectura: x86_64

   Mantenga todas las demás opciones predeterminadas y elija Crear función.
4. En la sección Código fuente de la página de resumen de la función, seleccione el menú desplegable Cargar desde y seleccione el archivo .zip. Busque el archivo `my-deployment-package.zip` que ha creado y seleccione Guardar.
5. El controlador es el método de su código de función que procesa eventos. En Configuración de tiempo de ejecución, elija Editar y cambie el nombre del controlador de acuerdo con el nombre del archivo en el paquete de implementación donde se encuentra la función de Lambda. Como el archivo se denomina `opensearch-lambda.py`, cambie el nombre del controlador a *`opensearch-lambda`*`.lambda_handler`. Para más información, consulte controlador de función de Lambda en Python.

Paso 3: Cree la API en API Gateway

Usar API Gateway le permite crear una API más limitada y simplifica el proceso de interactuar con la API `_search` de OpenSearch. API Gateway le permite habilitar las características de seguridad, como la autenticación de Amazon Cognito y la limitación controlada. Realice los siguientes pasos para crear e implementar una API:

Crear y configurar la API

Para crear una API mediante la consola de API Gateway

1. Nave hasta la consola de API Gateway en https://console.aws.amazon.com/apigateway/home. En el panel de navegación izquierdo, seleccione APIs.
2. Localice API de REST (no privado) y elija Crear.
3. En la siguiente página, busque la sección Crear nueva API y asegúrese de que Nueva API esté seleccionada.

4. Configure los siguientes campos:
   - Nombre de la API: opensearch-api
   - Descripción: API pública para buscar un dominio de Amazon OpenSearch Service
   - Tipo de punto de conexión: Regional
5. Elija Crear API.
6. Elija Acciones y Crear método.
7. Seleccione GET (Obtener) en el menú desplegable y haga clic en la marca de verificación para confirmar.
8. Configure los siguientes ajustes y, a continuación, elija Guardar:

Opción	Valor
Tipo de integración	Función de Lambda
Usar integración de proxy de Lambda	Sí
Región de Lambda	*us-west-1*
Función de Lambda	`opensearch-lambda`
Usar tiempo de espera predeterminado	Sí

Configurar la solicitud de método

Elija Solicitud de método y configure los siguientes ajustes:

Opción	Valor
Autorización	NONE
Validador de solicitud	Validar parámetros de cadena de consulta y encabezados
Clave de API requerida	falso

En Parámetros de cadena de consulta de URL, seleccione Añadir cadena de consulta y configure el siguiente parámetro:

Opción	Valor
Nombre	q
Obligatoria	Sí

Implemente la API y configure una etapa

La consola de API Gateway le permite implementar una API creando una implementación y asociándola a una etapa nueva o una existente.

1. Elija Acciones e Implementar API.
2. Para Etapa de implementación elija Nueva etapa y nombre la etapa `opensearch-api-test`.
3. Elija Implementar.
4. Configure los siguientes ajustes en el editor de etapas y, a continuación, elija Guardar los cambios:

Opción	Valor
Habilitar limitación controlada	Sí
Tarifa	1 000
Ráfagas	500

Estos ajustes configuran una API que solo tiene un método: una solicitud `GET` al punto de conexión raíz (`https://`*`some-id`*`.execute-api.`*`us-west-1`*`.amazonaws.com/search-es-api-test`). La solicitud requiere un solo parámetro (q), la cadena de consulta que se busca. Cuando se llama, el método pasa la solicitud a Lambda, que ejecuta la función `opensearch-lambda`. Para más información, consulte Creación de una API en Amazon API Gateway e Implementación de una API de REST en Amazon API Gateway.

Paso 4: (Opcional) Modificar la política de acceso a dominios

Su dominio de OpenSearch Service debe permitir a la función de Lambda realizar solicitudes `GET` en el índice `movies`. Si su dominio tiene una política de acceso abierto con control de acceso detallado habilitado, puede dejarlo tal cual:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
      "Action": "es:*",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/*"
    }
  ]
}
```

Como alternativa, puede elegir hacer su política de acceso a dominio más detallada. Por ejemplo, la siguiente política mínima proporciona acceso de lectura a `opensearch-lambda-role` (creado a través de Lambda) al índice `movies`. Para obtener el nombre exacto del rol que Lambda crea automáticamente, vaya a la consola de AWS Identity and Access Management (IAM), elija Roles, y busque “Lambda”.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/service-role/opensearch-lambda-
role-1abcdefg"
      },
      "Action": "es:ESHttpGet",
      "Resource": "arn:aws:es:us-west-1:123456789012:domain/domain-name/movies/_search"
    }
  ]
}
```

> **Important**
>
> Si tiene habilitado un control de acceso detallado para el dominio, también deberá que asignar el rol a un usuario en OpenSearch Dashboards; de lo contrario, verá errores de permisos.

Para obtener más información sobre las políticas de acceso, consulte the section called “Configurar políticas de acceso”.

Asigne el rol de Lambda (si utiliza un control de acceso detallado)

El control de acceso detallado presenta un paso adicional antes de poder probar la aplicación. Incluso si utiliza la autenticación básica HTTP para todos los demás fines, es necesario asignar el rol de Lambda a un usuario, de lo contrario verá errores de permisos.

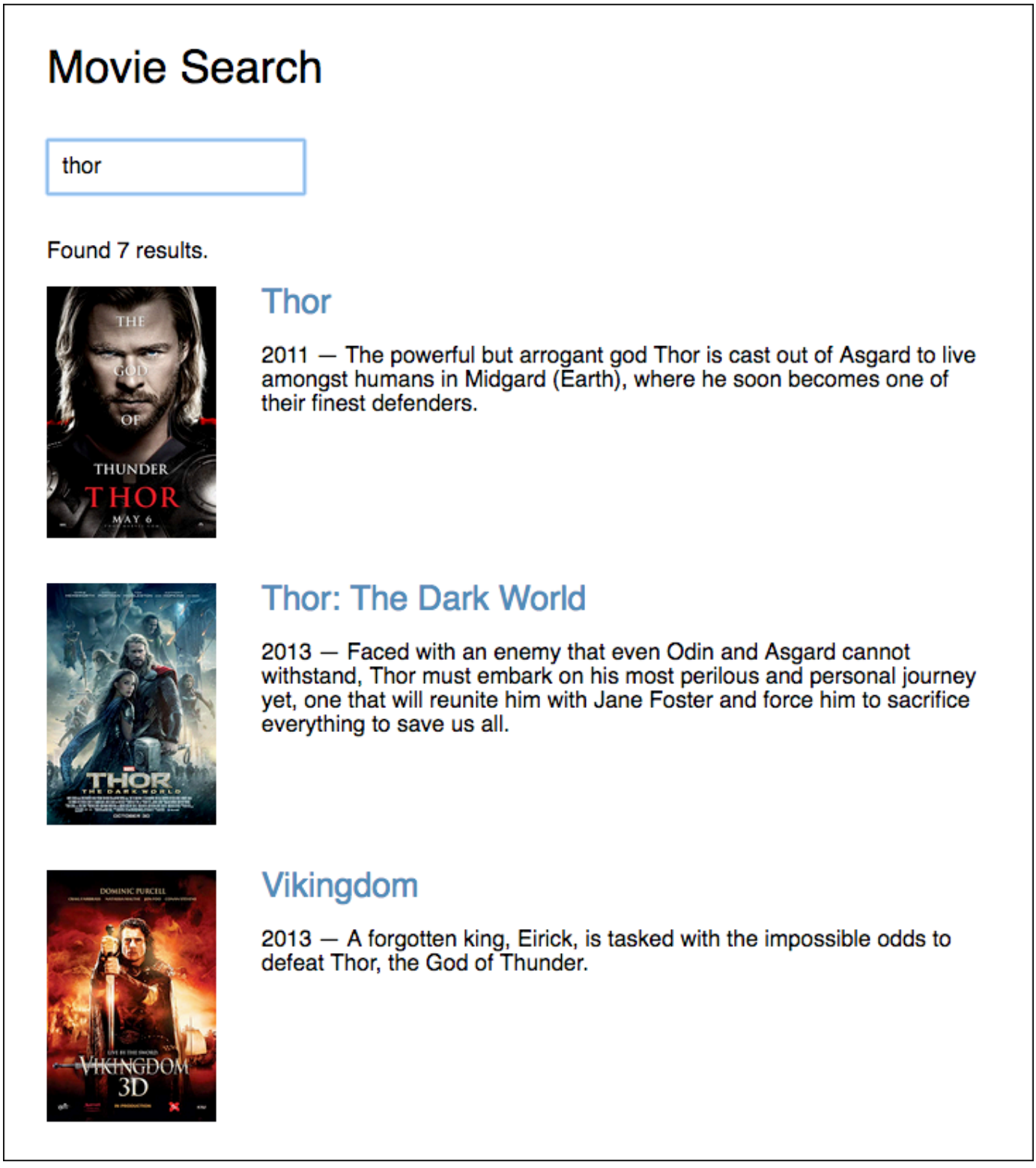
1. Desplácese hasta la URL de OpenSearch Dashboards para el dominio.
2. En el menú principal, seleccione Seguridad, Roles y elija el enlace a `all_access`, el rol al que necesita asignar el rol de Lambda.
3. Elija Usuarios asignados, Administrar mapeo.
4. En Roles de backend, agregue el nombre de recurso de Amazon (ARN) del rol de Lambda. El ARN debe adoptar la forma de `arn:aws:iam::123456789123:role/service-role/opensearch-lambda-role-1abcdefg`.
5. Seleccione Asignar y confirme que el usuario o el rol aparecen en Usuarios asignados.

Paso 5: Pruebe la aplicación web

Para probar la aplicación web

1. Descargue sample-site.zip, descomprímalo y abra `scripts/search.js` en el editor de texto de su elección.
2. Actualice la variable `apigatewayendpoint` para que apunte al punto de conexión de API Gateway y añada una barra oblicua al final de la ruta en cuestión. Puede encontrar rápidamente el punto de conexión en API Gateway seleccionando Etapas y seleccionando el nombre de la API. La variable `apigatewayendpoint` debe adoptar la forma de `https://some-id.execute-api.us-west-1.amazonaws.com/opensearch-api-test/`.

3. Abra `index.html` e intente ejecutar búsquedas de thor, house y algunos otros términos.



Solucionar errores de CORS

Aunque la función de Lambda incluye contenido en la respuesta para admitir CORS, es posible que aparezca el siguiente error:

```
Access to XMLHttpRequest at '<api-gateway-endpoint>' from origin 'null' has been
 blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present in the
 requested resource.
```

Si esto sucede, pruebe lo siguiente:

1. Habilitar CORS en el recurso GET. En Avanzado, configure Access-Control-Allow-Credentials en `'true'`.
2. Vuelva a implementar su API en API Gateway (Acciones, Implementar API).
3. Elimine y vuelva a agregar el activador de la función de Lambda. Agregue volver a añadirlo, elija Agregar desencadenador y cree el punto de conexión HTTP que invoca su función. El desencadenador debe tener la siguiente configuración:

Desencadenador	API	Etapa de implementación	Seguridad
API Gateway	opensearch-api	opensearch-api-test	Abra

Siguientes pasos

Este capítulo es solo un punto de partida para demostrar un concepto. Podría considerar las siguientes modificaciones:

- Agregue sus propios datos al dominio de OpenSearch Service.
- Agregue métodos a su API.
- En la función de Lambda, modifique la consulta de búsqueda o aumente los diferentes campos.
- Aplique un estilo diferente a los resultados o modifique `search.js` para mostrar diferentes campos al usuario.

Tutorial: Visualización de llamadas de soporte al cliente con OpenSearch Service y OpenSearch Dashboards

Este capítulo es un tutorial completo de la siguiente situación: el servicio de atención al cliente de una empresa recibe llamadas y quiere analizarlas. ¿Cuál es el tema de cada llamada? ¿Cuántas fueron positivas? ¿Cuántas negativas? ¿Cómo los gerentes pueden buscar o revisar las transcripciones de estas llamadas?

Un flujo de trabajo manual puede implicar que los empleados escuchen las grabaciones, apunten el tema de cada llamada y decidan si la interacción con el cliente fue positiva.

Dicho proceso requeriría mucho esfuerzo y trabajo. Suponiendo un tiempo medio de 10 minutos por llamada, cada empleado podría escuchar solo 48 llamadas al día. Salvo sesgo humano, los datos que generan sería de alta precisión, pero la cantidad de datos sería mínima: tan solo el tema de la llamada y un valor booleano para determinar si el cliente quedó satisfecho. Cualquier información más compleja, como, por ejemplo, una transcripción completa, requeriría gran cantidad de tiempo.

El uso de Amazon S3, Amazon Transcribe, Amazon Comprehend y Amazon OpenSearch Service, puede automatizar un proceso similar con muy poco código y obtener muchos más datos. Por ejemplo, puede obtener una transcripción completa de la llamada, palabras clave de la transcripción, y un "sentimiento" general de la llamada (positiva, negativa, neutra o mixta). A continuación, puede utilizar OpenSearch y OpenSearch Dashboards para buscar y visualizar los datos.

Aunque puede utilizar este tutorial tal y como está, su finalidad es dar ideas sobre cómo enriquecer sus documentos JSON antes de indexarlos en OpenSearch Service.

Costo estimado:

En general, seguir los pasos que se indican en este tutorial debería costar menos de 2 USD. En este tutorial se utilizan los siguientes recursos:

- bucket de S3 con menos de 100 MB transferidos y almacenados

  Para obtener más información, consulte Precios de Amazon S3.
- Un dominio de OpenSearch Service con una instancia `t2.medium` y 10 GiB de almacenamiento de EBS durante varias horas

  Para obtener más información, consulte Precios de Amazon OpenSearch Service.
- Varias llamadas a Amazon Transcribe

Para obtener más información, consulte Precios de Amazon Transcribe.

- Varias llamadas de procesamiento de lenguaje natural a Amazon Comprehend

  Para obtener más información, consulte Precios de Amazon Comprehend.

Temas

Paso 1: configure los requisitos previos

Antes de continuar, debe contar con los siguientes recursos.

Requisito previo	Descripción
Bucket de Amazon S3	Para obtener más información, consulte Creación de un bucket en la Guía del usuario de Amazon Simple Storage Service.
Dominio de OpenSearch Service	El destino de los datos. Para obtener más información, consulte Creación de dominios de OpenSearch Service.

Si aún no tiene estos recursos, puede crearlos utilizando los siguientes comandos de la AWS CLI:

```
aws s3 mb s3://my-transcribe-test --region us-west-2
```

```
aws opensearch create-domain --domain-name my-transcribe-test --engine-version
 OpenSearch_1.0 --cluster-config  InstanceType=t2.medium.search,InstanceCount=1
 --ebs-options EBSEnabled=true,VolumeType=standard,VolumeSize=10 --access-
policies '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::123456789012:root"},"Action":"es:*","Resource":"arn:aws:es:us-
west-2:123456789012:domain/my-transcribe-test/*"}]}' --region us-west-2
```

> **Note**
>
> Estos comandos utilizan la región `us-west-2`, pero puede utilizar cualquier región que admita Amazon Comprehend. Para obtener más información, consulte Referencia general de AWS.

Paso 2: copie el código de muestra

1. Copie y pegue el siguiente código de muestra de Python 3 en un archivo nuevo denominado `call-center.py`:

```
import boto3
import datetime
import json
import requests
from requests_aws4auth import AWS4Auth
import time
import urllib.request

# Variables to update
audio_file_name = '' # For example, 000001.mp3
bucket_name = '' # For example, my-transcribe-test
domain = '' # For example, https://search-my-transcribe-test-12345.us-
west-2.es.amazonaws.com
index = 'support-calls'
type = '_doc'
region = 'us-west-2'

# Upload audio file to S3.
s3_client = boto3.client('s3')

audio_file = open(audio_file_name, 'rb')

print('Uploading ' + audio_file_name + '...')
response = s3_client.put_object(
    Body=audio_file,
    Bucket=bucket_name,
    Key=audio_file_name
)

# # Build the URL to the audio file on S3.
```

```
# # Only for the us-east-1 region.
# mp3_uri = 'https://' + bucket_name + '.s3.amazonaws.com/' + audio_file_name

# Get the necessary details and build the URL to the audio file on S3.
# For all other regions.
response = s3_client.get_bucket_location(
    Bucket=bucket_name
)
bucket_region = response['LocationConstraint']
mp3_uri = 'https://' + bucket_name + '.s3-' + bucket_region + '.amazonaws.com/' +
 audio_file_name

# Start transcription job.
transcribe_client = boto3.client('transcribe')

print('Starting transcription job...')
response = transcribe_client.start_transcription_job(
    TranscriptionJobName=audio_file_name,
    LanguageCode='en-US',
    MediaFormat='mp3',
    Media={
        'MediaFileUri': mp3_uri
    },
    Settings={
        'ShowSpeakerLabels': True,
        'MaxSpeakerLabels': 2 # assumes two people on a phone call
    }
)

# Wait for the transcription job to finish.
print('Waiting for job to complete...')
while True:
    response =
 transcribe_client.get_transcription_job(TranscriptionJobName=audio_file_name)
    if response['TranscriptionJob']['TranscriptionJobStatus'] in ['COMPLETED',
 'FAILED']:
        break
    else:
        print('Still waiting...')
    time.sleep(10)

transcript_uri = response['TranscriptionJob']['Transcript']['TranscriptFileUri']

# Open the JSON file, read it, and get the transcript.
```

```
response = urllib.request.urlopen(transcript_uri)
raw_json = response.read()
loaded_json = json.loads(raw_json)
transcript = loaded_json['results']['transcripts'][0]['transcript']

# Send transcript to Comprehend for key phrases and sentiment.
comprehend_client = boto3.client('comprehend')

# If necessary, trim the transcript.
# If the transcript is more than 5 KB, the Comprehend calls fail.
if len(transcript) > 5000:
    trimmed_transcript = transcript[:5000]
else:
    trimmed_transcript = transcript

print('Detecting key phrases...')
response = comprehend_client.detect_key_phrases(
    Text=trimmed_transcript,
    LanguageCode='en'
)

keywords = []
for keyword in response['KeyPhrases']:
    keywords.append(keyword['Text'])

print('Detecting sentiment...')
response = comprehend_client.detect_sentiment(
    Text=trimmed_transcript,
    LanguageCode='en'
)

sentiment = response['Sentiment']

# Build the Amazon OpenSearch Service URL.
id = audio_file_name.strip('.mp3')
url = domain + '/' + index + '/' + type + '/' + id

# Create the JSON document.
json_document = {'transcript': transcript, 'keywords': keywords, 'sentiment':
 sentiment, 'timestamp': datetime.datetime.now().isoformat()}

# Provide all details necessary to sign the indexing request.
credentials = boto3.Session().get_credentials()
```

```
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region,
 'opensearchservice', session_token=credentials.token)

# Index the document.
print('Indexing document...')
response = requests.put(url, auth=awsauth, json=json_document, headers=headers)

print(response)
print(response.json())
```

2. Actualice las seis variables iniciales.
3. Instale los paquetes necesarios mediante los siguientes comandos:

```
pip install boto3
pip install requests
pip install requests_aws4auth
```

4. Guarde el MP3 en el mismo directorio que `call-center.py` y ejecute el script. A continuación se indica un ejemplo de salida:

```
$ python call-center.py
Uploading 000001.mp3...
Starting transcription job...
Waiting for job to complete...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Still waiting...
Detecting key phrases...
Detecting sentiment...
Indexing document...
<Response [201]>
{u'_type': u'call', u'_seq_no': 0, u'_shards': {u'successful': 1, u'failed': 0,
 u'total': 2}, u'_index': u'support-calls4', u'_version': 1, u'_primary_term': 1,
 u'result': u'created', u'_id': u'000001'}
```

`call-center.py` realiza una serie de operaciones:

1. El script carga un archivo de audio (en este caso, un MP3, pero Amazon Transcribe es compatible con varios formatos) en su bucket de S3.
2. Envía la URL del archivo de audio a Amazon Transcribe y espera que realice la tarea de transcripción.

   El tiempo necesario para terminar el trabajo de transcripción depende de la duración del archivo de audio. Supongamos que tomará minutos, no segundos.

   > **Tip**
   >
   > Para mejorar la calidad de la transcripción, puede configurar un vocabulario personalizado para Amazon Transcribe.

3. Una vez que el trabajo de transcripción termina, el script extrae la transcripción, la recorta a 5 000 caracteres y envía a Amazon Comprehend para identificar palabras clave y analizar el sentimiento.
4. Por último, el script añade toda la transcripción, palabras clave, sentimiento y marca de tiempo actual a un documento JSON, y lo indexa en OpenSearch Service.

> **Tip**
>
> LibriVox tiene audiolibros de dominio público que puede utilizar para hacer pruebas.

(Opcional) Paso 3: indexe los datos de ejemplo

Si no tiene a mano varias grabaciones de llamadas, y no es algo muy frecuente, puede indexar los documentos de muestra en sample-calls.zip, que son comparables a lo que produce `call-center.py`.

1. Cree un archivo denominado `bulk-helper.py`:

```
import boto3
from opensearchpy import OpenSearch, RequestsHttpConnection
import json
from requests_aws4auth import AWS4Auth

host = '' # For example, my-test-domain.us-west-2.es.amazonaws.com
```

```
region = '' # For example, us-west-2
service = 'es'

bulk_file = open('sample-calls.bulk', 'r').read()

credentials = boto3.Session().get_credentials()
awsauth = AWS4Auth(credentials.access_key, credentials.secret_key, region, service,
 session_token=credentials.token)

search = OpenSearch(
    hosts = [{'host': host, 'port': 443}],
    http_auth = awsauth,
    use_ssl = True,
    verify_certs = True,
    connection_class = RequestsHttpConnection
)

response = search.bulk(bulk_file)
print(json.dumps(response, indent=2, sort_keys=True))
```

2. Actualice las dos variables iniciales para `host` y `region`.
3. Instale el paquete necesario mediante el siguiente comando:

```
pip install opensearch-py
```

4. Descargue y descomprima sample-calls.zip.
5. Guarde `sample-calls.bulk` en el mismo directorio que `bulk-helper.py` y ejecute el ayudante. A continuación se indica un ejemplo de salida:

```
$ python bulk-helper.py
{
  "errors": false,
  "items": [
    {
      "index": {
        "_id": "1",
        "_index": "support-calls",
        "_primary_term": 1,
        "_seq_no": 42,
        "_shards": {
          "failed": 0,
          "successful": 1,
```

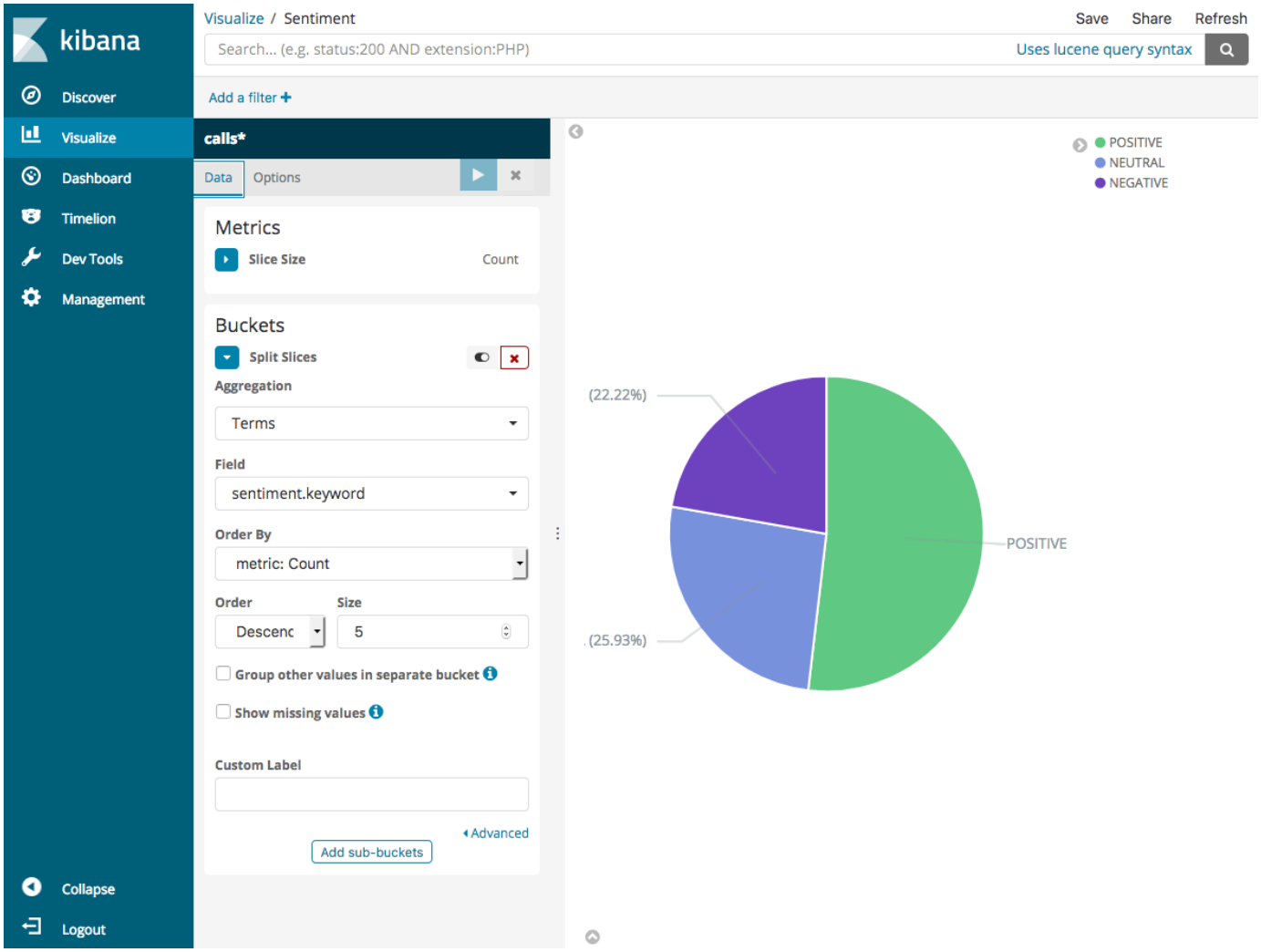
```
          "total": 2
        },
        "_type": "_doc",
        "_version": 9,
        "result": "updated",
        "status": 200
      }
    },
    ...
  ],
  "took": 27
}
```

Paso 4: analice y visualice sus datos

Ahora que tiene en algunos datos en OpenSearch Service, puede visualizarlos con OpenSearch Dashboards.

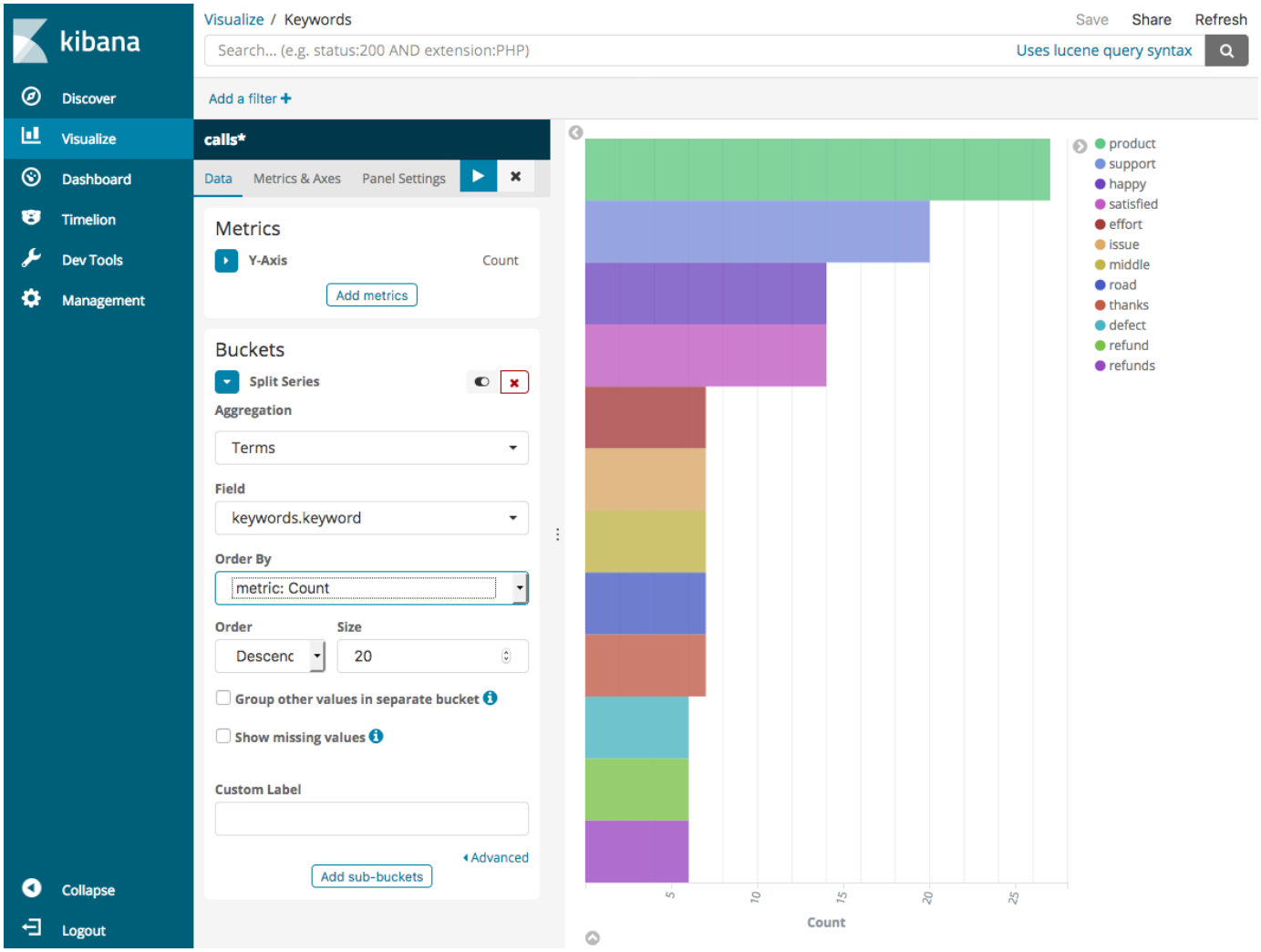
1. Vaya a `https://search-`*`domain`*`.`*`region`*`.es.amazonaws.com/_dashboards`.
2. Para poder utilizar OpenSearch Dashboards, necesita un patrón de índice. Dashboards utiliza patrones de índice para limitar su análisis a uno o más índices. Para que coincida con el `support-calls`índice que`call-center.py` cree, diríjase a Pila de administración, Patrones, y defina un patrón de índice de `support*`. y luego elija Paso siguiente.
3. En Time Filter field name (Nombre de campo Filtro de tiempo), elija timestamp (marca temporal).
4. Ahora pude comenzar a crear visualizaciones. Elija Visualize (Visualizar) y añada una nueva visualización.
5. Elija el gráfico circular y el patrón de índice `support*`.
6. El valor predeterminado de visualización es básico. Si quiere crear una visualización más interesante, elija Split Slices (Sectores divididos).

   Para Aggregation (Agregación), elija Terms (Términos). En Field (Campo), elija sentiment.keyword. Elija Apply changes (Aplicar cambios) y Save (Guardar).

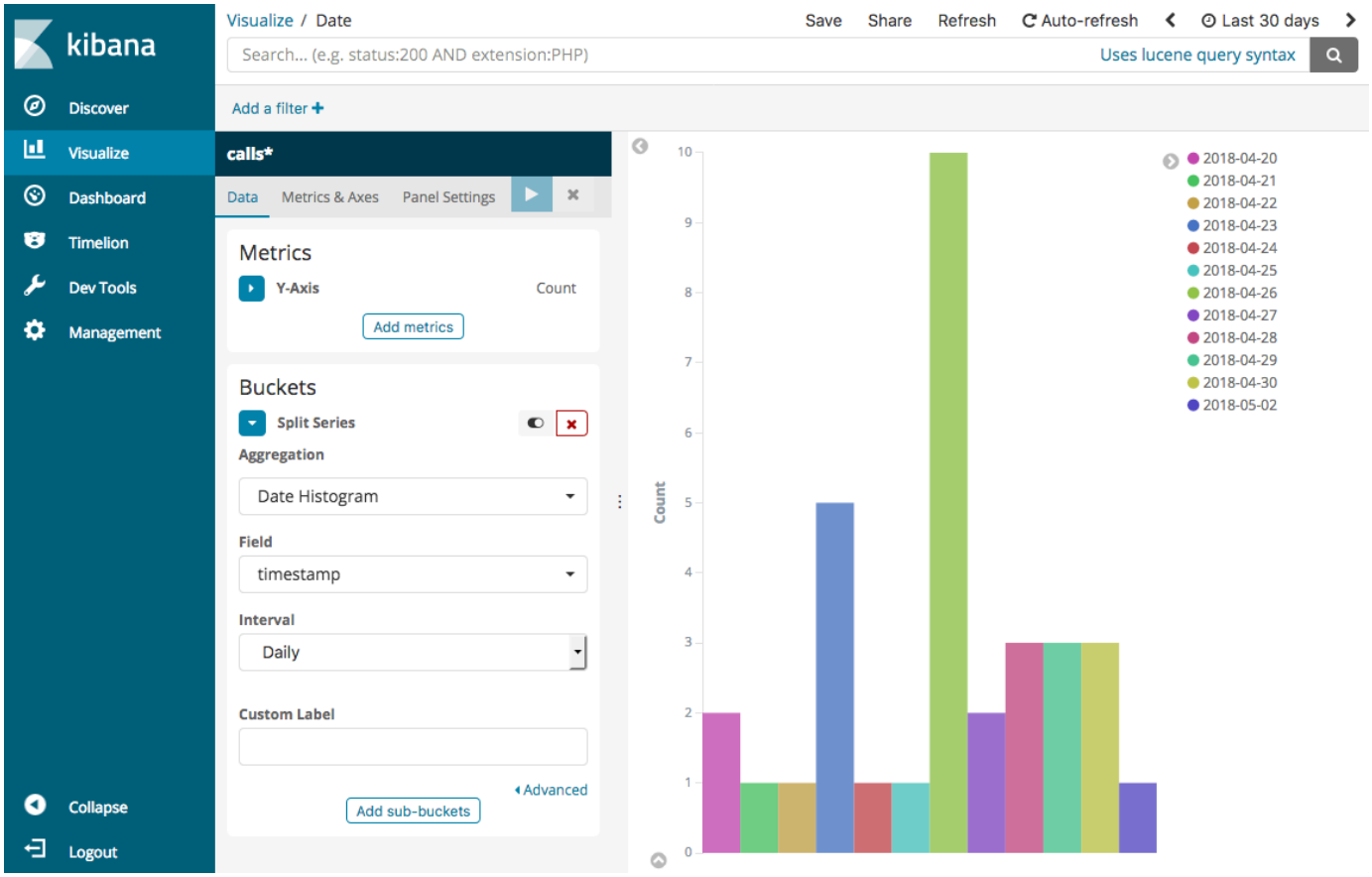


7. Vuelva a la página Visualize (Visualizar) y añada otra visualización. Esta vez, elija el gráfico de barras horizontales.
8. Elija Split Series (Series divididas).

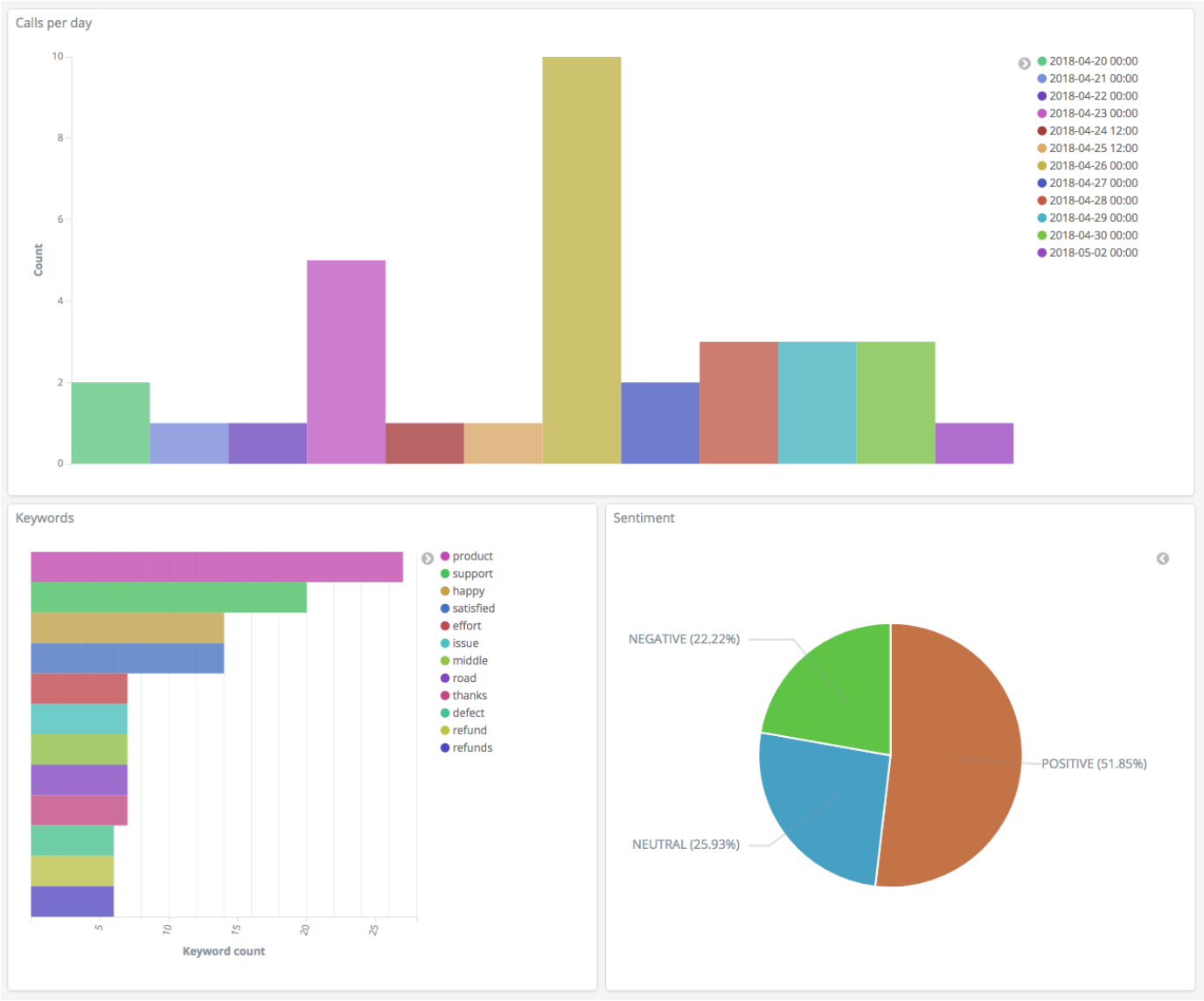
   Para Aggregation (Agregación), elija Terms (Términos). En Field (Campo), elija keywords.keyword y cambie el valor de Size (Tamaño) a 20. Elija Apply Changes (Aplicar cambios) y Save (Guardar).



9. Vuelva a la página Visualize (Visualizar) y añada una última visualización, un gráfico de barras verticales.
10. Elija Split Series (Series divididas). En Aggregation (Agregación), elija Date Histogram (Histograma de fecha). En Field (Campo), elija timestamp (marca temporal) y cambie Interval (Intervalo) a Daily (Diario).
11. Elija Metrics & Axes (Métricas y ejes) y cambie Mode (Modo) a normal.
12. Elija Apply Changes (Aplicar cambios) y Save (Guardar).



13. Ahora que tiene tres visualizaciones, puede añadirlas a un panel de Dashboards. Elija Dashboard (Panel), cree un panel y añada sus visualizaciones.



Paso 5: elimine recursos y pasos siguientes

Para evitar gastos innecesarios, elimine el bucket de S3 y el dominio de OpenSearch Service. Para obtener más información, consulte Eliminación de un bucket en la Guía del usuario de Amazon Simple Storage Service y Eliminación de un dominio de OpenSearch Service en esta guía.

Las transcripciones requieren mucho menos espacio de disco que los archivos MP3. Puede reducir su ventana de retención de MP3 por ejemplo, de tres meses de grabaciones de llamadas a un mes guarde años de transcripciones, y ahorre en costos de almacenamiento.

También puede automatizar el proceso de transcripción con AWS Step Functions y Lambda, agregue los metadatos adicionales antes de indexar, o cree visualizaciones más complejas para adaptarse a su caso de uso exacto.

Cambio de nombre de Amazon OpenSearch Service: resumen de cambios

El 8 de septiembre de 2021, nuestro conjunto de aplicaciones de búsqueda y análisis pasó a llamarse Amazon OpenSearch Service. OpenSearch Service es compatible con OpenSearch, así como con Elasticsearch OSS heredado. En las secciones siguientes, se describen las diferentes partes del servicio que sufrieron modificaciones con el cambio de nombre y las acciones que se deben realizar para garantizar que los dominios sigan funcionando correctamente.

Algunos de estos cambios solo se aplican cuando actualiza sus dominios de Elasticsearch a OpenSearch. En otros casos, como en la consola de Billing and Cost Management, la experiencia cambia inmediatamente.

Tenga en cuenta que esta lista no es exhaustiva. Mientras que otras partes del producto también cambiaron, estas actualizaciones son las más relevantes.

Temas

Nueva versión de la API

La nueva versión de la API de configuración de OpenSearch Service (01/01/2021) funciona con OpenSearch, así como con Elasticsearch OSS heredado. Se reemplazaron 21 operaciones de la API por nombres más concisos e independientes del motor (por ejemplo,

`CreateElasticsearchDomain` cambió a `CreateDomain`), pero OpenSearch Service aún es compatible con ambas versiones de la API.

Recomendamos utilizar las nuevas operaciones de la API para crear y administrar dominios en el futuro. Tenga en cuenta que cuando utilice las nuevas operaciones de la API para crear un dominio, debe especificar el parámetro `EngineVersion` en el formato `Elasticsearch_X.Y` o `OpenSearch_X.Y`, en lugar de solo el número de versión. Si no especifica ninguna versión, toma de forma predeterminada la versión más reciente de OpenSearch.

Actualice la AWS CLI a la versión 1.20.40 o posterior para utilizar `aws opensearch ...` a fin de crear y administrar los dominios. Para obtener el nuevo formato de la CLI, consulte la Referencia de la CLI de OpenSearch.

Tipos de instancia con cambio de nombre

Los tipos de instancias de Amazon OpenSearch Service ahora tienen el formato `<type>.<size>.search`, por ejemplo, `m6g.large.search` en lugar de `m6g.large.elasticsearch`. No es necesario realizar ninguna acción. Los dominios existentes comenzarán a hacer referencia automáticamente a los nuevos tipos de instancias dentro de la API y en la consola de Billing and Cost Management.

Si dispone de instancias reservadas (RI), el cambio no afectará al contrato. La versión antigua de la API de configuración aún es compatible con el formato de nomenclatura anterior, pero si desea utilizar la nueva versión de la API, debe utilizar el nuevo formato.

Cambios en las políticas de acceso

En las secciones siguientes, se describen las acciones que debe realizar para actualizar las políticas de acceso.

Políticas de IAM

Recomendamos que actualice sus Políticas de IAM para utilizar las operaciones de la API con cambio de nombre. Sin embargo, OpenSearch Service seguirá respetando las políticas existentes al replicar internamente los permisos de la API antiguos. Por ejemplo, si actualmente tiene permiso para realizar la operación `CreateElasticsearchDomain`, ahora puede realizar llamadas a ambos `CreateElasticsearchDomain` (operación antigua de la API) y `CreateDomain` (nueva

operación de la API). Lo mismo se aplica a las denegaciones explícitas. Para obtener una lista de las operaciones de la API actualizadas, consulte la referencia de elementos de política.

Políticas de SCP

Las políticas de control de servicios (SCP) presentan una capa adicional de complejidad en comparación con IAM estándar. Para evitar que las políticas de SCP se rompan, debe agregar tanto las operaciones de la API antiguas como las nuevas a cada una de sus políticas de SCP. Por ejemplo, si actualmente un usuario tiene permisos para `CreateElasticsearchDomain`, también debe concederles permisos para `CreateDomain` a fin de que puedan retener la capacidad de crear dominios. Lo mismo se aplica a las denegaciones explícitas.

Por ejemplo:

```
"Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "es:CreateElasticsearchDomain",
        "es:CreateDomain"
         ...
      ],
    },
      "Effect": "Deny",
      "Action:" [
        "es:DeleteElasticsearchDomain",
        "es:DeleteDomain"
         ...
```

Nuevos tipos de recursos

OpenSearch Service presenta los siguientes tipos de recursos nuevos:

Recurso	Descripción
`AWS::OpenSearchService::Domain`	Representa un dominio de Amazon OpenSearch Service. Este recurso existe en el nivel de servicio y no es específico del software que se ejecuta en el dominio. Se aplica a servicios

Recurso	Descripción
	como AWS CloudFormation y AWS Resource Groups, en los que crea y administra recursos para el servicio en su conjunto. Para obtener instrucciones para actualizar los dominios definidos en CloudFormation de Elasticsearch a OpenSearch, consulte Observaciones en la Guía del usuario de CloudFormation.
`AWS::OpenSearch::Domain`	Representa el software OpenSearch/Elastic search que se ejecuta en un dominio. Este recurso se aplica a servicios como AWS CloudTrail y AWS Config, que hacen referenci a al software que se ejecuta en el dominio en lugar de a OpenSearch Service como un todo. Estos servicios ahora contienen tipos de recursos separados para dominios que ejecutan Elasticsearch (`AWS::Elas ticsearch::Domain`) frente a dominios que ejecutan OpenSearch (`AWS::Open Search::Domain`).

> **Note**
>
> En AWS Config, seguirá viendo sus datos en el tipo de recurso `AWS::Elasticsearch::Domain` existente durante varias semanas, incluso si actualiza uno o más dominios a OpenSearch.

Kibana cambió de nombre a OpenSearch Dashboards

OpenSearch Dashboards, la alternativa de AWS a Kibana, es una herramienta de visualización de código abierto diseñada para funcionar con OpenSearch. Después de actualizar un dominio de Elasticsearch a OpenSearch, el punto de enlace `/_plugin/kibana` cambia a `/_dashboards`.

OpenSearch Service redirigirá todas las solicitudes al nuevo punto de enlace, pero si utiliza el punto de enlace de Kibana en cualquiera de sus políticas de IAM, actualice esas políticas para incluir el nuevo punto de enlace de `/_dashboards` también.

Si utiliza the section called “Autenticación SAML para paneles OpenSearch ”, antes de actualizar su dominio a OpenSearch, debe cambiar todas las URL de Kibana configuradas en su proveedor de identidad (IdP) de `/_plugin/kibana` a `/_dashboards`. Las URL más comunes son las URL de servicio al consumidor de aserción (ACS) y las URL de destinatario.

Se ha cambiado el nombre del rol `kibana_read_only` predeterminado para OpenSearch Dashboards por `opensearch_dashboards_read_only`, y al rol `kibana_user` se le ha cambiado el nombre por `opensearch_dashboards_user`. El cambio es de aplicación a todos los dominios recién creados de OpenSearch 1.x en los que se ejecute el software de servicio R20211203 o posterior. Si se actualiza un dominio existente al software de servicio R20211203, los nombres de los roles siguen siendo los mismos.

Métricas de CloudWatch con cambio de nombre

Varias métricas de CloudWatch cambian para los dominios que ejecutan OpenSearch. Cuando actualiza un dominio a OpenSearch, las métricas cambian automáticamente y las alarmas actuales de CloudWatch fallarán. Antes de actualizar el clúster de una versión de Elasticsearch a una versión de OpenSearch, asegúrese de actualizar las alarmas de CloudWatch para utilizar las nuevas métricas.

Cambiaron las siguientes métricas:

Nombre de métrica original	Nombre nuevo
`KibanaHealthyNodes`	`OpenSearchDashboardsHealthyNodes`
`KibanaConcurrentConnections`	`OpenSearchDashboardsConcurrentConnections`
`KibanaHeapTotal`	`OpenSearchDashboardsHeapTotal`
`KibanaHeapUsed`	`OpenSearchDashboardsHeapUsed`
`KibanaHeapUtilization`	`OpenSearchDashboardsHeapUtilization`

Nombre de métrica original	Nombre nuevo
KibanaOS1MinuteLoad	OpenSearchDashboardsOS1MinuteLoad
KibanaRequestTotal	OpenSearchDashboardsRequestTotal
KibanaResponseTimesMaxInMillis	OpenSearchDashboardsResponseTimesMaxInMillis
ESReportingFailedRequestSysErrCount	KibanaReportingFailedRequestSysErrCount
ESReportingRequestCount	KibanaReportingRequestCount
ESReportingFailedRequestUserErrCount	KibanaReportingFailedRequestUserErrCount
ESReportingSuccessCount	KibanaReportingSuccessCount
ElasticsearchRequests	OpenSearchRequests

Para obtener una lista completa de las métricas que OpenSearch Service envía a Amazon CloudWatch, consulte the section called “Monitoreo de métricas del clúster”.

Cambios en la consola de Billing and Cost Management

Los datos históricos en la consola de Administración de facturación y costos y en los Informes de costos y usos seguirán utilizando el nombre del servicio antiguo, por lo que debe comenzar a emplear filtros tanto para Amazon OpenSearch Service como para el nombre de Elasticsearch heredado cuando haga búsquedas de datos. Si ya tiene informes guardados, actualice los filtros para asegurarse de que también incluyen OpenSearch Service. Es posible que reciba inicialmente una alerta cuando su utilización disminuya para Elasticsearch y aumente para OpenSearch, pero desaparezca en varios días.

Además del nombre del servicio, los siguientes campos cambiarán para todos los informes, facturas y operaciones de la API de lista de precios:

Campo	Formato antiguo	Formato nuevo
Tipo de instancia	`m5.large.elasticsearch`	`m5.large.search`
Familia de productos	Instancia de Elasticsearch Volumen de Elasticsearch	Instancia de Amazon OpenSearch Service Volumen de Amazon OpenSearch Service
Descripción del precio	5,098 USD por hora de instancia c5.18xlarge.elasticsearch (u hora parcial), UE	5,098 USD por hora de instancia c5.18xlarge.search (u hora parcial), UE
Familia de instancias	`ultrawarm.elasticsearch`	`ultrawarm.search`

Nuevo formato de evento

El formato de los eventos que OpenSearch Service envía a Amazon EventBridge y Amazon CloudWatch ha cambiado, específicamente el campo `detail-type`. El campo fuente (`aws.es`) aún es el mismo. Para obtener el formato completo de cada tipo de evento, consulte the section called "Supervisión de eventos". Si tiene reglas de evento existentes que dependen del formato antiguo, asegúrese de actualizarlas para que se ajusten al nuevo formato.

¿Qué permanece igual?

Las siguientes características y funcionalidades, entre otras no enumeradas, permanecerán iguales:

- Entidad principal de servicio (`es.amazonaws.com`)
- Código de proveedor
- ARN del dominio
- Puntos de enlace del dominio

Comience: Actualice sus dominios a OpenSearch 1.x

OpenSearch 1.x soporta actualizaciones de Elasticsearch versión 6.8 y 7.x. Para obtener instrucciones a fin de actualizar su dominio, consulte the section called “Inicio de una actualización (consola)”. Si utiliza la AWS CLI o la API de configuración para actualizar su dominio, debe especificar la `TargetVersion` como `OpenSearch_1.x`.

OpenSearch 1.x presenta una configuración de dominio adicional llamada Habilitar modo de compatibilidad. Debido a que algunos clientes y complementos de Elasticsearch OSS verifican la versión del clúster antes de conectarse, el modo de compatibilidad establece que OpenSearch informe su versión como 7.10 para que estos clientes sigan funcionando.

Puede habilitar el modo de compatibilidad al crear dominios de OpenSearch por primera vez o al actualizar a OpenSearch desde una versión de Elasticsearch. Si no está establecido, el parámetro predeterminado es `false` al crear un dominio y `true` cuando actualiza un dominio.

Para habilitar el modo de compatibilidad mediante la API de configuración, establezca `override_main_response_version` en `true`:

```
POST https://es.us-east-1.amazonaws.com/2021-01-01/opensearch/upgradeDomain
{
  "DomainName": "domain-name",
  "TargetVersion": "OpenSearch_1.0",
  "AdvancedOptions": {
    "override_main_response_version": "true"
   }
}
```

Para habilitar o desactivar el modo de compatibilidad en dominios de OpenSearch existentes, es necesario utilizar la operación de la API de OpenSearch _cluster/settings:

```
PUT /_cluster/settings
{
  "persistent" : {
    "compatibility.override_main_response_version" : true
  }
}
```

Solución de problemas de Amazon OpenSearch Service

En este tema se describe cómo identificar y resolver problemas comunes de Amazon OpenSearch Service. Consulte la información de esta sección antes de ponerse en contacto con el Soporte de AWS.

No se puede acceder a OpenSearch Dashboards

El punto de conexión de OpenSearch Dashboards no admite solicitudes firmadas. Si la política de control de acceso del dominio solo concede acceso a determinados roles de IAM y no se ha configurado la autenticación de Amazon Cognito, es posible que aparezca el siguiente error cuando se intente acceder a Dashboards:

```
"User: anonymous is not authorized to perform: es:ESHttpGet"
```

Si su dominio de OpenSearch Service utiliza el acceso mediante VPC, probablemente no ocurra este error, pero puede que se agote el tiempo de espera. Para obtener más información acerca de cómo solucionar este problema y las distintas opciones de configuración disponibles the section called “Controlar el acceso a los paneles OpenSearch ”, consulte the section called “Acerca de las políticas de acceso en los dominios de VPC” y the section called “Identity and Access Management”.

No se puede obtener acceso al dominio de VPC

Consulte the section called “Acerca de las políticas de acceso en los dominios de VPC” y the section called “Probar los dominios de VPC”.

Clúster en estado de solo lectura

Comparado con versiones anteriores de Elasticsearch, OpenSearch y Elasticsearch 7.x utilizan un sistema diferente para la coordinación de clústeres. En este nuevo sistema, cuando el clúster pierde quórum, el clúster no estará disponible hasta que realice alguna acción. La pérdida de quórum puede adoptar dos formas:

- Si el clúster utiliza nodos principales dedicados, la pérdida de cuórum se produce cuando la mitad o más no están disponibles.

- Si el clúster no utiliza nodos principales dedicados, la pérdida de cuórum se produce cuando la mitad o más de los nodos de datos no están disponibles.

Si se produce una pérdida de cuórum y el clúster tiene más de un nodo, OpenSearch Service restaura el cuórum y coloca el clúster en un estado de solo lectura. Dispone de dos opciones para hacerlo:

- Elimine el estado de solo lectura y utilice el clúster tal y como está.
- Restaure el clúster o los índices individuales a partir de una instantánea.

Si prefiere utilizar el clúster tal y como está, verifique que el estado del clúster sea verde mediante la siguiente solicitud:

```
GET _cat/health?v
```

Si el estado del clúster es rojo, le recomendamos que restaure el clúster a partir de una instantánea. También puede consultar the section called “Estado rojo del clúster” para ver los pasos de solución de problemas. Si el estado del clúster es verde, compruebe que todos los índices esperados estén presentes utilizando la siguiente solicitud:

```
GET _cat/indices?v
```

A continuación, ejecute algunas búsquedas para verificar que los datos esperados están presentes. Si es, puede eliminar el estado de solo lectura utilizando la siguiente solicitud:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.blocks.read_only": false
  }
}
```

Si se produce una pérdida de cuórum y el clúster solo tiene un nodo, OpenSearch Service sustituye el nodo y no coloca el clúster en un estado de solo lectura. De lo contrario, las opciones son las mismas: utilice el clúster tal y como está o restaure a partir de una instantánea.

En ambas situaciones, OpenSearch Service envía dos eventos a su AWS Health Dashboard. El primero le informa de la pérdida de cuórum. El segundo ocurre después de que OpenSearch Service

restaure correctamente el cuórum. Para obtener más información acerca del uso de AWS Health Dashboard, consulte la Guía de usuario de AWS Health.

Estado rojo del clúster

El estado rojo del clúster significa que al menos una partición principal y sus réplicas no están asignados a un nodo. OpenSearch Service sigue tratando de tomar instantáneas automatizadas de todos los índices independientemente de su estado, pero las instantáneas fallan mientras el estado del clúster rojo persiste.

Las causas más comunes de un estado rojo del clúster son que los nodos del clúster han fallado y que el proceso de OpenSearch se ha bloqueado debido a una carga de procesamiento elevada continua.

> **Note**
>
> OpenSearch Service almacena instantáneas automatizadas durante 14 días, independientemente del estado del clúster. Por lo tanto, si el estado del clúster rojo persiste durante más de dos semanas, se eliminará la última instantánea automatizada correcta y podría perder permanentemente los datos del clúster. Si el dominio de OpenSearch Service pasa a un estado rojo del clúster, el equipo de AWS Support podría contactar con usted para preguntarle si desea corregir el problema por sí mismo o si prefiere que ellos lo ayuden. También puede definir una alarma de CloudWatch que le notifique cuando se produzca un estado rojo del clúster.

En última instancia, los fragmentos rojos causan clústeres rojos y los índices rojos causan fragmentos rojos. Para identificar los índices que causan el estado rojo del clúster, OpenSearch tiene algunas API útiles.

- `GET /_cluster/allocation/explain` elige el primer fragmento no asignado que encuentra y explica por qué no se puede asignar a un nodo:

```
{
    "index": "test4",
    "shard": 0,
    "primary": true,
    "current_state": "unassigned",
    "can_allocate": "no",
```

```
    "allocate_explanation": "cannot allocate because allocation is not permitted to
 any of the nodes"
}
```

- `GET /_cat/indices?v` muestra el estado, el número de documentos y el uso de disco de cada índice:

```
health status index           uuid                   pri rep docs.count docs.deleted
 store.size pri.store.size
green  open   test1           30h1EiMvS5uAFr2t5CEVoQ   5   0        820            0
       14mb           14mb
green  open   test2           sdIxs_WDT56afFGu5KPbFQ   1   0          0            0
       233b           233b
green  open   test3           GGRZp_TBRZuSaZpAGk2pmw   1   1          2            0
     14.7kb          7.3kb
red    open   test4           BJxfAErbTtu5HBjIXJV_7A   1   0
green  open   test5           _8C6MIXOSxCqVYicH3jsEA   1   0          7            0
     24.3kb         24.3kb
```

Eliminar los índices rojos es la forma más rápida de solucionar el estado rojo del clúster. Según el motivo del estado rojo del clúster, podría ampliar el dominio de OpenSearch Service para utilizar tipos de instancias de mayor tamaño, más instancias o más almacenamiento basado en EBS e intentar volver a crear los índices problemáticos.

Si eliminar un índice problemático no es factible, puede restaurar una instantánea, eliminar documentos del índice, cambiar la configuración del índice, reducir el número de réplicas o eliminar otros índices para liberar espacio en el disco. El paso más importante es resolver el estado rojo del clúster antes de volver a configurar su dominio de OpenSearch Service. Volver a configurar un dominio con un estado rojo del clúster puede agravar el problema y el dominio podría quedarse bloqueado en el estado de configuración Processing (Procesando) hasta que se resuelva el estado.

Corrección automática de clústeres en rojo

Si el estado del clúster permanece en rojo de manera continuada durante más de una hora, OpenSearch Service intenta corregirlo automáticamente redirigiendo particiones no asignadas o restaurando desde instantáneas anteriores.

Si no consigue corregir uno o varios índices en rojo y el estado del clúster permanece en rojo durante un total de 14 días, OpenSearch Service solo toma medidas adicionales si el clúster cumple al menos uno de los siguientes criterios:

- Tiene solo una zona de disponibilidad
- No tiene nodos maestros dedicados
- Contiene tipos de instancias de ráfaga (T2 o T3)

En este momento, si el clúster cumple uno de estos criterios, OpenSearch Service envía notificaciones diarias durante los siguientes 7 días en las que explica que, si no se corrigen estos índices, se eliminarán todas las particiones no asignadas. Si el estado del clúster sigue en rojo transcurridos 21 días, OpenSearch Service elimina las particiones no asignadas (almacenamiento y computación) de todos los índices en rojo. Las notificaciones correspondientes a cada uno de estos eventos se reciben en el panel Notificaciones de la consola de OpenSearch Service. Para obtener más información, consulte the section called “Eventos del estado del clúster”.

Recuperación de una carga de procesamiento elevada continua

Para determinar si el estado rojo de un clúster se debe a una carga de procesamiento elevada continua en un nodo de datos, monitorice las siguientes métricas de clúster.

Métrica relevante	Descripción	Recuperación
JVMMemoryPressure	Especifica el porcentaje del montón de Java que se emplea para todos los nodos de datos de un clúster. Vea la estadística Máximo de esta métrica y busque caídas cada vez más pequeñas en la presión de memoria a medida que el recolector de elementos no utilizados de Java no consigue reclamar suficiente memoria. Probablemente, este patrón se deba a consultas complejas o a campos de datos de gran tamaño. Los tipos de instancias x86 utilizan el recolector de basura Concurrent Mark Sweep (CMS), que se ejecuta junto a subprocesos de aplicaciones	Establezca interruptores de memoria para la JVM. Para obtener más información, consulte the section called “OutOfMemoryError de JVM”. Si el problema persiste, elimine los índices innecesarios, reduzca el número o la complejidad de las solicitudes al dominio, agregue instancias o utilice tipos de instancia más grandes.

Métrica relevante	Descripción	Recuperación
	para que las pausas sigan siendo breves. Si CMS no puede obtener memoria suficiente durante sus recolecciones normales, desencadena una recolección de basura completa, lo que puede provocar pausas prolongadas de las aplicaciones y afectar a la estabilidad del clúster. Los tipos de instancias Graviton basados en ARM utilizan el recolector de basura Garbage-First (G1), que es similar a CMS, pero utiliza pausas breves adicionales y desfragmentación del montón para reducir aún más la necesidad de recolecciones de basura completas. En cualquier caso, si el uso de memoria continúa creciendo por encima de lo que el recopilador de basura puede obtener durante la recopilación de basura completa, OpenSearch se bloquea con un error de memoria insuficiente. En todos los tipos de instancias, una buena regla es mantener el uso por debajo del 80 %. La API `_nodes/stats/jvm` ofrece un resumen útil sobre estadísticas de JVM, el uso del grupo de memoria e información de recolección de elementos no utilizados:	

Métrica relevante	Descripción	Recuperación
	`GET domain-endpoint /_nodes/stats/jvm?pretty`	
CPUUtilization	Especifica el porcentaje de recursos de CPU usados para los nodos de datos de un clúster. Consulte la estadística Máximo para esta métrica y busque un patrón continuo de uso elevado.	Agregue nodos de datos o aumente el tamaño de los tipos de instancia de los nodos de datos existentes.
Nodos	Especifica el número de nodos de un clúster. Vea la estadística Mínimo para esta métrica. Este valor fluctúa cuando el servicio implementa una nueva flota de instancias para un clúster.	Agregue nodos de datos.

Estado amarillo del clúster

Un estado amarillo del clúster significa que los fragmentos principales de todos los índices están asignados a nodos de un clúster, pero los fragmentos de réplica de al menos un índice no lo están. Los clústeres de un nodo siempre se inicializan con un estado amarillo, ya que no existe ningún otro nodo al que OpenSearch Service pueda asignar una réplica. Para conseguir el estado verde del clúster, aumente el número de nodos. Para obtener más información, consulte the section called “Determinación del tamaño de dominios”.

Los clústeres de varios nodos pueden tener brevemente un estado de clúster amarillo después de crear un nuevo índice o después de un error de nodo. Este estado se resuelve automáticamente a medida que OpenSearch replica datos en todo el clúster. La falta de espacio en disco también puede causar el estado de clúster amarillo; el clúster sólo puede distribuir fragmentos de réplica si los nodos tienen espacio en disco para acomodarlos.

ClusterBlockException

Puede que reciba un error `ClusterBlockException` por los siguientes motivos.

Falta de espacio de almacenamiento disponible

Si uno o más nodos de su clúster tienen un espacio de almacenamiento inferior al valor mínimo de 1) 20 % del espacio de almacenamiento disponible, o 2) 20 GB de espacio de almacenamiento, las operaciones básicas de escritura, como la adición de documentos y la creación de índices, pueden empezar a fallar. the section called “Cálculo de requisitos de almacenamiento” proporciona un resumen de cómo OpenSearch Service utiliza el espacio en disco.

Para evitar problemas, monitorice la métrica `FreeStorageSpace` en la consola de OpenSearch Service y crear alarmas de CloudWatch que se activan cuando `FreeStorageSpace` esté por debajo de un determinado umbral. `GET /_cat/allocation?v` también proporciona un resumen útil de la asignación de particiones y el uso del disco. Para solucionar los problemas asociados a una falta de espacio de almacenamiento, amplíe su dominio de OpenSearch Service para utilizar tipos de instancias de mayor tamaño, más instancias o más almacenamiento basado en EBS.

Presión alta de memoria de JVM

Si la métrica JVMMemoryPressure supera el 92 % durante 30 minutos, OpenSearch Service activa un mecanismo de protección y bloquea todas las operaciones de escritura para impedir que el clúster alcance el estado rojo. Cuando la protección está activada, se produce un error `ClusterBlockException` en las operaciones de escritura, los nuevos índices no se pueden crear y se genera el error `IndexCreateBlockException`.

Si la métrica JVMMemoryPressure vuelve al 88% o un valor inferior durante cinco minutos, la protección queda deshabilitada y las operaciones de escritura en el clúster se desbloquean.

La presión alta de memoria de JVM puede deberse a picos en el número de solicitudes al clúster, asignaciones de particiones desequilibradas en los nodos, demasiadas particiones en un clúster, explosiones de mapeo de índices o datos de campo, o tipos de instancias que no pueden gestionar las cargas entrantes. También puede deberse al uso de agregaciones, comodines o intervalos de tiempo amplios en las consultas.

Para reducir el tráfico al clúster y resolver problemas de presión alta de memoria de JVM, pruebe una o más de las siguientes acciones:

- Escale el dominio para que el tamaño máximo de la pila por nodo sea de 32 GB.
- Reduzca el número de particiones mediante la eliminación de los índices antiguos o no utilizados.

- Borre la memoria caché de datos con la Operación de la API de `POST index-name/_cache/clear?fielddata=true`. Tenga en cuenta que borrar la memoria caché puede interrumpir las consultas en curso.

En general, para evitar una presión alta de memoria de JVM en el futuro, siga estas prácticas recomendadas:

- Evite la agregación en los campos de texto o cambie el tipo de mapeo para sus índices `keyword`.
- Optimice las solicitudes de búsqueda e indexación mediante la selección del número correcto de particiones.
- Configure políticas de Index State Management (ISM) paraeliminar los índices que no se utilizan periódicamente.

Error al migrar a multi-AZ con modo de espera

Se pueden producir los siguientes problemas al migrar un dominio existente a Multi-AZ con modo de espera.

Crear un índice, una plantilla de índice o una política de ISM durante la migración de dominios sin modo de espera a dominios con modo de espera

Si crea un índice al migrar un dominio de Multi-AZ sin modo de espera a uno con modo de espera, y la plantilla de índice o la política de ISM no siguen las pautas de copia de datos recomendadas, esto puede provocar una incoherencia en los datos y es posible que la migración no se realice correctamente. Para evitar esta situación, cree el nuevo índice con un recuento de copias de datos (incluidos los nodos principales y las réplicas) que sea múltiplo de tres. Puede comprobar el progreso de la migración mediante la API de `DescribeDomainChangeProgress`. Si encuentra un error en el recuento de réplicas, corrija el error y, a continuación, póngase en contacto con Soporte de AWS para volver a intentar la migración.

Número incorrecto de copias de datos

Si no tiene el número correcto de copias de datos en su dominio, la migración a Multi-AZ con modo de espera fallará.

OutOfMemoryError de JVM

`OutOfMemoryError` de una JVM significa normalmente que se ha alcanzado uno de los siguientes interruptores de la JVM.

Interruptor	Descripción	Propiedad de configuración del clúster
Interruptor principal	Porcentaje total de memoria del montón de la JVM permitido para todos los interruptores. El valor predeterminado es 95 %.	`indices.breaker.total.limit`
Interruptor de datos de campo	Porcentaje de memoria del montón de la JVM permitido para cargar en memoria un único campo de datos. El valor predeterminado es 40%. Si carga datos con campos de gran tamaño, probablemente deba aumentar este límite.	`indices.breaker.fielddata.limit`
Interruptor de solicitud	Porcentaje de memoria del montón de la JVM permitido para las estructuras de datos que se usan para responder a una solicitud de servicio. El valor predeterminado es 60%. Si sus solicitud es de servicio implican el cálculo de agregaciones, es posible que deba aumentar este límite.	`indices.breaker.request.limit`

Nodos de clúster defectuosos

Las instancias de Amazon EC2 pueden experimentar terminaciones y reinicios inesperados. Normalmente, OpenSearch Service reinicia los nodos automáticamente. Sin embargo, es posible que uno o varios nodos de un clúster de OpenSearch permanezcan en una condición de error.

Para comprobar si se da esta condición, abra el panel del dominio en la consola de OpenSearch Service. Vaya a la pestaña Estado del clúster y busque la métrica Nodos totales. Compruebe si el número de nodos que aparece es menor que el número que configuró para el clúster. Si la métrica indica que uno o varios nodos no funcionan durante más de un día, contacte con AWS Support.

También puede definir una alarma de CloudWatch para recibir un aviso cuando se produzca este problema.

> **Note**
>
> La métrica Nodos totales no es precisa durante los cambios en la configuración del clúster y durante el mantenimiento rutinario del servicio. Este es el comportamiento esperado. La métrica informará en breve del número correcto de nodos del clúster. Para obtener más información, consulte the section called “Cambios de configuración”.

Para proteger los clústeres frente a terminaciones y reinicios inesperados de los nodos, cree al menos una réplica para cada índice en su dominio de OpenSearch Service.

Límite máximo de fragmentos superado

OpenSearch y las versiones 7.x de Elasticsearch tienen una configuración predeterminada de no más de 1000 fragmentos por nodo. OpenSearch/ElasticSearch genera un error si una solicitud, como crear un nuevo índice, provocara que se supere este límite. Si detecta este error, dispone de varias opciones:

- Añada más nodos de datos al clúster.
- Aumente la configuración `_cluster/settings/cluster.max_shards_per_node`.
- Utilice la API _shrink para reducir el número de fragmentos en el nodo.

Dominio atascado en estado de procesamiento

El dominio de OpenSearch Service entra en el estado “Processing” (Procesando) cuando se encuentra en medio de un cambio de configuración. Si se inicia un cambio de configuración, el estado del dominio cambia a “Processing” (Procesando) mientras OpenSearch Service crea un nuevo entorno. En el nuevo entorno, OpenSearch Service lanza un nuevo conjunto de nodos aplicables (tales como datos, maestro o UltraWarm). Una vez que finaliza la migración, se terminan los nodos más antiguos.

El clúster puede quedarse atascado en el estado “Processing” (Procesando) si se produce una de estas situaciones:

- No se lanza un nuevo conjunto de nodos de datos.
- La migración de particiones al nuevo conjunto de nodos de datos no se realiza correctamente.
- La comprobación de validación ha fallado con errores.

Para ver pasos de resolución detallados para cada una de estas situaciones, consulte ¿Por qué mi dominio de Amazon OpenSearch Service se queda atascado en el estado “Processing” (Procesando)?.

Bajo balance de ráfaga EBS

OpenSearch Service le envía una notificación de consola cuando el balance de ráfaga de EBS en uno de sus volúmenes de uso general (SSD) está por debajo del 70 % y una notificación de seguimiento si el balance cae por debajo del 20 %. Para solucionar este problema, puede escalar verticalmente el clúster o reducir las IOPS de lectura y escritura para que se pueda acreditar el balance de ráfaga. El balance de ráfagas se mantiene en 0 para los dominios con tipos de volúmenes gp3, así como para los dominios con volúmenes gp2 que tengan un tamaño de volumen superior a 1000 GiB. Para obtener más información, consulte Volúmenes de SSD de uso general (gp2). Puede monitorizar el balance de ráfagas de EBS con la métrica `BurstBalance` de CloudWatch.

No se pueden habilitar los registros de auditoría

Cuando intente habilitar la publicación de registro de auditoría mediante la consola del servicio de OpenSearch, puede encontrar el error siguiente:

La política de acceso a recursos especificada para el grupo de registros de CloudWatch Logs no concede permisos suficientes para que Amazon OpenSearch Service cree una secuencia de registro. Compruebe la política de acceso a recursos.

Si detecta este error, compruebe que el `resource`elemento de su política incluye el ARN del grupo de registro correcto. Si lo hace, siga estos pasos:

1. Espere varios minutos.
2. Actualice la página en el navegador web.
3. Elija Seleccionar grupo existente.
4. Para Grupo de registros existente, seleccione el grupo de registro que ha creado antes de recibir el mensaje de error.
5. En la sección de políticas de acceso, elija Seleccionar política existente.
6. Para Política existente, elija la política que ha creado antes de recibir el mensaje de error.
7. Elija Habilitar.

Si el error persiste después de repetir el proceso varias veces, póngase en contacto con el servicio de Soporte de AWS.

No se puede cerrar el índice

El servicio OpenSearch es compatible con la API `_close` solo para las versiones 7.4 y posteriores de OpenSearch y Elasticsearch. Si está usando una versión anterior está restaurando un índice desde una instantánea, puede eliminar el índice existente (antes o después de volver a indexarlo).

Verificaciones de licencias del cliente

Las distribuciones predeterminadas de Logstash y Beats incluyen una comprobación de licencia de propiedad exclusiva y no se puede conectar a la versión de código abierto de OpenSearch. Asegúrese de utilizar las distribuciones de Apache 2.0 (OSS) de estos clientes con OpenSearch Service.

Limitación controlada de solicitudes

Si recibe errores persistentes de `403 Request throttled due to too many requests` o `429 Too Many Requests`, considere la posibilidad de escalar verticalmente. Amazon OpenSearch

Service realiza una limitación controlada de las solicitudes si la carga puede provocar que el uso de memoria supere el tamaño máximo de la pila de Java.

No se puede usar SSH en nodo

No se puede utilizar SSH para obtener acceso a ninguno de los nodos del clúster de OpenSearch, y no puede modificar directamente `opensearch.yml`. En su lugar, utilice la consola, AWS CLI o los SDK para configurar su dominio. Puede especificar unos ajustes en el nivel de clúster mediante las API de OpenSearch REST . Para obtener más información, consulte la Referencia de API de Amazon OpenSearch Service y the section called “Operaciones admitidas”.

Si necesita más información sobre el rendimiento del clúster, puede publicar los registros de errores y los registros lentos en CloudWatch.

Error de instantánea "No válido para la clase de almacenamiento del objeto"

Las instantáneas de OpenSearch Service no admiten la clase de almacenamiento de S3 Glacier. Es posible que aparezca este error al intentar mostrar las instantáneas si el bucket de S3 incluye una regla de ciclo de vida que traslada los objetos a la clase de almacenamiento de S3 Glacier.

Si tiene que restaurar una instantánea desde el bucket, restaure los objetos de S3 Glacier, copie los objetos a un nuevo bucket y registre el nuevo bucket como repositorio de instantáneas.

Encabezado de host no válido

OpenSearch Service requiere que los clientes especifiquen `Host` en los encabezados de solicitud. Un valor de `Host` válido es el punto de enlace del dominio sin `https://`, como:

```
Host: search-my-sample-domain-ih2lhn2ew2scurji.us-west-2.es.amazonaws.com
```

Si recibe un error de `Invalid Host Header` al realizar una reserva, compruebe que su cliente o proxy incluye el punto de enlace del dominio de OpenSearch Service (y no, por ejemplo, su dirección IP) en el encabezado `Host`.

Tipo de instancia M3 no válido

OpenSearch Service no admite agregar o modificar instancias M3 a dominios existentes que ejecutan OpenSearch o Elasticsearch versión 6.7 o posteriores. Puede seguir utilizando instancias M3 con Elasticsearch 6.5 y versiones anteriores.

Recomendamos elegir un tipo de instancia más reciente. Para dominios que ejecutan OpenSearch o Elasticsearch 6.7 o versiones posteriores, se aplica la siguiente restricción:

- Si el dominio existente no utiliza instancias M3, ya no podrá cambiar a ellas.
- Si cambia un dominio existente de un tipo de instancia M3 a otro tipo de instancia, no puede volver a cambiar.

Las consultas activas dejan de funcionar después de habilitar UltraWarm

Cuando habilita UltraWarm en un dominio, si no hay anulaciones preexistentes en la configuración de `search.max_buckets`, OpenSearch Service establece automáticamente el valor en `10000` para evitar que las consultas con gran cantidad de memoria saturen los nodos calientes. Si sus consultas activas utilizan más de 10 000 buckets, es posible que dejen de funcionar cuando habilite UltraWarm.

Dado que no puede modificar esta configuración debido a la naturaleza administrada de Amazon OpenSearch Service, debe abrir un caso de soporte para aumentar el límite. Los aumentos de límite no requieren una suscripción de premium support.

No se puede cambiar a una versión anterior después de una actualización

Las actualizaciones in situ son irreversibles, pero si se pone en contacto con AWS Support, pueden ayudarle a restaurar la instantánea automática previamente actualizada en un nuevo dominio. Por ejemplo, si actualiza un dominio de Elasticsearch 5.6 a 6.4, AWS Support puede ayudarle a restaurar la instantánea previamente actualizada en un nuevo dominio de Elasticsearch 5.6. Si ha realizado una instantánea manual del dominio original, puede realizar ese paso usted mismo.

Resumen necesario de dominios para todas las Regiones de AWS

El siguiente script utiliza el comando de Amazon EC2 describe-regions de AWS CLI para crear una lista de todas las regiones en las que OpenSearch Service podría estar disponible. A continuación, llama a list-domain-names para cada región:

```
for region in `aws ec2 describe-regions --output text | cut -f4`
do
    echo "\nListing domains in region '$region':"
    aws opensearch list-domain-names --region $region --query 'DomainNames'
done
```

Recibe el siguiente resultado para cada región:

```
Listing domains in region:'us-west-2'...
[
  {
    "DomainName": "sample-domain"
  }
]
```

Las regiones en las que OpenSearch Service no está disponible devuelven el error "Could not connect to the endpoint URL" (No se pudo conectar con la URL del punto de enlace).

Error del navegador al usar paneles de OpenSearch

El navegador incluye los mensajes de error de servicio en los objetos de respuesta HTTP cuando usa Dashboards para ver datos de su dominio de OpenSearch Service. Puede usar las herramientas para desarrolladores que suele haber disponibles en los navegadores web, como el Modo desarrollador de Chrome, para ver los errores de servicio subyacentes y como ayuda en las tareas de depuración.

Para ver errores de servicio en Chrome

1. Desde la barra del menú superior de Chrome, seleccione Ver, Desarrollador, Herramientas de desarrollador.
2. Elija la pestaña Red.
3. En la columna Estado, elija cualquier sesión HTTP que tenga un estado de 500.

Para ver errores de servicio en Firefox

1. Desde el menú, seleccione Herramientas, Desarrollador de web, Red.
2. Elija cualquier sesión HTTP que tenga un estado de 500.
3. Elija la pestaña Respuesta para ver la respuesta de servicio.

Partición de nodos y sesgo de almacenamiento

El sesgo de partición de nodo es cuando uno o más nodos de un clúster tienen significativamente más particiones que los demás nodos. El sesgo de almacenamiento de nodo es cuando uno o más nodos de un clúster tienen mucho más almacenamiento (`disk.indices`) que los demás nodos. Si bien estas dos condiciones pueden ocurrir temporalmente, por ejemplo, cuando un dominio ha reemplazado un nodo y todavía le está asignando particiones, debe abordarlas si persisten.

Para identificar ambos tipos de sesgo, ejecute la operación de la API _cat/allocation y compare las entradas `shards` y `disk.indices` en la respuesta:

```
shards    | disk.indices  | disk.used  | disk.avail   | disk.total   | disk.percent |
host     | ip       | node
   264    |      465.3mb  |   229.9mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node1
   115    |        7.9mb  |    83.7mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node2
   264    |      465.3mb  |   235.3mb  |      1.4tb   |      1.5tb   |            0 |
 x.x.x.x  | x.x.x.x  | node3
   116    |        7.9mb  |    82.8mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node4
   115    |        8.4mb  |      85mb  |     49.1gb   |     49.2gb   |            0 |
x.x.x.x  | x.x.x.x  | node5
```

Si bien es normal que haya algún sesgo de almacenamiento, cualquier valor por encima del 10 % del promedio es significativo. Cuando la distribución de las particiones está sesgada, el uso de la CPU, la red y el ancho de banda del disco también puede verse sesgado. Debido a que una mayor cantidad de datos generalmente implica más operaciones de indexación y búsqueda, los nodos más pesados también tienden a ser los nodos con mayor carga de recursos, mientras que los nodos más livianos representan una capacidad infrautilizada.

Corrección: utilice recuentos de particiones que sean múltiplos del recuento de nodos de datos para garantizar que cada índice se distribuya de manera uniforme entre los nodos de datos.

Partición del índice y el sesgo de almacenamiento

El sesgo de partición del índice es cuando uno o más nodos contienen más particiones de un índice que los otros nodos. El sesgo de almacenamiento de índice es cuando uno o más nodos contienen una cantidad desproporcionadamente grande del almacenamiento total de un índice.

El sesgo del índice es más difícil de identificar que el sesgo del nodo porque requiere cierta manipulación de la salida de la API _cat/shards. Investigue el sesgo del índice si hay algún indicio de sesgo en las métricas de clúster o nodo. A continuación, se indican algunos indicios comunes del sesgo de índice:

- Errores HTTP 429 que se producen en un subconjunto de nodos de datos
- Colocación en cola de operaciones de búsqueda o índice desigual en los nodos de datos
- Utilización desigual de la CPU o la pila de JVM en los nodos de datos

Corrección: utilice recuentos de particiones que sean múltiplos del recuento de nodos de datos para garantizar que cada índice se distribuya de manera uniforme entre los nodos de datos. Si sigue viendo un sesgo de almacenamiento de índices o partición, es posible que tenga que forzar una reasignación de particiones, que se produce con cada implementación azul/verde de su dominio de OpenSearch Service.

Operación no autorizada tras seleccionar acceso a la VPC

Cuando crea un dominio a través de la consola de OpenSearch Service, tiene la opción de seleccionar el acceso público o el acceso a la VPC. Si selecciona Acceso a la VPC, OpenSearch Service consulta la información de la VPC y genera un error si no tiene permisos adecuados:

```
You are not authorized to perform this operation. (Service: AmazonEC2; Status Code:
 403; Error Code: UnauthorizedOperation
```

Para poder realizar esta consulta, debe tener acceso a las operaciones `ec2:DescribeVpcs`, `ec2:DescribeSubnets` y `ec2:DescribeSecurityGroups`. Este requisito solo es para la consola. Si utiliza la CLI de AWS para crear y configurar un dominio con un punto de conexión de la VPC, no es necesario que tenga acceso a dichas operaciones.

Bloqueo al cargar después de crear el dominio de la VPC

Después de crear un dominio que utiliza el acceso a la VPC, es posible que la operación Configuration state (esado de configuración) del dominio no pase del estado Loading (Cargando). Si se produce este problema, es probable que AWS Security Token Service (AWS STS) esté desactivado para su región.

Para añadir puntos de enlace de la VPC a la VPC, OpenSearch Service debe asumir el rol `AWSServiceRoleForAmazonOpenSearchService`. Por lo tanto, AWS STS debe estar habilitado para crear nuevos dominios que utilicen el acceso a la VPC en una región determinada. Para obtener más información sobre la activación y desactivación de AWS STS, consulte la Guía del usuario de IAM.

Solicitudes denegadas a la API de OpenSearch

Con la introducción del control de acceso basado en etiquetas para la API de OpenSearch, es posible que empiece a ver errores de acceso denegado donde no lo hacía antes. Esto puede deberse a que una o más de sus políticas de acceso contienen `Deny` y utilizan la condición `ResourceTag`, y ahora se están respetando esas condiciones.

Por ejemplo, la política siguiente solo denegaba el acceso a la `CreateDomain` de la API de configuración, si el dominio tenía la etiqueta `environment=production`. Aunque la lista de acciones también incluye `ESHttpPut`, la declaración de denegación no se aplicó a esa acción ni a ninguna otra acción `ESHttp*`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Action": [
      "es:CreateDomain",
      "es:ESHttpPut"
    ],
    "Effect": "Deny",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:ResourceTag/environment": [
          "production"
        ]
```

```
      }
    }
  }]
}
```

Con la compatibilidad agregada de etiquetas para los métodos HTTP de OpenSearch, una política basada en la identidad de IAM como la anterior dará lugar a que se deniegue el acceso a la acción `ESHttpPut` al usuario adjunto. Anteriormente, en ausencia de validación de etiquetas, el usuario adjunto habría podido enviar solicitudes PUT.

Si empieza a ver errores de acceso denegado después de actualizar sus dominios al software de servicio R20220323 o posterior, compruebe las políticas de acceso basadas en identidad para ver si es así y actualícelas si es necesario para permitir el acceso.

No se puede conectar desde Alpine Linux

Alpine Linux limita el tamaño de respuesta de DNS a 512 bytes. Si intenta conectarse a su dominio de OpenSearch Service desde Alpine Linux versión 3.18.0 o anterior, la resolución de DNS puede tener un error si el dominio está en una VPC y tiene más de 20 nodos. Si utiliza una versión de Alpine Linux superior a la 3.18.0, debería poder resolver más de 20 hosts. Para obtener más información, consulte las notas de la versión de Alpine Linux 3.18.0.

Si su dominio está en una VPC, le recomendamos que utilice otras distribuciones de Linux, como Debian, Ubuntu, CentOS, Red Hat Enterprise Linux o Amazon Linux 2, para conectarse a él.

Hay demasiadas solicitudes de Search Backpressure

El control de admisión basado en la CPU es un mecanismo de control que limita de forma proactiva el número de solicitudes a un nodo en función de su capacidad actual, tanto en caso de incrementos orgánicos como de picos de tráfico. Las solicitudes excesivas devuelven un código de estado HTTP 429 “Demasiadas solicitudes” en caso de rechazo. Este error indica que los recursos del clúster son insuficientes, que las solicitudes de búsqueda consumen muchos recursos o que se ha producido un aumento imprevisto de la carga de trabajo.

Search Backpressure proporciona el motivo del rechazo, lo que puede ayudar a ajustar las solicitudes de búsqueda que consumen muchos recursos. En caso de picos de tráfico, recomendamos volver a intentarlo desde el lado del cliente, con un retroceso y una fluctuación exponenciales.

Error de certificado cuando se utiliza un SDK

Dado que los SDK de AWS utilizan certificados de entidad de certificación desde su equipo, los cambios en los certificados en los servidores de AWS pueden provocar errores de conexión cuando intentar usar un SDK. Los mensajes de error varían, pero suelen contener el siguiente texto:

```
Failed to query OpenSearch
...
SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

Puede evitar estos errores manteniendo actualizados los certificados de CA de su equipo y el sistema operativo. Si detecta este problema en un entorno corporativo y no administra su propio equipo, es posible que deba pedir ayuda a un administrador con el proceso de actualización.

La siguiente lista muestra las versiones mínimas necesarias del sistema operativo y Java:

- Las versiones de Microsoft Windows con actualizaciones instaladas a partir de enero de 2005 o fechas posteriores, contienen al menos uno de los CA necesarios en su lista de confianza.
- Mac OS X 10.4 con Java para Mac OS X 10.4 Release 5 (febrero de 2007), Mac OS X 10.5 (octubre de 2007) y las versiones posteriores contienen al menos uno de los CA necesarios en su lista de confianza.
- Red Hat Enterprise Linux 5 (marzo de 2007), 6 y 7 y CentOS 5, 6 y 7 contienen al menos uno de los CA necesarios en su lista de confianza predeterminada.
- Java 1.4.2_12 (mayo de 2006), 5 Update 2 (marzo de 2005) y todas las versiones posteriores, incluido Java 6 (diciembre de 2006), 7 y 8, contienen al menos uno de los CA necesarios en su lista de confianza predeterminada.

Las tres entidades de certificación son:

- Amazon Root CA 1
- Starfield Services Root Certificate Authority - G2
- Starfield Class 2 Certification Authority

Los certificados raíz de las primeras dos entidades están disponibles en Amazon Trust Services, aunque mantener el equipo actualizado es la solución más sencilla. Para obtener más información sobre certificados proporcionados por ACM, consulte Preguntas frecuentes sobre AWS Certificate Manager.

> **Note**
>
> En la actualidad, los dominios de OpenSearch Service de la región us-east-1 utilizan certificados de una entidad diferente. Tenemos previsto actualizar la región para utilizar estas nuevas entidades de certificación en un futuro próximo.

Historial de documentos de Amazon OpenSearch Service

En este tema se describen los cambios importantes en Amazon OpenSearch Service. Las actualizaciones de software de servicio añaden compatibilidad con nuevas características, parches de seguridad, correcciones de errores y otras mejoras. Para utilizar las nuevas características, tal vez deba actualizar el software de servicio de su dominio. Para obtener más información, consulte the section called “Actualizaciones del software del servicio”.

Las funciones del servicio se implementan de forma gradual según el Regiones de AWS lugar donde esté disponible el servicio. Actualizamos esta documentación solo para la primera versión. No proporcionamos información sobre la disponibilidad en regiones ni anunciamos lanzamientos posteriores en regiones. Para obtener información sobre la disponibilidad regional de las funciones del servicio y suscribirse a las notificaciones sobre actualizaciones, consulte ¿Qué hay de nuevo en el mercado? AWS

Fechas pertinentes para este historial:

- Versión del producto actual: 01/01/2021
- Última versión del producto: 1 de abril de 2024
- Última actualización de la documentación: 1 de abril de 2024

Para recibir notificaciones sobre las actualizaciones, puede suscribirse a la fuente RSS.

> **Note**
>
> Versiones de revisión: las versiones de software de servicio que terminan en “-P” y un número, como R20211203-P4, son versiones de revisión. Es probable que las revisiones incluyan mejoras de rendimiento, correcciones de errores menores y correcciones de seguridad o mejoras de posición. Dado que las revisiones no incluyen nuevas características ni cambios extraordinarios, por lo general no tienen un impacto directo en el usuario ni la documentación, y por ese motivo no se incluyen los detalles específicos de cada revisión en este historial de documentos.

Cambio	Descripción	Fecha

Soporte OpenSearch de Amazon Ingestion para Data Prepper versión 2.7	Amazon OpenSearch Ingestion añade compatibilidad con la versión 2.7 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.7.	4 de abril de 2024
Servicio de AWS acceso privado para colecciones OpenSearch sin servidor	Ahora puede conceder acceso específico Servicios de AWS, como Amazon Bedrock, a sus colecciones OpenSearch Serverless dentro de una política de acceso a la red.	28 de marzo de 2024
Actualizaciones locales de EBS	Ahora puede realizar algunos cambios de EBS en sus dominios sin una implementación azul/verde en Amazon Service. OpenSearch	14 de febrero de 2024
Visibilidad de los cambios de configuración	Ahora puedes realizar un seguimiento de los cambios en la configuración del dominio en la consola de Amazon OpenSearch Service y mediante la API de configuración.	6 de febrero de 2024

Disponibilidad general de las colecciones de búsquedas vectoriales	Las colecciones de búsquedas vectoriales de Amazon OpenSearch Serverless ya están disponibles de forma general. Durante la fase de versión preliminar se realizaron las siguientes mejoras notables: • Las colecciones de búsquedas vectoriales ahora admiten cargas de trabajo con miles de millones de vectores, cada uno con hasta 128 dimensiones. • OpenSearch Los paneles ahora admiten las colecciones de búsquedas vectoriales.	29 de noviembre de 2023
Instancias OR1	Amazon OpenSearch Service ahora admite los tipos de instancias OR1.	29 de noviembre de 2023
Consultas directas con Amazon S3 (versión preliminar)	Las consultas directas proporcionan una solución totalmente gestionada para que los datos transaccionales estén disponibles en Amazon OpenSearch Service en cuestión de segundos después de haberlos escrito en un bucket de Amazon S3.	29 de noviembre de 2023

Capacidad de 10 TiB para colecciones de series temporales	Amazon OpenSearch Serverless añade compatibilidad con hasta 10 TiB de datos de índice para recopilaciones de series temporales. Esta versión también admite una capacidad máxima permitida de 200 OCU para todos los tipos de colecciones y la posibilidad de deshabilitar las réplicas en espera al crear una colección.	29 de noviembre de 2023
OpenSearch Compatibilidad con 2.1.1	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 2.11. Esta versión incluye todas las características que formaban parte de las versiones 2.10 y 2.11. Para obtener más información, consulte las notas de las versiones 2.10 y 2.11.	17 de noviembre de 2023
Soporte OpenSearch de Amazon Ingestion para Data Prepper versión 2.6	Amazon OpenSearch Ingestion añade compatibilidad con la versión 2.6 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.6. Además, puede especificar Amazon DynamoDB como fuente de canalización. Para obtener más información, consulte Uso de una canalización OpenSearch de ingestión con Amazon DynamoDB.	17 de noviembre de 2023

Soporte OpenSearch de Amazon Ingestion para Data Prepper versión 2.5	Amazon OpenSearch Ingestion añade compatibilidad con la versión 2.5 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.5. Además, ahora puede especificar un dominio de OpenSearch servicio o una colección OpenSearch sin servidor como fuente de canalización. Para obtener más información, consulte el complemento OpenSearch fuente en la documentación de Data Prepper.	17 de noviembre de 2023
CloudFormation plantilla para inferencia remota	Para facilitar la configuración de la inferencia remota para la búsqueda semántica, Amazon OpenSearch Service proporciona una AWS CloudFormation plantilla en la consola que automatiza el proceso de aprovisionamiento de modelos.	7 de noviembre de 2023

Actualización de la política de roles vinculados a servicios	Añade los permisos necesarios para que la política `AmazonOpenSearchServiceRolePolicy` de roles vinculados a servicios asigne y desasigne direcciones IPv6. La política `AmazonElasticsearchServiceRolePolicy` de Elasticsearch en desuso también se ha actualizado para garantizar la compatibilidad con versiones anteriores.	26 de octubre de 2023
Políticas de ciclo de vida de Amazon OpenSearch Serverless	Amazon OpenSearch Serverless presenta políticas de ciclo de vida de indexación para agilizar la administración de la retención y eliminación de datos. Ahora puede usar las API o una interfaz de configuración en la consola para establecer políticas de retención de datos para las colecciones de series temporales, lo que elimina la necesidad de crear índices o scripts diarios para eliminar datos antiguos.	25 de octubre de 2023

Soporte de instancias iM4gn	Amazon OpenSearch Service ahora admite los tipos de instancias de IM4GN. Las instancias iM4GN están optimizadas para cargas de trabajo que gestionan grandes conjuntos de datos y necesitan una alta densidad de almacenamiento por vCPU.	20 de octubre de 2023
Opciones administrativas	Amazon OpenSearch Service ahora ofrece varias opciones administrativas que proporcionan un control detallado si necesitas solucionar problemas con tu dominio. Estas opciones incluyen la posibilidad de reiniciar el OpenSearch proceso en un nodo de datos y la posibilidad de reiniciar un nodo de datos.	17 de octubre de 2023
Complementos opcionales	Amazon OpenSearch Service añade compatibilidad con cuatro nuevos complementos de análisis de idiomas: Nori (coreano), Sudachi (japonés), Pinyin (chino) y STConvert Analysis (chino), así como el complemento Amazon Personalize Search Ranking.	16 de octubre de 2023

OpenSearch Compatibilidad con la versión 2.9	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 2.9. Esta versión incluye todas las características que formaban parte de las versiones 2.8 y 2.9. Para obtener más información, consulte las notas de las versiones 2.8 y 2.9.	2 de octubre de 2023
Conectores ML	Amazon OpenSearch Service añade soporte para conectore s de aprendizaje automático (ML). Los conectores facilitan el acceso a los modelos de aprendizaje automático alojados en otras Servicios de AWS plataformas de aprendizaje automático (ML) o en plataformas de aprendizaje automático (ML) de terceros.	6 de septiembre de 2023
Amazon OpenSearch Ingestion añade compatibi lidad con la versión 2.4 de Data Prepper	Amazon OpenSearch Ingestion añade compatibi lidad con la versión 2.4 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.4. Además, ahora puede especificar Amazon Managed Streaming for Apache Kafka (Amazon MSK) como fuente de canalización.	31 de agosto de 2023

Capacidad de 6 TiB para colecciones de series temporales	Amazon OpenSearch Serverless añade compatibilidad con hasta 6 TiB de datos de índice para recopilaciones de series temporales. Esta versión también admite una capacidad máxima permitida de 100 OCU para las colecciones de series temporales y de búsqueda.	15 de agosto de 2023
Colecciones de búsqueda vectorial	Amazon OpenSearch Serverless añade la opción de crear una colección de búsquedas vectoriales, que puede utilizar para almacenar incrustaciones vectoriales para potenciar las búsquedas semánticas y de similitud.	26 de julio de 2023
OpenSearch Soporte para 2.7	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 2.7. Esta versión incluye todas las características que formaban parte de las versiones 2.6 y 2.7. Para obtener más información, consulte las notas de las versiones 2.6 y 2.7.	10 de julio de 2023

Compatibilidad con Data Prepper 2.3	Amazon OpenSearch Ingestion añade compatibilidad con la versión 2.3 de Data Prepper. Para obtener más información, consulte las notas de la versión 2.3. Además, ahora puede especificar Amazon Security Lake como fuente de canalización.	26 de junio de 2023
Multi-AZ con modo de espera	Amazon OpenSearch Service añade la opción de implementar un dominio en tres zonas de disponibilidad (AZ), cada una de las cuales contiene una copia completa de los datos y los nodos de una de estas AZ actúan como zona de reserva. La opción de implementación Multi-AZ con modo de espera ofrece una disponibilidad del 99,99 % y un rendimiento uniforme en caso de que se produzca un fallo en la infraestructura.	3 de mayo de 2023

Nuevo rol vinculado a servicio	Amazon OpenSearch Service añade un rol vinculado a un servicio denominado `AWSServiceRoleForAmazonOpenSearchIngestion` , que permite a Amazon OpenSearch Ingestion enviar datos de métricas a. Amazon CloudWatch	26 de abril de 2023
OpenSearch Ingestión de Amazon	Amazon OpenSearch Ingestion es un recopilador de datos totalmente gestionado que proporciona datos de registro y rastreo en tiempo real a los dominios de OpenSearch servicio y a las colecciones OpenSearch sin servidor. OpenSearch Ingestion elimina la necesidad de utilizar soluciones de terceros, como Logstash o Jaeger, para incorporar datos a sus dominios y colecciones.	26 de abril de 2023
OpenSearch Soporte 2.5	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 2.5. Esta versión incluye todas las características que formaban parte de las versiones 2.4 y 2.5. Para obtener más información, consulte las notas de las versiones 2.4 y 2.5.	13 de marzo de 2023

Ventanas de menor actividad para mantenimiento	Amazon OpenSearch Service añade ventanas fuera de las horas pico, que son bloques de tiempo diarios de 10 horas y poco tráfico durante los cuales puede programar actualizaciones del software de servicio y optimizaciones de Auto-Tune que requieren una implementación azul/verde. Las actualizaciones en ventanas de menor actividad ayudan a minimizar la carga de los nodos maestros dedicados de un clúster durante los períodos de mayor tráfico. En el caso de los dominios nuevos creados después del 16 de febrero, la ventana de menor actividad se configura automáticamente para que funcione entre las 22:00 y las 8:00, hora local. Para los dominios existentes, debe habilitar la ventana de forma explícita.	16 de febrero de 2023

Configurar la autenticación SAML durante la creación del dominio	Amazon OpenSearch Service ahora admite la configuración de la autenticación SAML durante la creación del dominio. Anteriormente, había que configurar las opciones de SAML una vez que ya se había creado el dominio.	1 de febrero de 2023
Reindexación remota para dominios de VPC	Amazon OpenSearch Service añade la opción de una conexión de punto final de VPC entre dos dominios. Ahora se puede utilizar reindexación remota para copiar índices de un dominio de VPC a otro sin un proxy inverso. Los dominios de VPC deben ejecutar el software de servicio R20221114 o posterior para utilizar esta característica.	31 de enero de 2023

Disponibilidad general de Amazon OpenSearch Serverless	Amazon OpenSearch Serverless ya está disponible de forma general. Durante la fase de versión preliminar se realizaron las siguientes mejoras notables: • Ahora la capacidad se puede reducir verticalmente hasta el mínimo de OCU configuradas cuando se produce una disminución del tráfico en el punto de conexión de la colección. • El número máximo de OCU permitido tanto para la indexación como para la búsqueda se incrementó de 20 a 50. Cada OCU incluye suficiente almacenamiento efímero en caliente para 120 GiB de datos de índice. • Ahora puede configurar los ajustes de acceso a datos mientras crea colecciones, en lugar de tener que configurarlos en un flujo de trabajo independiente.	25 de enero de 2023

Ejecución de prueba asíncrona	Amazon OpenSearch Service ahora admite la ejecución en seco asíncrona, lo que te permite realizar una comprobación de validación antes de realizar un cambio de configuración y te notifica si los cambios provocarán una implementación azul/verde.	19 de enero de 2023
Nuevo rol vinculado a servicio	Amazon OpenSearch Service añade un rol vinculado a un servicio denominad o`AWSServiceRoleForAmazonOpenSearchServerless` , que permite a OpenSearch Serverless enviar datos de métricas a. Amazon CloudWatch	29 de noviembre de 2022
Vista previa de Amazon OpenSearch Serverless	Amazon OpenSearch Serverless es una configuración bajo demanda, de escalado automático y sin servidores para Amazon OpenSearch Service. Serverless elimina las complejidades operativas del aprovisionamiento, la configuración y el ajuste de los clústeres. OpenSearch	29 de noviembre de 2022

OpenSearch 2.3 soporte	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 2.3. Esta versión incluye todas las características que formaban parte de las versiones 2.0, 2.1 y 2.2. Para obtener más información, consulte las notas de las versiones 2.0, 2.1, 2.2 y 2.3. La versión 2.3 contiene un cambio importante. Para obtener más información, consulte Rutas de actualización admitidas.	15 de noviembre de 2022
Compatibilidad con el complemento de Notificaciones	Amazon OpenSearch Service ahora es compatible con el complemento Notifications, que ofrece una ubicación central para todas las notificaciones de los OpenSearch complementos. A partir de la versión 2.0, los destinos de alerta quedaron obsoletos y se sustituyeron por canales de notificación.	15 de noviembre de 2022

Compatibilidad con Kibana 7.1.1	Los dominios OpenSearch de Amazon Service que ejecutan Elasticsearch 7.1 ahora admiten la última versión del parche para Kibana 7.1.1, que añade correccio nes de errores y mejora la seguridad. Cuando actualice sus dominios 7.1 al software de servicio R20221114, OpenSearch Service los actualizará automáticamente a esta versión de parche.	15 de noviembre de 2022
Compatibilidad con Kibana 6.8.13	Los dominios OpenSearch de Amazon Service que ejecutan Elasticsearch 6.8 ahora admiten la última versión del parche para Kibana 6.8.13, que añade correccio nes de errores y mejora la seguridad. Cuando actualice sus dominios 6.8 al software de servicio R20221114, OpenSearch Service los actualizará automáticamente a esta versión de parche.	15 de noviembre de 2022

Compatibilidad con Kibana 6.3.2	Los dominios OpenSearch de Amazon Service que ejecutan Elasticsearch 6.3 ahora admiten la última versión del parche para Kibana 6.3.2, que añade correccio nes de errores y mejora la seguridad. Cuando actualice sus dominios 6.3 al software de servicio R20221114, OpenSearch Service los actualizará automáticamente a esta versión de parche.	15 de noviembre de 2022

AWS PrivateLink	Con los puntos de enlace OpenSearch de VPC gestionados por Amazon Service, puede conectarse directamente a los dominios de VPC de servicio mediante un punto de enlace de OpenSearch VPC de interfaz en lugar de conectarse a través de Internet. Solo se puede acceder a un punto final de OpenSearch VPC gestionado por el servicio desde la VPC en la que se aprovisiona el punto de conexión o desde cualquier VPC emparejada con la VPC en la que se aprovisio na el punto final, según lo permitan las tablas de enrutamiento y los grupos de seguridad. Su dominio de VPC debe ejecutar el software de servicio R20220928 o posterior para conectarse a un punto de conexión de VPC de interfaz.	7 de noviembre de 2022
Correcciones de errores y mejoras de rendimiento	El software de servicio R20220928 incluye correccio nes de errores y mejoras de rendimiento, incluido un registro SAML mejorado. La actualización también cambia el inquilino predeterminado a `Global` en lugar de `Private`.	3 de octubre de 2022

Referencia de la API mejorada	Amazon OpenSearch Service ofrece una referencia de API de configuración mejorada y completa. Las nuevas referencias contienen todos los tipos de datos y acciones disponibles, ejemplos de sintaxis de solicitudes y respuestas, y enlaces a las referencias de SDK correspondientes para todos los idiomas admitidos.	13 de septiembre de 2022
Validación azul-verde	Amazon OpenSearch Service ahora realiza una comprobación de validación antes de las implementaciones azul/verde y muestra errores de validación si tu dominio no es apto para una actualización.	16 de agosto de 2022
OpenSearch 1.3 soporte	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 1.3. Para obtener más información, consulte las notas de la versión 1.3.	27 de julio de 2022

Compatibilidad con el complemento ML Commons	Amazon OpenSearch Service añade compatibilidad con el complemento ML Commons, que proporciona un conjunto de algoritmos de aprendizaje automático comunes mediante llamadas a la API de transport e y REST. También puede interactuar con el complemen to ML Commons a través de comandos de PPL.	27 de julio de 2022
Compatibilidad con los volúmenes gp3	Amazon OpenSearch Service añade compatibilidad con el tipo de volumen SSD de uso general de gp3 EBS. Puede especificar las IOPS aprovisionadas y el rendimien to adicionales al crear o modificar el dominio.	26 de julio de 2022
Documentación de prácticas recomendadas mejoradas	La documentación OpenSearc h de Amazon Service proporciona mejores prácticas operativas mejoradas y recomendaciones generales para crear y operar dominios OpenSearch de servicio.	6 de julio de 2022
Integración con Service Quotas	Ahora puedes ver las cuotas de Amazon OpenSearch Service y solicitar aumentos de cuota desde la consola Service Quotas.	29 de junio de 2022

Control de acceso a la API basado en OpenSearch etiquetas	Ahora puede usar etiquetas para controlar el acceso a las OpenSearch API. Anteriorm ente, solo podía utilizar etiquetas para controlar el acceso a la API de configura ción.	16 de junio de 2022
Búsqueda entre clústeres en regiones	Ahora se admite la búsqueda entre clústeres Regiones de AWS siempre que ambos dominios ejecuten la versión 7.10 o posterior de Elasticse arch, o cualquier versión de. OpenSearch	14 de junio de 2022
Compatibilidad con Kibana 5.6 individual	Amazon OpenSearch Service añade soporte para una versión única de Kibana 5.6.16. Con Kibana 5.6.16 individual, puede utilizar Kibana 5.6 como front-end mientras se conecta a las versiones 5.1, 5.3, 5.5 y 5.6 de Elasticsearch. Debe estar en el software del servicio R20220323 o posterior para utilizar Kibana 5.6 individual.	4 de abril de 2022

R20220323-P1	Amazon OpenSearch Service publicó recientemente la actualización del software de servicio R20220323, pero la actualización se anuló posteriormente debido a un problema. Se recomiend a actualizar los dominios a la versión de revisión R20220323-P1 o posterior, que soluciona el problema.	4 de abril de 2022
OpenSearch 1.2 soporte	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 1.2. Para obtener más informaci ón, consulte las notas de la versión 1.2.	4 de abril de 2022
Observabilidad	La instalación predeterminada de OpenSearch Dashboard s for Amazon OpenSearch Service incluye el complemen to Observability, que puedes usar para visualizar eventos basados en datos mediante el lenguaje de procesami ento canalizado (PPL) para explorar y consultar tus datos. El complemento requiere la versión OpenSearch 1.2 o una versión posterior y el software de servicio R20220323 o una versión posterior.	4 de abril de 2022

Compatibilidad con Kibana 7.7.1	Los dominios OpenSearch de Amazon Service que ejecutan Elasticsearch 7.7 ahora admiten la última versión del parche para Kibana 7.7, que añade correccio nes de errores y mejora la seguridad. Cuando actualice sus dominios 7.7 al software de servicio R20220323 o posterior, OpenSearch Service los actualizará automátic amente a esta versión de parche.	4 de abril de 2022

Cambios en la métrica de presión de memoria de JVM	Amazon OpenSearch Service cambió la lógica de las `JVMMemoryPressure` CloudWatch métricas para reflejar con mayor precisión el uso de la memoria. Anteriormente, las métricas solo tenían en cuenta el grupo de memoria de antigua generación del montón de JVM. Con este cambio, la métrica también tiene en cuenta el grupo de memoria de nueva generación. Después de actualizar el dominio al software del servicio R20220323, es posible que observe un incremento en las métricas `JVMMemoryPressure` , `MasterJVMMemoryPressure` o `WarmJVMMemoryPressure` .	4 de abril de 2022
Diccionarios personalizados con el complemento IK (Chinese) Analysis	Amazon OpenSearch Service ahora admite el uso de diccionarios personalizados con el complemento IK (chino) Analysis.	4 de abril de 2022

Replicación entre clústeres en dominios existentes	Amazon OpenSearch Service eliminó la limitación de que solo se pueden implementar la búsqueda y la replicación entre clústeres en dominios creados a partir del 3 de junio de 2020. Ahora puede habilitar estas caracterí sticas en todos los dominios, independientemente de cuándo se hayan creado. Ambos dominios deben estar en el software del servicio R20220323 o posterior.	4 de abril de 2022
Visibilidad de implementación azul-verde	Amazon OpenSearch Service ahora ofrece más visibilidad del progreso de las implement aciones azul/verde. Puede supervisar estos detalles en la consola o mediante la API de configuración.	27 de enero de 2022

Control de acceso detallado en dominios existentes	Ahora puede habilitar el control de acceso detallado en los dominios existentes. Puede habilitar un período de migración temporal para las políticas de acceso abiertas o basadas en IP para garantizar que los usuarios puedan seguir accediendo a su dominio mientras crea y asigna roles. La habilitación del control de acceso detallado en los dominios existentes requiere el software de servicio R20211203 o posterior.	6 de enero de 2022
Se han cambiado los nombres de las funciones de OpenSearch	Con el software de servicio R20211203, se le ha cambiado el nombre al rol `kibana_user` por `opensearch_dashboards_user`, y a `kibana_read_only` se le ha cambiado el nombre por `opensearch_dashboards_read_only`. Este cambio se aplica a todos los 1 recién creados OpenSearch . x dominios. En el caso de OpenSearch los dominios existentes que se actualicen al software de servicio R20211203, las funciones siguen siendo las mismas.	4 de enero de 2022

OpenSearch 1.1 soporte	Amazon OpenSearch Service ahora es compatible con OpenSearch la versión 1.1. Para obtener más informaci ón, consulte las notas de la versión 1.1.	4 de enero de 2022
Editor visual de ISM	La instalación predeterminada de OpenSearch Dashboard s for Amazon OpenSearc h Service ahora admite el editor visual de las políticas de ISM. Esta función requiere la versión OpenSearch 1.1 o una versión posterior.	4 de enero de 2022
Actualización de la prevenció n del suplente confuso entre servicios	Amazon OpenSearch Service admite el uso de las claves de contexto de condición `aws:SourceAccount` global `aws:SourceArn` y las claves de contexto en las políticas de recursos de IAM para evitar el confuso problema de los diputados . Debe estar en el software de servicio R20211203 o posterior para utilizar estas claves de condición.	4 de enero de 2022

Parche de Log4j	El software de servicio R20211203-P2 actualiza la versión de Log4j utilizada en Service, tal como se recomienda en las recomendaciones de los documentos CVE-2021-44228 y OpenSearch CVE-2021-45046. El parche se aplica a los dominios que ejecutan todas las versiones OpenSearch de Elasticsearch y de Elasticsearch. OpenSearch El servicio seguirá actualizando varias versiones de Log4j internamente y no se restringirán necesariamente a la última versión de Log4j. La versión de Log4j de su dominio depende de la versión de software que ejecute el dominio. Sin embargo, independientemente de la versión de Log4j, siempre que ejecute R20211203-P2 o posterior, sus dominios contienen la actualización de Log4j necesaria para abordar CVE-2021-44228 y CVE-2021-45046.	15 de diciembre de 2021

Replicación entre clústeres	La replicación entre clústeres le permite replicar índices, mapeos y metadatos de un dominio de servicio a otro. OpenSearch La replicación entre clústeres requiere un dominio que ejecute Elasticsearch 7.10 o 1.1 o una versión posterior. OpenSearch	5 de octubre de 2021
AWS Nuevas políticas administradas	El lanzamiento de Amazon OpenSearch Service incluye nuevas políticas AWS gestionadas y la obsolescencia de las políticas antiguas.	8 de septiembre de 2021
Compatibilidad con Kibana 6.4.3	Los dominios OpenSearch de Amazon Service que ejecutan la versión 6.4 antigua de Elasticsearch ahora son compatibles con la última versión del parche para Kibana 6.4, que añade correcciones de errores y mejora la seguridad. OpenSearch El servicio actualizará automáticamente los dominios a esta versión del parche.	8 de septiembre de 2021

Flujos de datos	Amazon OpenSearch Service añade soporte para flujos de datos, lo que simplific a el proceso de gestión de datos de series temporales. Su dominio debe ejecutar la OpenSearch versión 1.0 o una versión posterior para utilizar los flujos de datos.	8 de septiembre de 2021
OpenSearch Servicio Amazon	AWS cambia el nombre de Amazon OpenSearch Service para eliminar la antigua marca «Elasticsearch». Amazon OpenSearch Service es compatible con OpenSearch Elasticsearch OSS heredado. Al crear un clúster, tiene la opción de elegir qué motor de búsqueda utilizar. OpenSearc h El servicio ofrece una amplia compatibilidad con Elasticse arch OSS 7.10, la versión final de código abierto del software.	8 de septiembre de 2021

Almacenamiento en frío	El almacenamiento en frío es un nuevo nivel de almacenamiento para datos históricos o a los que se accede con poca frecuencia. Los índices almacenados en frío solo ocupan el almacenamiento de S3 y no tienen informática vinculada a ellos. El almacenamiento en frío requiere un dominio que ejecute Elasticsearch 7.9 o posterior y el software de servicio R20210426 o posterior.	13 de mayo de 2021
Instancias de Graviton basadas en ARM	Amazon OpenSearch Service ahora admite los tipos de instancias de Graviton basados en ARM (M6G, C6G, R6G y R6GD). Los tipos de instancias de Graviton están disponibles en dominios nuevos y existentes que ejecutan Elasticsearch 7.9 o posterior y el software de servicio R20210331 o posterior.	4 de mayo de 2021

Plantillas de ISM	Amazon OpenSearch Service añade compatibilidad con las plantillas de ISM, que te permiten adjuntar automáticamente una política de ISM a un índice si el índice coincide con un patrón definido en la política. Las plantillas de ISM requieren el software de servicio R20210426 o posterior. Esta actualización también deja obsoleta la configuración `policy_id`, que significa que ya no puede utilizar plantillas de índice para aplicar políticas de ISM a los índices recién creados. La actualización introduce un cambio radical en las CloudFormation plantillas existentes que utilizan esta configuración.	27 de abril de 2021
Compatibilidad con Elasticsearch 7.10	Amazon OpenSearch Service ahora es compatible con la versión 7.10 de Elasticsearch. Para obtener más información, consulte las notas de la versión de 7.10.	21 de abril de 2021

Búsqueda asíncrona	Amazon OpenSearch Service ahora admite la búsqueda asíncrona, lo que te permite ejecutar solicitudes de búsqueda en segundo plano. La búsqueda asíncrona requiere un dominio que ejecute Elasticsearch 7.10 o posterior, y el software de servicio R20210331 o posterior.	21 de abril de 2021
Control de acceso basado en etiquetas para la API de configuración	Ahora puede usar AWS etiquetas para controlar el acceso a la API de configuración de Amazon ES.	2 de marzo de 2021
Ajuste automático	Amazon OpenSearch Service añade Auto-Tune, que utiliza las métricas de rendimiento y uso del clúster para sugerir cambios en la configuración de JVM de los nodos. El ajuste automático requiere un dominio que ejecute Elasticsearch 6.7 o posterior y el software de servicio R20201117 o posterior.	24 de febrero de 2021

Trace Analytics	La instalación predeterminada de Kibana for Amazon OpenSearch Service ahora incluye el complemento de análisis de rastreo, que te permite monitorear los datos de rastreo de tus aplicaciones distribuidas. El complemento requiere un dominio que ejecute Elasticsearch 7.9 o posterior y un software de servicio R20210201 o posterior.	17 de febrero de 2021
Métricas de particiones	Amazon OpenSearch Service añade las siguientes CloudWatch métricas para el seguimiento del estado de los fragmentos:`Shards.active` ,`Shards.unassigned` ,, `Shards.delayedUnassigned` `Shards.activePrimary` `Shards.initializing` ,`Shards.relocating` . Las métricas están disponibles en dominios con el software de servicio R20210201 o posterior.	17 de febrero de 2021

Informes de Kibana	La instalación predeterminada de Kibana for Amazon OpenSearch Service ahora admite informes bajo demanda para las páginas Discover, Visualize y Dashboard. Esta característica requiere Elasticsearch 7.9 o posterior y el software de servicio R20210201 o posterior.	17 de febrero de 2021
Compatibilidad con Kibana 5.6.16	Los dominios OpenSearch de Amazon Service que ejecutan Elasticsearch 5.6 ahora son compatibles con la última versión del parche para Kibana 5.6, que añade correcciones de errores y mejora la seguridad. Amazon ES actualizará de forma automática los dominios a esta versión de parche.	17 de febrero de 2021
Cifrado para dominios existentes	Amazon OpenSearch Service ahora permite habilitar el cifrado de los datos en reposo y el node-to-node cifrado en los dominios existentes que ejecutan Elasticsearch 6.7 o una versión posterior. Después de habilitar esta configuración, no podrá deshabilitarla.	27 de enero de 2021

Reindexación remota	Amazon OpenSearch Service ahora admite la reindexación remota, lo que te permite migrar índices desde dominios remotos. Esta característica requiere el software de servicio R20201117 o una versión posterior.	24 de noviembre de 2020
Lenguaje de procesamiento con plecas	Amazon OpenSearch Service ahora es compatible con el lenguaje de procesamiento canalizado (PPL), un lenguaje de consultas que te permite usar la sintaxis pipe (|) para consultar los datos almacenados en Elasticsearch. Esta característica requiere el software de servicio R20201117 o una versión posterior. Para obtener más información, consulte .	24 de noviembre de 2020
Cuadernos de Kibana	Amazon OpenSearch Service añade compatibilidad con las libretas Kibana, lo que te permite combinar visualizaciones en directo y texto narrativo en una única interfaz. Esta característica requiere el software de servicio R20201117 o una versión posterior.	24 de noviembre de 2020

Diagramas de Gantt	La instalación predeterminada de Kibana for Amazon OpenSearch Service ahora admite un nuevo tipo de visualización, los diagramas de Gantt. Esta característica requiere el software de servicio R20201117 o una versión posterior.	24 de noviembre de 2020
Compatibilidad con Elasticsearch 7.9	Amazon OpenSearch Service ahora es compatible con la versión 7.9 de Elasticsearch. Para obtener más información, consulte las notas de la versión de 7.9.	24 de noviembre de 2020
Actualizaciones de detección de anomalías	La detección de anomalías para Amazon OpenSearch Service añade compatibilidad con la alta cardinalidad, lo que te permite clasificar las anomalías con una dimensión como la dirección IP, el identificador del producto, el código de país, etc. Esta característica requiere el software de servicio R20201117 o una versión posterior.	24 de noviembre de 2020

Actualizaciones de diccionario dinámicas	Amazon OpenSearch Service ahora te permite actualizar tus analizadores de búsqueda sin tener que volver a indexarlos. Puede actualizar los archivos de diccionario en algunos o todos sus dominios y Amazon ES realiza un seguimien to de las versiones de los paquetes a lo largo del tiempo para que tenga un historial de lo que cambió y cuándo. Esta caracterí stica requiere el software de servicio R20201019 o una versión posterior.	17 de noviembre de 2020
Puntos de conexión personali zados	Amazon OpenSearch Service ahora admite puntos de enlace personalizados, lo que te permite asignar una nueva URL a tu dominio de Amazon ES. Si alguna vez intercamb ia dominios, puede mantener la misma URL. Esta caracterí stica requiere el software de servicio R20201019 o una versión posterior.	5 de noviembre de 2020

Nuevos complementos de idioma	Amazon OpenSearch Service ahora admite los complementos IK (Chinese) Analysis, Vietnamese Analysis y Thai Analysis en dominios que ejecutan Elasticsearch 7.7 o posterior con el software de servicio R20201019 o posterior.	28 de octubre de 2020
Compatibilidad con Elasticsearch 7.8	Amazon OpenSearch Service ahora es compatible con la versión 7.8 de Elasticsearch. Para obtener más información, consulte las notas de la versión de 7.8.	28 de octubre de 2020
Autenticación SAML para Kibana	Amazon OpenSearch Service ahora admite la autenticación SAML para Kibana, que te permite usar proveedores de identidad de terceros para iniciar sesión en Kibana, administrar un control de acceso detallado, buscar tus datos y crear visualizaciones. Esta característica requiere el software de servicio R20201019 o una versión posterior.	27 de octubre de 2020
Instancias T3	Amazon OpenSearch Service ahora admite los tipos de instancia `t3.medium` y `t3.small`.	23 de septiembre de 2020

Registros de auditoría	Amazon OpenSearch Service ahora admite los registros de auditoría de tus datos, lo que te permite realizar un seguimiento de los intentos fallidos de inicio de sesión, del acceso de los usuarios a índices, documentos y campos, y mucho más. Esta característica requiere el software de servicio R20200910 o una versión posterior.	16 de septiembre de 2020
UltraWarm actualizaciones	UltraWarm for Amazon OpenSearch Service añade nuevas métricas, nuevos ajustes, una cola de migración más grande y una API de cancelación. Estas actualizaciones requieren el software de servicio R20200910 o posterior. Para obtener más información, consulte .	14 de septiembre de 2020
Learning to Rank	Amazon OpenSearch Service ahora es compatible con el complemento de código abierto Learning to Rank, que te permite utilizar tecnologías de aprendizaje automático para mejorar la relevancia de las búsquedas. Esta característica requiere el software de servicio R20200721 o una versión posterior.	27 de julio de 2020

Similitud coseno de k-NN	k-Nearest Neighbor (k-NN) ahora permite buscar “vecinos más cercanos” por similitud coseno además de la distancia euclidiana. Esta caracterí stica requiere el software de servicio R20200721 o una versión posterior.	23 de julio de 2020
Compresión con gzip	Amazon OpenSearch Service ahora admite la compresió n gzip para la mayoría de las solicitudes y respuestas HTTP, lo que puede reducir la latencia y conservar el ancho de banda. Esta caracterí stica requiere el software de servicio R20200721 o una versión posterior.	23 de julio de 2020
Compatibilidad con Elasticse arch 7.7	Amazon OpenSearch Service ahora es compatible con la versión 7.7 de Elasticsearch. Para obtener más informaci ón, consulte las notas de la versión de 7.7.	23 de julio de 2020
Servicio de mapas de Kibana	La instalación predeterm inada de Kibana for Amazon OpenSearch Service ahora incluye un servidor de mapas WMS, excepto para los dominios de las regiones de India y China.	18 de junio de 2020

Mejoras de SQL	El soporte de SQL para Amazon OpenSearch Service ahora admite muchas operaciones nuevas, una interfaz de usuario de Kibana dedicada para la exploración de datos y una CLI interactiva. Para obtener más información, consulte .	3 de junio de 2020
Búsqueda en clústeres	Amazon OpenSearch Service te permite realizar consultas y agregaciones entre clústeres en varios dominios conectados.	3 de junio de 2020
Detección de anomalías	Amazon OpenSearch Service te permite detectar automáticamente las anomalías casi en tiempo real.	3 de junio de 2020
UltraWarm	UltraWarm El almacenamiento de Amazon OpenSearch Service ha salido de la versión preliminar pública y ahora está disponible de forma general. La función ahora es compatible con una gama más amplia de versiones y Regiones de AWS. Para obtener más información, consulte .	5 de mayo de 2020

Diccionarios personalizados	Amazon OpenSearch Service te permite cargar archivos de diccionarios personalizados para usarlos con tu clúster. Estos archivos mejoran los resultados de la búsqueda al indicarle a Elasticsearch que ignore ciertas palabras de alta frecuencia o que trate los términos como equivalentes.	21 de abril de 2020
Compatibilidad con Elasticsearch 7.4	Amazon OpenSearch Service ahora es compatible con la versión 7.4 de Elasticsearch. Para obtener más información, consulte Versiones compatibles.	12 de marzo de 2020
k-NN	Amazon OpenSearch Service añade compatibilidad con la búsqueda del vecino más cercano (k-NN). K-nn requiere el software de servicio R20200302 o posterior.	3 de marzo de 2020
Index State Management	Amazon OpenSearch Service añade Index State Management (ISM), que te permite automatizar las tareas rutinarias, como la eliminación de índices cuando llegan a cierta edad. Esta característica requiere el software de servicio R20200302 o una versión posterior.	3 de marzo de 2020

Compatibilidad con Elasticsearch 5.6.16	Amazon OpenSearch Service ahora es compatible con la última versión del parche de la versión 5.6, que añade correcciones de errores y mejora la seguridad. Amazon ES actualizará de forma automática los dominios 5.6 existentes a esta versión. Tenga en cuenta que esta versión de Elasticsearch informa incorrectamente su versión como 5.6.17.	2 de marzo de 2020
Control de acceso detallado	Amazon OpenSearch Service ahora admite un control de acceso detallado, que ofrece seguridad a nivel de índice, documento y campo, la multitenencia de Kibana y la autenticación básica HTTP opcional para su clúster.	11 de febrero de 2020

UltraWarm almacenamiento (versión preliminar)	Amazon OpenSearch Service añade UltraWarm un nuevo nivel de almacenamiento en caliente que utiliza Amazon S3 y una sofisticada solución de almacenamiento en caché para mejorar el rendimiento. Para los índices en los que no está escribiendo activamente y consultando con menos frecuencia, el UltraWarm almacenamiento ofrece costos por GiB significativamente más bajos.	3 de diciembre de 2019
Características de cifrado para las regiones de China	El cifrado de los datos en reposo y el node-to-node cifrado ya están disponibles en la región de `cn-north-1` China (Pekín) y en la región de `cn-northwest-1` China (Ningxia).	20 de noviembre de 2019
Exigir HTTPS	Ahora puede exigir que todo el tráfico a sus dominios de Amazon ES llegue a través de HTTPS. Al configurar su dominio, marque la casilla Exigir HTTPS. Esta característica requiere el software de servicio R20190808 o una versión posterior.	3 de octubre de 2019

Compatibilidad con Elasticsearch 7.1 y 6.8	Amazon OpenSearch Service ahora es compatible con las versiones 7.1 y 6.8 de Elasticsearch. Para obtener más información, consulte Versiones compatibles.	13 de agosto de 2019
Instantáneas cada hora	En lugar de instantáneas diarias, Amazon OpenSearch Service ahora toma instantáneas cada hora de los dominios que ejecutan Elasticsearch 5.3 y versiones posteriores para que tengas copias de seguridad más frecuentes desde las que restaurar tus datos.	8 de julio de 2019
Compatibilidad con Elasticsearch 6.7	Amazon OpenSearch Service ahora es compatible con la versión 6.7 de Elasticsearch. Para obtener más información, consulte Versiones compatibles.	29 de mayo de 2019
Compatibilidad con SQL	Amazon OpenSearch Service ahora te permite consultar tus datos mediante SQL. La compatibilidad con SQL requiere el software de servicio R20190418 o una versión posterior.	15 de mayo de 2019

Tipos de instancias de la serie 5	Amazon OpenSearch Service ahora admite los tipos de instancias M5, C5 y R5. En comparación con los tipos de instancias de la generación anterior, estos nuevos tipos ofrecen un mejor rendimien to a precios más bajos. Para obtener más información, consulte Límites.	24 de abril de 2019
Compatibilidad con Elasticse arch 6.5	Amazon OpenSearch Service ahora es compatible con la versión 6.5 de Elasticsearch.	8 de abril de 2019
Alertas	Las alertas para Amazon OpenSearch Service le notifican cuando los datos de uno o más índices de Amazon ES cumplen determinadas condiciones. Las alertas requieren el software de servicio R20190221 o una versión posterior.	25 de marzo de 2019
Compatibilidad con tres zonas de disponibilidad	Amazon OpenSearch Service ahora admite tres zonas de disponibilidad en muchas regiones. Esta versión incluye también una experiencia de consola simplificada. Este multi-AZ requiere el software de servicio R20181023 o una versión posterior.	7 de febrerode 2019

Compatibilidad con Elasticsearch 6.4	Amazon OpenSearch Service ahora es compatible con la versión 6.4 de Elasticsearch.	23 de enero de 2019
Clústeres de 200 nodos	Ahora Amazon ES permite crear clústeres con hasta 200 nodos de datos y un total de 3 PB de almacenamiento.	22 de enero de 2019
Actualizaciones del software del servicio	Amazon ES ahora permite actualizar manualmente el software de servicio de su dominio con el fin de obtener beneficios de nuevas características con mayor rapidez o realizar las actualizaciones en el momento en que hay menos tráfico. Para obtener más información, consulte .	20 de noviembre de 2018
Nuevas métricas CloudWatch	Amazon ES ahora ofrece métricas a nivel de nodo y las pestañas Estado del clúster e Estado de instancia en la consola de Amazon ES.	20 de noviembre de 2018
Compatibilidad en China (Pekín)	Amazon OpenSearch Service ya está disponible en la región cn-north-1, donde admite los tipos de instancias M4, C4 y R4.	17 de octubre de 2018

Sin cifrado ode-to-node	Amazon OpenSearch Service ahora admite el node-to-node cifrado, lo que mantiene los datos cifrados a medida que Amazon ES los distribuye por todo el clúster.	18 de septiembre de 2018
Actualizaciones de versiones in situ	Amazon OpenSearch Service ahora admite actualizaciones de versiones locales.	14 de agosto de 2018
Compatibilidad con Elasticsearch 6.3 y 5.6	Amazon OpenSearch Service ahora es compatible con las versiones 6.3 y 5.6 de Elasticsearch.	14 de agosto de 2018
Registros de errores	Amazon ES ahora le permite publicar los registros de errores de Elasticsearch en Amazon. CloudWatch	31 de julio de 2018
Instancias reservadas en China (Ningxia)	Amazon ES ahora ofrece instancias reservadas en la región China (Ningxia).	29 de mayo de 2018
Instancias reservadas	Ahora Amazon ES ofrece compatibilidad con Instancias reservadas.	7 de mayo de 2018

Actualizaciones anteriores

En la siguiente tabla se describen los cambios importantes en Amazon ES realizados antes de mayo de 2018.

Cambio	Descripción	Fecha
Autenticación de Amazon Cognito para Kibana	Amazon ES ahora ofrece protección de la página de inicio de sesión para Kibana. Para obtener más información, consulte the section called “Descripción de la autenticación de Amazon Cognito para OpenSearch Dashboards”.	2 de abril de 2018
Compatibilidad con Elasticsearch 6.2	Amazon OpenSearch Service ahora es compatible con la versión 6.2 de Elasticsearch.	14 de marzo de 2018
Complemento Korean Analysis	Amazon ES ahora admite una versión optimizada para memoria del complemento del análisis coreano Seunjeon.	13 de marzo de 2018
Actualizaciones de control de acceso instantáneas	Los cambios en las políticas de control de acceso en los dominios de Amazon ES ahora se aplican al instante.	7 de marzo de 2018
Escala de petabytes	Amazon ES admite ahora tipos de instancias I3 y una capacidad total de almacenamiento del dominio de hasta 1,5 PB. Para obtener más información, consulte the section called “Escala de petabytes”.	19 de diciembre de 2017
Cifrado de datos en reposo	Amazon ES ahora admite el cifrado de datos en reposo. Para obtener más información, consulte the section called “Cifrado en reposo”.	7 de diciembre de 2017
Compatibilidad con Elasticsearch 6.0	Amazon ES ahora admite la versión 6.0 de Elasticse arch. Para ver consideraciones e instrucciones sobre las migraciones, consulte the section called “Actualización de dominios”.	6 de diciembre de 2017
Compatibilidad con VPC	Amazon ES ahora permite lanzar dominios dentro de una Amazon Virtual Private Cloud. La compatibilidad con VPC proporciona una capa de seguridad adicional y simplifica las comunicaciones entre Amazon ES y otros servicios dentro de una VPC. Para obtener más informaci ón, consulte the section called “Compatibilidad con VPC”.	17 de octubre de 2017

Cambio	Descripción	Fecha
Publicación de registros lentos	Amazon ES ahora admite la publicación de registros lentos en CloudWatch Logs. Para obtener más información, consulte the section called “Monitoreo de registros”.	16 de octubre de 2017
Compatibilidad con Elasticsearch 5.5	Amazon ES ahora admite la versión 5.5 de Elasticsearch. Ahora puede restablecer las instantáneas automatizadas sin contactar con AWS Support y almacenar scripts con la API de `_scripts`.	7 de septiembre de 2017
Compatibilidad con Elasticsearch 5.3	Amazon ES agregó compatibilidad a la versión 5.3 de Elasticsearch.	1 de junio de 2017
Más instancias y capacidad de EBS por clúster	Amazon ES ahora admite hasta 100 nodos y 150 TB de capacidad de EBS por clúster.	5 de abril de 2017
Compatibilidad en Canadá (Central) y la UE (Londres)	Amazon ES agregó compatibilidad en las siguiente s regiones: Canadá (Central), ca-central-1 y Europa (Londres), eu-west-2.	20 de marzo de 2017
Más instancias y mayores volúmenes de EBS	Amazon ES incorpora la compatibilidad con más instancias y mayores volúmenes de EBS.	21 de febrero de 2017
Compatibilidad con Elasticsearch 5.1	Amazon ES agregó compatibilidad a la versión 5.1 de Elasticsearch.	30 de enero de 2017
Compatibilidad con el complemento Phonetic Analysis	Amazon ES lleva incorporada la integración con el complemento Phonetic Analysis, que permite ejecutar consultas con el operador “sounds-like” (sonido similar a) en los datos.	22 de diciembre de 2016
Compatibilidad con la región EE. UU Este (Ohio)	Amazon ES incorpora compatibilidad con la siguiente región: Este de EE. UU. (Ohio), us-east-2.	17 de octubre de 2016

Cambio	Descripción	Fecha
Nueva métrica de desempeño	Amazon ES agregó una métrica de rendimiento, `ClusterUsedSpace` .	29 de julio de 2016
Compatibilidad con Elasticsearch 2.3	Amazon ES agregó compatibilidad con la versión 2.3 de Elasticsearch.	27 de julio de 2016
Compatibilidad con la región Asia Pacífico (Mumbai)	Amazon ES agregó compatibilidad a la siguiente región: Asia-Pacífico (Mumbai), ap-south-1.	27 de junio de 2016
Más instancias por clúster	Amazon ES aumenta de 10 a 20 el número máximo de instancias (recuento de instancias) por clúster.	18 de mayo de 2016
Compatibilidad con la región Asia Pacífico (Seúl)	Amazon ES agregó compatibilidad a la siguiente región: Asia-Pacífico (Seúl), ap-northeast-2.	28 de enero de 2016
Amazon ES	Versión inicial.	1 de octubre de 2015

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

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.